

# **Kingdom of Bahrain State of the Nation Review of Internet Safety**

**July 2010**

---

**Prof. Julia Davidson, Kingston University and Dr Elena  
Martellozzo, Middlesex University**

**on behalf of**

**The Telecommunications Regulatory Authority,  
Kingdom of Bahrain**

---

## 1. Acknowledgements

We would like to thank the Telecommunications Regulatory Authority (TRA) staff who contributed to the planning and organization of the research. We are particularly grateful to the chairman Dr. Mohamed Al Amer for his support. We are grateful to Nick Truman, Internet Security Advisor for his assistance and invaluable support throughout this project; to Robert Middlehurst, Deputy General Director, for his support and constant encouragement; to Mohammed Mahmood, director of technical and operations, and Basil Al Arrayed, Director of Communications and Consumer Affairs for their help. We are also grateful to Ghada Ebrahim Alqassab, Reem Al Alawi, Rana Majed Sultan, Abdulelah Abdulla and Adel Darwish.

We would like to thank Dr Khalid Al-Mutawah for managing and conducting the qualitative focus groups in the public schools and his colleagues Doctor Athraa Al Mosawi, Doctor Mohamed Baqer and Ghazwa B. Sulaibeekh from Bahrain University for their invaluable help with the data collection. We would also like to thank Mazen Khamis, Samuel, VK and Sundeep Mathias from Nielsen for their help and assistance with the survey data.

The authors would also like to acknowledge the contribution of Internet Service Providers (Lightspeed, Zain, Mena and Batelco), Ministry Representatives (Education, Health and Social Development), The Sura Council, Bahrain Internet Society, Bahraini Society for Child Development NGOs, Child Protection Centre, all the schools that participated in the research and the invaluable support of the British Embassy in Bahrain. We would also like to thank Karen Moffat from the British School of Bahrain for her help.

***'Bahrain - which means "two seas" - was once viewed by the ancient Sumerians as an island paradise to which the wise and the brave were taken to enjoy eternal life'.***

[http://news.bbc.co.uk/1/hi/world/middle\\_east/country\\_profiles/790690.stm](http://news.bbc.co.uk/1/hi/world/middle_east/country_profiles/790690.stm)

## 2. Glossary of Terms:

ACLU American Civil Liberties Union

BIS Bahrain Internet Society

BSCD Bahraini Society for Child Development

BSB British School of Bahrain

CEOP Child Exploitation and Online Protection Centre

CHIS Children's Charities' Coalition on Internet Safety

CSP Communication Service Provider

COPINE Combatting Paedophile Information Networks in Europe

CPC Child Protection Committee

CRDS Centre de Recherche en Défense sociale (Belgium)

CRIOC Centre de Recherche et d'Information des Organisations de Consommation (Belgium)

EFC European Financial Coalition

EC SIP European Commission Safer Internet Programme

HTU Human Trafficking Unit

ICAC Internet Crime Against Children Task Force (USA)

ICANN The International Corporation for Assigned Names and Numbers

ITU International Telecommunications Union

IM Instant Messaging

INTECO National Institute of Communications Technology

IWF Internet Watch Foundation

INHOPE International Association of Internet Hotlines

MARC Multi-Agency Risk Conference structure

MOE Ministry of Education

MOH Ministry of Health

MOSD Ministry of Social Development

MOU Memorandum of Understanding

NCMEC National Centre for Missing and Exploited Children

NGO Non Governmental Organisation

PC Personal Computer

SCS Specialized Correctional Services

SIP EC's Safer Internet Action Plan and

SMC Salmaniya Medical Complex

SNS Social Networking Sites

TRA Telecommunication Regulatory Authority

TUK ThinkuKnow (CEOP intervention)

UOB University of Bahrain

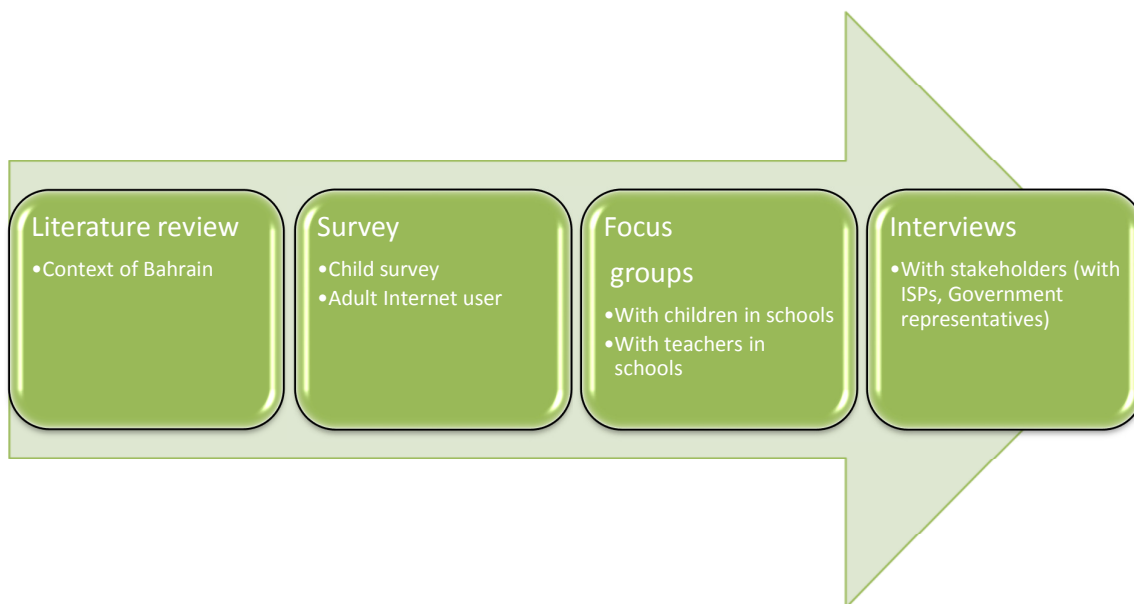
UKCCIS UK Council for Child Internet Safety  
VGT Virtual Global Taskforce

### 3. Executive Summary

The project was lead by Professor Julia Davidson, from Kingston University, London and Doctor Elena Martellozzo from Middlesex University. Qualitative focus groups in public sector schools were undertaken by the University of Bahrain and were managed by Dr Khalid Al-Mutawah.

To date there has been no comprehensive review conducted in the Kingdom of Bahrain to identify the risks to adult internet users and children of using the internet. The first State of the Nation Review provides a comprehensive analysis of Internet safety issues amongst adults and children, and sets out recommendations to ensure the safety of young people and adults navigating the information highway. The research aimed to explore adults and young people's (aged 7-18) experience and awareness of Internet use and Internet /other digital media safety. The research included an online survey with a representative sample of 2600 children stratified by age, gender, religion and school sector, an online survey of over 800 adults, focus groups with young people (n=130), interviews with teachers (n=30), and stakeholder interviews with representatives from the Bahraini Internet industry, Government Ministries (Social Development, Education and Health), NGOs, a University and charities (n=20). The research was undertaken between April and July 2010. The research process is summarised in figure 1.

**Figure 1**The research design and the research process



Careful consideration was given to all relevant ethical aspects of this research to ensure strict adherence to professional codes of conduct, primarily the British Society of

Criminology (BSC) Ethical Guide was used to inform ethical design and conduct throughout.

## **4. Key Findings and Recommendations:**

### **4.1 Summary of Key Findings:**

#### **4.1.1 Adult Survey Findings**

- Adults are experienced Internet users
- However, internet security awareness appears to be generally low. There appears to be a high level of trust which was evident from both the adult and the child data.
- Adults are frequently exposed to negative online experiences.
- Adults do not have a reliable source of information to consult regarding Internet advice.

#### **4.1.2 Child and Teacher Findings**

- Young people use the Internet an average of 2.5 – 3.5 hours every day. They use the Internet for a number of different reasons; mainly for homework purposes, to play games or to interact with other people.
- Young people connect via instant messaging, chat rooms, games, blogging and Social Networking Sites (SNS).
- Young people do not have a great understanding of what is meant by personal information.
- It appears that some children do not realise how public and accessible their information really is. A significant number of young people had their profile on SNS set to public and did not know how to set it to private.
- Generally older children in the 14-16 and 17-18 age groups took the most risks in terms of online safety; they were more likely to have shared personal information with a stranger and to have opened an email attachment from an unknown source than children in the 11-13 age group. This finding is consistent with data from a recent UK study (Davidson, Lorenz, and Martellozzo 2010) and from research conducted in Europe (Livingstone, 2009).
- A high number (43%, 1090) of young people had met with an online contact who they had not met in person before. This data indicates much higher proportions of children meeting with online contacts when compared to recent research undertaken in Europe.

- Young Muslims were more likely to meet an online stranger than any other religious group and children attending public schools were more likely to meet contacts than children attending private schools. Girls at public schools took more online risks than girls at private schools.
- The majority of the child respondents took positive action in responding to an unpleasant contact either by blocking them or by closing the window. However young people seemed reluctant to seek adult advice.
- Children seem to enjoy their online privacy and protect their anonymity. As a result, most do not share their online experience with adults.
- Most parents do not participate in online activities with their children.
- A large proportion of respondents were allowed unsupervised access to the internet and there was little significant variation by nationality, religion, age or gender.
- Cyberbullying was identified as a problem by young people and by teachers, particularly in private schools.
- Teachers suggested that cyber bullying or 'teacher humiliation' on SNS is becoming problematic particularly in the private school sector.
- Teachers often feel deskilled as many young people are more computer literate than they are.
- The majority of children had not received internet safety training at school, where they had received training it tended to be provided on an ad-hoc basis.

#### **4.1.3 Stakeholder Findings**

- There is currently no legislative framework that either seeks to protect children from Internet related or other forms of abuse, or that seeks to protect adults from cybercrime (other than basic e-transaction legislation passed in 2002).
- A legislative framework in the child protection area which includes online 'luring' (grooming) and indecent child image production and collection is proposed.
- Cybercrime legislation is also proposed.
- There is a strong opposition to blanket blocking of the Internet and attempts to further control Internet usage.
- Educational awareness training for parents and children was instead strongly advocated.
- There is an increasing trend of young female teenagers interacting with male peers online. Parental reaction is sometimes extreme and has resulted in a number (unspecified – but 7 confirmed cases in April 2010) of suicide attempts. The Bahrain Child Protection Centre has been working with the families.

- Although most of these interactions have occurred between young people, a minority have been perpetrated by adult males, although no meeting has taken place.
- There is currently no precedent for prosecuting cases of sexual abuse and physical abuse. There is no mandatory referral law in Bahrain, but there is a professional requirement for health professionals to refer abused children to the Child Protection Committee. However, there are currently no such requirements for other professionals, such as teachers or social workers, to report abuse. The proposed child protection legislation does however address this issue.
- There is a strong social class digital divide in the Kingdom. Poorer, less educated parents have lower computer literacy and understanding of Internet safety issues and stakeholders suggested that there may be a greater tendency to exert extreme physical punishment upon children. Stakeholders recommended that informal outreach work be undertaken with poorer communities to raise awareness.
- Stakeholders emphasised the importance of ensuring that the proposed child protection legislation be introduced and that steps be taken to ensure that the legislation is implemented, this includes training for the police and prosecutors for example.
- Stakeholders suggested that a national media campaign to raise awareness should accompany training programmes for children and parents.
- Stakeholders recommended that an e –safety Committee be set up to plan and implement the Kingdoms Internet safety strategy. The Committee should include a broad range of representatives from the government, NGOs, higher education, TRA, ISPs and community group.

## 4.2 Key Recommendations

It is recommended that:

1. A committee or working group should be established to set out and ensure implementation of the Kingdom's child e-safety strategy. The Bahrain Committee for Child Internet Safety (BCCIS)(or similar) should include representatives from: Government ministries; the legal profession; relevant NGOs; child welfare organisations; academia; ISPs; TRA and key community groups. The strategy should be informed by the findings from this research.
2. The proposed legislative child protection framework be introduced and implementation in respect of the online luring clause monitored by BCCIS;



3. Training for police officers and prosecutors should be introduced to ensure effective implementation of the new legislation;
4. The proposed cybercrime legislation should be implemented;
5. ISPs and TRA should play an active role in providing safety advice and technical advice on computer protection to adult Internet users via their websites and occasional public workshops.
6. A comprehensive Internet safety training programme be developed for both the private and public school sectors as part of the national curriculum (public school sector). The programme should draw upon good practice from programmes developed in other countries, but should take account of the cultural context in Bahrain. The training should include safety information along with guidance on ethical online behaviour. An evaluation component should be built into the programme from the outset to enable monitoring and good quality control ;
7. Young people should be consulted on the most appropriate and effective means of delivering the programme and on programme design;
8. Schools should introduce a designated e-safety staff function to ensure that programmes are delivered on a rolling basis in each school and that outreach safety advice work is undertaken with parents;
9. Schools and NGOs should play an active role in working with parents to raise awareness about Internet safety and about the nature of young people's online behaviour. Families in socially deprived areas might benefit from more informal advice offered by community groups and via Mosques. The digital divide between generations currently allows young people the freedom to navigate the information highway largely free from parental guidance and supervision, this is more marked amongst the lower social classes.
10. A far reaching media campaign should be organised by BCCIS using a wide range of media including: Newspapers; television and radio. Safety messages should be clear and simple and designed to appeal to different audiences.
11. The e-safety strategy should be developed and implemented in stages within a specified time frame. Progress against agreed objectives should be monitored and evaluated 1 full year following initial implementation to enable further development of the strategy.

## Contents

<b>1. ACKNOWLEDGEMENTS.....</b>	<b>2</b>
<b>2. GLOSSARY:.....</b>	<b>3</b>
<b>3. EXECUTIVE SUMMARY .....</b>	<b>5</b>
<b>4. KEY FINDINGS AND RECOMMENDATIONS: .....</b>	<b>6</b>
4.1 SUMMARY OF KEY FINDINGS: .....	6
4.1.1 Adult Survey Findings .....	6
4.1.2 Child and Teacher Findings.....	6
4.1.3 Stakeholder Findings .....	7
4.2 KEY RECOMMENDATIONS .....	8
<b>5. INTRODUCTION AND INTERNATIONAL CONTEXT.....</b>	<b>14</b>
5.1 THE BAHRAIN CONTEXT.....	14
5.2 THE EUROPEAN CONTEXT .....	18
5.3 ONLINE BEHAVIOUR .....	19
5.3.1 Adults and Children Online .....	19
5.3.2 Offenders Online .....	21
5.3.3 The relationship between online and offline offences.....	23
5.4 ONLINE CHILD SAFETY & RISK TAKING BEHAVIOUR.....	25
5.5 LEGISLATION & POLICY: HARMFUL CONTENT AND ONLINE GROOMING .....	28
5.5.1 The Scale of the Problem.....	28
5.5.2 European and International Legislation .....	30
5.5.3 Online Grooming .....	32
5.5.4 Indecent Child Images .....	35
5.6 BAHRAIN- POLICY AND LEGISLATION .....	37
5.6.1 Bahrain: Responsibility for Child Protection and Welfare .....	40
5.7 INTERNET SAFETY AND YOUNG PEOPLE: INTERNATIONAL APPROACHES AND INITIATIVES .....	42
5.7.1 Protecting children .....	42
5.7.2 Teaching Safety Online.....	44
5.8 LITERATURE REVIEW: SUMMARY OF KEY POINTS .....	50
<b>6. RESEARCH METHODOLOGY .....</b>	<b>52</b>
6.1 INTRODUCTION .....	52
6.1.1 Research Aims .....	52
6.2 PHASE ONE: ADULT SURVEY .....	53
6.3 PHASE TWO: SURVEY OF CHILDREN IN SCHOOLS.....	54
6.3.1 Limitations.....	55
6.4 PHASE THREE: FOCUS GROUPS WITH CHILDREN.....	56
6.5 PHASE FOUR: STAKEHOLDER INTERVIEWS .....	56
6.6 ACCESS: .....	58
6.7 ETHICS .....	58
6.8 INFORMED AND VOLUNTARY CONSENT.....	58
6.9 CONFIDENTIALITY AND ANONYMITY .....	59
6.10 DATA COLLECTION .....	59
<b>7. FINDINGS: ADULT SURVEY .....</b>	<b>60</b>
7.1 SAMPLE CHARACTERISTICS .....	60
7.2 ADULT SURVEY FINDINGS .....	62
7.2.1 How do people connect to the Internet?.....	62
7.2.2 Time spent online .....	63
7.2.3 Online activities.....	64
7.2.4 Use of social networking sites .....	64
7.2.5 Internet safety advice received .....	65
7.2.6 Source of advice: .....	66

7.2.7 Online experience .....	66
7.2.8 Risk taking behaviour and online negative experience .....	67
7.2.9 Personal information shared with people online .....	69
7.3 SUMMARY OF KEY FINDINGS .....	69
<b>8. FINDINGS: CHILD SURVEY AND FOCUS GROUPS.....</b>	<b>70</b>
8.1 ONLINE CHILD SURVEY SAMPLE .....	70
8.1.2 Sample Characteristics: Online Survey .....	71
8.2 FOCUS GROUP SAMPLE .....	72
8.2.1 Sample Characteristics: Child Focus Group Sample.....	72
8.3 CHILD SURVEY AND FOCUS GROUPS FINDINGS.....	74
8.3.1 Online Behaviour .....	74
8.4 ONLINE ACTIVITIES .....	78
8.4.1 Parental Supervision & Online Safety.....	81
8.5 BEHAVIOUR ON SOCIAL NETWORKING SITES AND POSTING PERSONAL INFORMATION.....	89
8.6 RISK TAKING AND UNPLEASANT ONLINE EXPERIENCE .....	94
8.7 ONLINE SAFETY TRAINING AND ADVICE .....	104
<b>9. TEACHERS INTERVIEW FINDINGS .....</b>	<b>112</b>
9.1 SAMPLE CHARACTERISTICS: FOCUS GROUP WITH TEACHERS .....	112
9.2 YOUNG PEOPLE'S AWARENESS OF INTERNET SAFETY AND ONLINE BEHAVIOUR.....	112
9.3 SAFETY TRAINING IN SCHOOLS .....	113
9.4 TRAINING FOR TEACHERS AND PARENTS .....	114
9.5 TEACHERS' RECOMMENDATIONS:.....	115
9.6 CHILD SURVEY: SUMMARY OF KEY FINDINGS .....	117
9.7 CHILD FOCUS GROUPS: SUMMARY OF KEY FINDINGS .....	119
9.8 TEACHERS FOCUS GROUPS: SUMMARY OF KEY FINDINGS.....	121
<b>10. FINDINGS: STAKEHOLDER INTERVIEW .....</b>	<b>122</b>
10.1 SAMPLE CHARACTERISTICS .....	122
10.2 NATURE AND ROLE OF THE ORGANISATIONS.....	122
10.2.1 Ministry of Education .....	122
10.2.2 Ministry of health .....	123
10.2.3 Ministry of Social Development.....	124
10.2.4 Shura Council.....	124
10.2.5 Bahrain University .....	124
10.2.6 Bahrain Internet Society (NGO).....	125
10.2.7 Bahraini Society for Child Development (NGO) .....	126
10.3 BACKGROUND AND LEGISLATIVE /POLICY OVERVIEW .....	126
10.3.1 Further Gaps in the Law .....	129
10.4 CURRENT APPROACH TO INTERNET SAFETY .....	130
10.5 THE CONTEXT OF INTERNET SAFETY .....	131
10.6 PROBLEMS FACED ONLINE .....	133
10.7 STAKEHOLDER RECOMMENDATIONS .....	135
10.8 SUMMARY OF KEY FINDINGS.....	137
<b>11. KEY FINDINGS &amp; RECOMMENDATIONS:.....</b>	<b>139</b>
11.1 THE BAHRAIN CONTEXT.....	139
11.2 SUMMARY OF KEY FINDINGS: ADULT SURVEY DATA.....	140
11.3 SUMMARY OF KEY FINDINGS: CHILD SURVEY AND FOCUS GROUPS .....	141
11.4 SUMMARY OF KEY FINDINGS: STAKEHOLDER INTERVIEWS .....	143
<b>12. RECOMMENDATIONS .....</b>	<b>145</b>
12.1 EDUCATION AND INFORMATION ABOUT INTERNET SAFETY .....	145
12.2 PARENTAL INVOLVEMENT .....	146
12.3 TECHNICAL SOLUTIONS.....	146
12.4 GOVERNMENT INVOLVEMENT.....	147

12.5 FURTHER RESEARCH .....	148
<b>13. KEY RECOMMENDATIONS .....</b>	<b>149</b>
<b>14. BIBLIOGRAPHY.....</b>	<b>151</b>
<b>15. APPENDIX ONE: ADULT SURVEY (IN ENGLISH) .....</b>	<b>154</b>
<b>16. APPENDIX 1: ADULT SURVEY (IN ARABIC) .....</b>	<b>158</b>
<b>17. APPENDIX 3: CHILDREN SURVEY (IN ENGLISH) .....</b>	<b>164</b>
<b>18. APPENDIX 4: CHILDREN SURVEY (IN ARABIC).....</b>	<b>168</b>
<b>19. APPENDIX 5: FOCUS GROUP INTERVIEW.....</b>	<b>177</b>
<b>20. APPENDIX 6: STAKEHOLDER INTERVIEWS .....</b>	<b>179</b>

## Table of Figures and Tables

FIGURE 1 THE RESEARCH DESIGN AND THE RESEARCH PROCESS .....	5
FIGURE 2: INTERNET GROWTH AND POPULATION STATISTICS IN BAHRAIN: .....	15
FIGURE 3 THE RESEARCH DESIGN AND THE RESEARCH PROCESS .....	52
FIGURE 4 SAMPLE NATIONALITY .....	62
FIGURE 5 HOW PEOPLE CONNECT TO THE INTERNET .....	63
FIGURE 6 TIME SPENT ONLINE .....	63
FIGURE 7 ONLINE ACTIVITIES.....	64
FIGURE 8 USE OF SOCIAL NETWORKING SITES .....	65
FIGURE 9 SOURCE OF ADVICE .....	66
FIGURE 10 ONLINE EXPERIENCE.....	66
FIGURE 11 RISK TAKEN .....	67
FIGURE 12 LEVEL OF SAFETY .....	68
FIGURE 13 FOCUS GROUP SAMPLE COMPOSITION: AGE AND GENDER.....	73
FIGURE 14 SCHOOLS PARTICIPATING IN THE FOCUS GROUPS .....	73
FIGURE 15 TIME SPENT ONLINE: PRIVATE SCHOOL SECTOR .....	75
FIGURE 16 TIME SPENT ONLINE: PUBLIC SCHOOL SECTOR (BOYS) .....	76
FIGURE 17 TIME SPENT ONLINE: PUBLIC SCHOOL SECTOR (GIRLS).....	77
FIGURE 18 INTERNET ACCESS.....	78
FIGURE 19 ONLINE ACTIVITIES (PRIVATE SCHOOL SECTOR).....	79
FIGURE 20 ONLINE ACTIVITIES PUBLIC SCHOOL SECTOR (BOYS) .....	80
FIGURE 21 ONLINE ACTIVITIES PUBLIC SCHOOL SECTOR (GIRLS) .....	80
FIGURE 22 ONLINE ACTIVITIES DISCUSSED WITH PARENTS: PRIVATE SECTOR .....	83
FIGURE 23 ONLINE ACTIVITIES DISCUSSED WITH PARENTS: PUBLIC SCHOOL SECTOR (BOYS) .....	83
FIGURE 24 ONLINE ACTIVITIES DISCUSSED WITH PARENTS: PUBLIC SCHOOL SECTOR (GIRLS) .....	83
FIGURE 25 DO PARENTS ASK WHAT CHILDREN DO ONLINE? PRIVATE SCHOOL SECTOR.....	85
FIGURE 26 DO PARENTS ASK WHAT CHILDREN DO ONLINE? PUBLIC SCHOOL SECTOR (BOYS) .....	85
FIGURE 27 DO PARENTS ASK WHAT CHILDREN DO ONLINE? PUBLIC SCHOOL SECTOR (GIRLS).....	86
FIGURE 28 LOCATION OF COMPUTER .....	87
FIGURE 29 KNOWLEDGE ABOUT ONLINE SAFETY: PUBLIC SCHOOL SECTOR (BOYS) .....	88
FIGURE 30 FRIENDS ON SOCIAL NETWORKING SITES: PRIVATE SCHOOL SECTOR.....	89
FIGURE 31 FRIENDS ON SOCIAL NETWORKING SITES.....	89
FIGURE 32 FRIENDS ON SOCIAL NETWORKING SITES: PUBLIC SCHOOL SECTOR (GIRLS) .....	90
FIGURE 33 POSTING PERSONAL INFORMATION PRIVATE SCHOOL SECTOR.....	91
FIGURE 34 POSTING PERSONAL INFORMATION: PUBLIC SCHOOL SECTOR (BOYS) .....	91
FIGURE 35 POSTING PERSONAL INFORMATION: PUBLIC SCHOOL SECTOR (GIRLS) .....	92
FIGURE 36 WHAT IS CONSIDERED TO BE 'PERSONAL INFORMATION'? (PRIVATE SCHOOL SECTOR) .....	93
FIGURE 37 WHAT IS CONSIDERED TO BE 'PERSONAL INFORMATION'? (PUBLIC SCHOOL SECTOR- GIRLS) .....	93
FIGURE 38 WHAT IS CONSIDERED TO BE 'PERSONAL INFORMATION'? (PUBLIC SCHOOL SECTOR-BOYS) .....	93
FIGURE 39 ONLINE STRANGERS ADDED TO SOCIAL NETWORKING SITES: PRIVATE SCHOOL SECTOR .....	95

FIGURE 40 ONLINE STRANGERS ADDED TO SOCIAL NETWORKING SITES: PUBLIC SCHOOL SECTOR (BOYS) .....	95
FIGURE 41 ONLINE STRANGERS ADDED TO SOCIAL NETWORKING SITES: PUBLIC SCHOOL SECTOR (GIRLS) .....	96
FIGURE 42 ONLINE EXPERIENCE .....	97
FIGURE 43 SOURCE OF UNPLEASANT ONLINE EXPERIENCE .....	100
FIGURE 44 PERSONAL INFORMATION SHARED WITH STRANGERS .....	101
FIGURE 45 MEETING ONLINE STRANGERS-PUBLIC SCHOOL SECTOR (BOYS) .....	102
FIGURE 46 MEETING ONLINE STRANGERS: PUBLIC SCHOOL SECTOR (GIRLS) .....	102
FIGURE 47 SOURCE OF ADVICE PRIVATE SECTOR SCHOOLS .....	105
FIGURE 48 SOURCE OF ADVICE PUBLIC SECTOR SCHOOLS (GIRLS) .....	105
FIGURE 49 SOURCE OF ADVICE: PUBLIC SECTOR SCHOOLS (GIRLS) .....	106
FIGURE 50 INTERNET SAFETY TRAINING RECEIVED AT SCHOOL BY AGE GROUP .....	107
FIGURE 51 PARENTAL KNOWLEDGE: PRIVATE SECTOR SCHOOLS .....	107
FIGURE 52 PARENTAL KNOWLEDGE: PUBLIC SECTOR SCHOOLS (BOYS AND GIRLS) .....	108
FIGURE 53 SOURCE OF INTERNET SAFETY ADVICE .....	109
FIGURE 54 IS SCHOOL SAFETY TRAINING NEEDED? PRIVATE SECTOR SCHOOLS .....	111
FIGURE 55 IS SCHOOL SAFETY TRAINING NEEDED? PUBLIC SECTOR SCHOOLS (BOYS) .....	111

TABLE 1 SCHOOLS PARTICIPATING TO THE SURVEY .....	54
TABLE 2 SAMPLE SIZE AND CONFIDENCE LEVEL .....	55
TABLE 3 AGE OF RESPONDENTS .....	61
TABLE 4 GENDER SAMPLE COMPOSITION .....	61
TABLE 5 SCHOOLS PARTICIPATING IN THE SURVEY .....	71
TABLE 6 AGE AND GENDER .....	72
TABLE 7 SCHOOL SECTOR AND RELIGION .....	72
TABLE 8 TIME SPENT ONLINE X SCHOOL SECTOR .....	74
TABLE 9 TIME SPENT ONLINE X NATIONALITY .....	75
TABLE 10 ONLINE ACTIVITIES X GENDER AND AGE .....	79
TABLE 11 ALLOWED UNSUPERVISED (BY AN ADULT) INTERNET ACCESS: GENDER .....	81
TABLE 12 PARENTAL KNOWLEDGE ABOUT CHILD'S ONLINE ACTIVITY X GENDER & AGE .....	82
TABLE 13 ONLINE RISK TAKING X AGE .....	98
TABLE 14 FEELING UNCOMFORTABLE ONLINE X GENDER .....	100
TABLE 15 NUMBER OF CHILDREN WHO HAVE MET ONLINE STRANGERS X GENDER AND AGE .....	103
TABLE 16 NUMBER OF CHILDREN WHO HAVE MET ONLINE STRANGERS X RELIGION .....	104
TABLE 17 SOURCE OF INTERNET SAFETY ADVICE .....	110

## **5. Introduction and International Context**

To date there has been no comprehensive review carried out in the Kingdom of Bahrain to identify the risks to adult internet users and children of using the internet and other technologies. Consequently there has been no concerted effort by any authority to establish a framework for internet safety. Such frameworks are developing in other countries supported by organisations such as the European Commission (Safer Internet Programme) in Europe. The first State of the Nation Review provides a comprehensive analysis of Internet safety issues amongst adults and children, and sets out recommendations to ensure the safety of young people and adults in the digital world. The research aimed to explore adults and young people's (aged 7-18) experience and awareness of Internet use and Internet /other digital media safety. The research included an online survey with a representative sample of 2600 children, an online survey of over 800 adults, focus groups with young people (n=150), and stakeholder interviews with representatives from the Bahraini Internet industry, Ministries (Social Development, Education and Health), NGOs and charities. The research was undertaken between April 2010 and July 2010.

The intention to conduct the review was first announced at a conference hosted by the Family Online Safety Institute (FOSI) and the Telecommunications Regulatory Authority (TRA) of Bahrain, who together hosted the Gulf's first Information Communication Technologies and Online Safety Conference in 2009. As child online safety is of paramount concern to communities throughout the world, the Bahrain TRA is taking the first steps to ensure such safety for its citizens and families in the region. Both the conference and the press conference held in Bahrain December 13 were extremely well attended and attracted a lot of attention from regional and international press.

### **5.1 The Bahrain Context**

Bahrain is the world's 110th largest economy by GDP and has a population of 727,785. Internet users as of June 2009 standing at 250,000, or 34.3% of the population (Family Online Safety Institute 2010). As shown in table 2, Internet use has grown considerably in the last decade. Information technology now forms a core part of the formal education system in many countries, ensuring that each new generation of Internet users is more adept than the last. Recent statistics from the International Telecommunications Union (ITU) suggest that there are currently approximately 403,000 Internet users (9/2009) in

the Kingdom of Bahrain representing 55% of the population. This represents an almost 50% increase in usage since 2000.

**Figure 2: Internet Growth and Population Statistics in Bahrain:**

YEAR	Users	Population	% Pop.	Usage Source
<b>2000</b>	40,000	699,400	5.7 %	ITU
<b>2003</b>	195,700	707,357	28.0 %	ITU
<b>2008</b>	250,000	718,306	34.8 %	ITU
<b>2009</b>	402,900	728,709	55.3 %	ITU

Source: <http://www.internetworldstats.com/me/bh.htm>

The Kingdom of Bahrain is a progressive Gulf state, with an increasingly liberalized telecommunications sector, well defined ICT and online safety strategy. As part of the Kingdom's wider VISION 2030 strategy, in early 2009 Microsoft and the Bahrain Internet Society developed a number of programs to improve the IT literacy of its citizens through its eGA National Portal<sup>1</sup>. An English-language version of the eGA National Portal is located at <http://www.bahrain.bh/wps/portal/>. Although there has been no research exploring Internet use amongst young people in Bahrain, one respondent stakeholder claimed that 146,000 young Bahrainis use the social networking site Facebook. The Kingdom has a Facebook site which currently has 11,766 fans<sup>2</sup>, so it is clear that social networking is an activity enjoyed by many Bahrainis. It is also clear that growth in ICT will play both an essential role in the economic development of Bahrain heading towards 2030, and in equipping young people with essential skills. Commenting at the Cisco Networkers Bahrain 2010 Business Conference Kamal Ahmed, Chief Operating Officer of the Bahrain Economic Development Board (EDB), commented: *"Bahrain has a growing young population eager to learn and exploit new technologies and provide us with the skilled ICT workforce of tomorrow. We also recognise our role to nurture and encourage additional export orientated industries to assure career opportunities for an increasingly well educated, flexible and skilled Bahraini workforce"* (ArabNetwork).

In 2008 the total number of mobile subscribers in Bahrain was 1,453,000 and in 2009 the total was 1,583,240, an increase of 9%. This figure includes both contract and pre-paid connections. Currently, the youth population (0 - 14 years) represents 25.9% of the population. In April 2010 the Telecommunications Regulatory Authority (TRA) of the Kingdom of Bahrain hosted one of the Gulf region's first online safety conference in Manama, in partnership with the Family Online Safety Institute (FOSI). Entitled, 'Building

<sup>1</sup> (<http://www.tra.org.bh/en/pdf/Vision2030Englishlowresolution.pdf>)

<sup>2</sup> (<http://www.facebook.com/pages/Bahrain/13313568716#!/pages/Bahrain/13313568716?v=wall>)

a National Consensus for Online Safety' it is part of its ongoing 'Bahrain Campaign for Online Safety'. A Memorandum of Understanding between Internet Service Providers was signed at the conference (see box 1):

**Box 1 Memorandum of Understanding**



**MEMORANDUM OF UNDERSTANDING BETWEEN  
INTERNET SERVICE PROVIDERS OF THE KINGDOM OF BAHRAIN  
ON ONLINE CHILD SAFETY**

The safety of children is a fundamental responsibility of any society.

As new technologies become increasingly important and more widely used by all members and segments of society, so too is the importance of adequately protecting children from threats that might emerge through the misuse of the internet.

We, the undersigned, commit to endeavor to implement the following strategies to promote the safety of children and young adults using the services of the Kingdom of Bahrain's internet service providers:

1. communicate with each other, with TRA and with all relevant government bodies when a party to this MOU detects a website or internet practice that poses a potential risk to the safety of children and young adults;
2. liaise and assist all relevant government bodies in the lawful investigation and prosecution of persons who commit crimes against children through use of the internet;
3. provide educational material of any relevant protection and control mechanisms for each subscriber (or end-user) on a regular basis to subscribers regarding child safety and the internet;
4. endeavor to suggest technical means to subscribers to enhance security on their access to their services, including but not limited to information about the tools available to them to control access and how to implement protective measures and with the best support possible;
5. coordinate with TRA (Consumer Affairs and ICT Operations) on internet risk found in the future;
6. work with TRA to develop and implement appropriate international best practices for online child safety;
7. to meet twice a year to discuss ongoing initiatives and shared best practices.

Notwithstanding the principles above as appropriate and necessary the signatories will, by general consensus, decide on the means by which that these will be implemented under this MOU.

Signed on 28<sup>th</sup> April 2010 in Manama, Kingdom of Bahrain.

## 5.2 The European Context

Recent comparative work (EUKids Online) on internet use across 27 European countries reveals that there have been substantial changes between 2005 and 2008. In 2005 70% of 6-17 year olds in the EU used the internet by 2008, this figure rose to 75%. The most striking rise has been amongst younger children: by 2008, 60% of 6-10 year olds were online. There has also been a substantial difference between 2005 and 2008 concerning location of use. In 2005 use of the internet at school was as common as home use. By 2008, 6-17 year olds in all EC countries were much more likely to use the internet at home (65%) than school (57%), and 34% are now going online using their own computer. (Livingstone and Haddon 2009). Research studies in the UK suggest that a majority of young people aged 9-19 access the Internet at least once a day. It provides the opportunity to interact with friends on social networking sites such as Facebook, Myspace and Bebo and enables young people to access information in a way that previous generations would not have thought possible. The medium also allows users to post detailed personal information, which may be accessed by any site visitor and provides a platform for peer communication previously unknown (Davidson and Martellozzo 2008a).

In a study of internet use among young people conducted in Belgium in 2008 by the *Centre de Recherche et d'Information des Organisations de Consommation* (CRIOC Belgian centre for consumer group information and research 2008), it emerged that 88% of the sample ( $N = 2336$ ) surfed the web regularly. The general average was 9.5 times a week. All the age groups surveyed engaged in surfing. Indeed, it was already customary practice for 72% of respondents aged 10 years of age. The pre-adolescents surveyed (11-12 years old) declared requiring no help to connect to and use the internet. Their favourite online activities were (a) viewing cartoons or music videos, (b) playing games, and (c) communicating via msn or email. Young adolescents (13-14 years old), too, required no help using the internet and their favourite activities included (a) creating and managing a personal blog to showcase themselves, (2) communicating, and (3) downloading music, games and videos. As for adolescents over 15 years old, they reported for the most part possessing their own personal computer and using the internet to (a) communicate with others, (b) comment on specific topics in discussion forums and (c) to download music, games and videos. It is clear that although the points of interest vary across age groups, "communicating" is nevertheless a constant. When asked what activity they most engaged in, "chatting" came out on top (82% of

respondents). Surprisingly, 74% of the children still in elementary school already chatted on a daily basis.

## **Summary Points: Children's use of the internet**

### **What do we know?**

- 1.Children spend more time online than their parents think.**
- 2. It is becoming more common for children to access the internet in their own bedrooms and on mobile phones without parental supervision**
- 3.There is a growth in using alternative portable devices (including mobiles and portable media players) to access online content in a variety of places and without parental supervision**
- 4.Most research evidence is from Europe and the US, this may not be as relevant in other contexts**

### **What do we not know?**

- 1.There is very little evidence on the links between using more portable devices and how this may increase online risks**
- 2. We do not know much about the extent to which children use such sites as 'Twitter' to share personal information**

## **5.3 Online Behaviour**

### **5.3.1 Adults and Children Online**

*'There are significant economic benefits to Government and businesses, as well as additional convenience for the public, from increasing the take-up of online services. However, the internet also provides more opportunities for criminals. It enables them to commit traditional crimes such as theft or fraud in new and more sophisticated ways, but also to commit new crimes such as the generation of malicious codes to attack the IT systems of citizens, businesses, and government. The internet also gives sexual predators a new means to access children and the impact of e-enabled harm on children is immeasurable' (National Audit Office 2010)*

Recent research and statistics demonstrate that in the past few years' home access to the Internet has rapidly grown in the Middle East, Europe and the United States, and school access has become widespread in many countries. As a result, adults and children spend more and more time online. In order to navigate the information highway safely people need good protective software on their PCs, but they, particularly children, also need to be educated in good practice to protect themselves from fraud, cyber bullying, exposure to harmful content and online abusers. The advent of wireless technology means that young people can access the Internet remotely almost anywhere and away from parental supervision.

Recent research conducted by the National Audit Office in the UK (2010) suggests that whilst adults are often aware of the threat posed by online fraud (personal identity and financial), the extent of their awareness was correlated strongly with their confidence in using the Internet. Those adults who described themselves as confident users were more likely to have taken steps to protect themselves against online fraud.

This TRA review represents the first attempt to explore the online experiences of adults and young people in Bahrain. Recent research conducted elsewhere has explored the risks faced by young people online. The EUKids Online research (opp cit) suggests that providing personal information is the most common risk- approximately half of online teenagers- seeing pornography the second most common risk. *'As regards meeting an online contact offline, this is the least common but arguably **the most dangerous risk**, showing consistency in the figures across Europe at around 9% (1 in 11) online teens going to such meetings'* (Hasebrink, Livingstone, Haddon, and Olafsson 2009).

There is a growth in using alternative devices to go online. Mobile phone use is widespread among children and young people and an increasing number access the internet via a mobile phone. They make extensive use of the Internet using interactive services such as games, Social Networking Sites and instant messages, increasingly to be found as mobile phone applications. Research, carried out by Ipsos Mori on behalf of Ofcom (2009 ) in the UK, comprised 797 face-to-face interviews with children aged 7-16 and their parent or carer. Just over 10% of children use their mobile phone to go online. When online they most frequently say they are downloading or playing music (80 %), visiting social networks (45 %) and instant messaging (38 %). In the UK 19% of parents said their child uses a games console to go online (Ipsos Mori, 2009). Another recent UK survey of schoolchildren examined the difference in use of the technology between girls and boys. It revealed that girls are more likely than boys to use mobile phones and digital cameras, with boys more likely than girls to play computer and console games (Eynon 2009).

And this pattern is not only evident in Europe. In Russia (2009, Foundation for Internet Development) recent research in large urban centres on children and teenagers' attitudes and perceptions of the Internet reveals that it is the primary information source ahead of television, books and printed mass media for both 14-15 yr olds and 16-17 yr olds. Approximately 65% of 16-17 year olds said that parents allow them free use of the internet and do so without imposing any time-limit. In terms of perceived risks and dangers it is clear that 16-17 year olds are currently more aware of pornography (80%)

than the 14-15 yr olds (45%) although as many of the older group placed viruses as an equal risk to pornography.

Research suggests that the most common risks facing young people in Europe appear to be providing personal information and accessing pornography and violent or hateful content (Hasebrink, Livingstone, Haddon, and Olafsson 2009). The internet has however facilitated bullying behaviour. Research suggests that cyberbullying often takes place via instant messaging or social networking sites – 18.9 per cent of girls reported typing hurtful things on MSN that they would not say face-to-face (CEOP, 2008). Another example is 'sexting', in which children produce and circulate sexual content with each other. Around a third of 11-16 year olds have received an unwanted or "nasty" message and a quarter has received an unwanted or "nasty" image of a sexual nature (Cross 2009). The Authors recent research conducted in the UK suggests that 1 in 5 children aged 11-17 had experienced cyberbullying (Davidson, Lorenz, and Martellozzo 2010).

A UK based Charity addressing bullying defines cyberbullying as follows:

- Sending nasty or threatening texts or emails
- Posting abusive messages online - on a social networking site, in a chatroom, or using IM
- Posting humiliating videos or pictures online, or sending them on to other people
- Taking on someone else's identity online in order to upset them
- Bad mouthing and spreading rumours
- Setting up a hate site or a hate group on a SNS site
- Prank calling, prank texts and messages

(Source: Beatbullying <http://www.beatbullying.org/abw/cyberbullying.html>)

### **5.3.2 Offenders Online**

There is increasing evidence that the Internet is used by some adults to access children and young people for the purposes of sexual abuse. According to Davidson and Martellozzo (2008a), Internet sex offender behaviour includes the construction of sites to be used for the exchange of information, experiences, and indecent images of children; the organization of criminal activities that seek to use children for prostitution purposes and that produce indecent images of children at a professional level and the organization

of criminal activities that promote sexual tourism. The definition of an online groomer (referred to as '*luring*' in some jurisdictions) is someone who has initiated online contact with a child with the intention of establishing a sexual relationship involving cyber-sex or sex with physical contact. Child grooming is a process that commences with sex offenders choosing a target area that is likely to attract children. In the physical world, this could be venues visited by children such as schools, shopping malls or playgrounds. The grooming process commences when offenders take a particular interest in the child and make them feel special with the intention of forming a bond as a precursor of abuse. The Internet has greatly facilitated this process in the virtual world in terms of geographic location, speed of contact and range of number of contacts.

Groomers will often offer incentives such as money, gifts, concert tickets, modelling contracts, day trips, phones and games as part of the grooming process or to encourage young people to produce and send images of themselves (Taylor, 2010). Internet sexual offenders are defined as falling into two principal categories, which are not mutually exclusive: Those who use the Internet to target and 'groom' children for the purposes of sexual abuse (Finkelhor, Kimberly, and Wolak 2000); and those who produce and/or download indecent illegal images of children from the Internet and distribute them (Davidson and Martellozzo 2005; Quayle and Taylor 2002).

Recent advances in computer technology have been aiding sex offenders, stalkers, child pornographers, child traffickers, and others with the intent of exploiting children. While such offences occurred prior to the Internet, the advent of the new technology two decades ago has allowed for easier and faster distribution of pornographic materials and communication across national and international boundaries (Kierkegaard 2008). The dynamics of this opportunism is the subject of ongoing discussion. In his research with a sample of 300 child pornography offenders Hernandez comments that it is through the exploration of sexual themes and seeking out adult pornography on the internet that offenders previous deviant sexual interests are re-awakened (Hernandez April 5-7, 2009).

The internet provides the opportunity to join a virtual community where people with similar interests can communicate and find useful information. 'Myspace' and other similar social networking sites encompass thriving 'communities' where young people engage in countless hours of photo-sharing. In addition to Myspace, other social networking and blogging sites such as Friendster.com, Facebook.com and MyYearbook.com allow users to post pictures, videos and blogs and send emails and instant messaging. Myspace and Facebook differ in security aspects in that Myspace is open to anyone, and has loose age restrictions, while Facebook users are encouraged and often required to register using their real name (Kierkegaard 2008). The anonymity,

availability of extremely sensitive personal information and ease of contacting people, make social networking sites a useful tool for online child sex offenders in general, but specifically for online groomers. Usage by young people develops, whereby if young people want to get to know each other better, then they may move into more private tools such as MSN, which intensifies the communication, and if the relationship is developed further, then the private arena of web cameras are utilised. While many of these sites have age restrictions, it is possible for offenders to misrepresent their age. Also, in order to hide their IP addresses and locations, they can piggyback on Wi-Fi connections or use proxy servers. Decentralized peer-to-peer networks prevent material from being tracked to a specific server, and encryption enables privacy and evasion from those policing the Web.

Therefore, technologies around social networking sites allow relatively easy access to children by online groomers, with children having frequent and open access to such sites at younger ages. Once in contact with a child, the online groomer can use incentives to encourage the child's participation, towards the goal of sexual contact. Recent research conducted by Webster, Davidson, Bifulco, Caretti & Pham (2009) with online groomers in four European countries suggests that the grooming approach can be prolonged spanning months, or can be swift. An analysis of offender chat logs suggests that conversations with young people can become immediately sexualised and that offenders have many young people on their friends list, which they will work through in order to find a child who is willing to meet with them.

### ***5.3.3 The relationship between online and offline offences***

"The 'Butner Redux' Study" (Bourke and Hernandez 2009) of child pornography offenders revealed that many who had no known history of contact sexual offences subsequently admitted to such crimes after participating in treatment. Whilst this is also true for some other crimes, the critical issue is what impact such information about self-reported crimes has in the realm of risk assessment and intervention. A number of other studies have reported a co-occurrence of contact sexual offences among child pornography offenders entering the criminal justice system or in clinical settings (Hernandez April 5-7, 2009; Wolak, D., and Mitchell 2005). A sub-analysis conducted in the Butner Redux Study explored the age of onset for online and offline (contact) sexual crimes on a subset of 42 of the total 155 investigated. The rationale for this was to shed light onto the developmental pathway of child pornography offences. Although caution is needed in generalising the findings given the small sample size, the majority reported

that they committed acts of hands-on abuse **prior** to seeking child pornography via the Internet (emphasis added).

However research comparing risk factors among contact sex offenders and child pornography offenders, indicate lower rates of risk variables for contact sexual offending than already identified sex offenders. Elliott, Beech, Mandeville-Norden, and Hayes (2008) examined psychological risk of reoffending in 505 child pornography offenders and 526 contact sex offenders. It was found that whilst there were many similarities on some psychological risk variables such as impulsivity, contact sex offenders had lower victim empathy and higher offence-supportive attitudes and beliefs.

#### **Summary Points: Online behaviour: Key research findings**

- **Adults users lacking confidence in computer literacy are particularly susceptible to cyberfraud and identity theft**
- **The most common risks facing young people appear to be giving out personal information, accessing pornography and violent or hateful content**
- **Research suggests that cyberbullying often takes place via instant messaging or social networking sites –UK research suggests that around one in five 11-17 year olds and 12-17 year olds have been cyberbullied in the last year**
- **Offenders use social networking sites to groom young people for the purposes of sexual abuse**

#### **Summary Points: Research gaps**

- **More evidence is needed to quantify the extent to which children encounter online risks, rather than just focusing on young people's and adults' perceptions of such risks**
- **There is very little evidence on the role of the internet in reinforcing negative behaviours or attitudes such as suicide, race-hate, or anorexia**
- **There is little research addressing the risks faced by adult users online**
- **There is little current research evidence exploring the link between online and contact child abuse**



## 5.4 Online Child Safety & Risk Taking Behaviour

The advantages of the Internet greatly outweigh the disadvantages, but young people can be exposed to cyber bullying, harmful content and online grooming. Research undertaken in Europe and the United States has also demonstrated that young people do engage in risk taking behaviour online.

A national random sample of young Internet users in the United States (ages 10-17) found 13 % had experienced an unwanted sexual solicitation on the Internet (Mitchell, Finkelhor, and Wolak 2005). Many of these incidents were confined to the Internet and relatively mild in nature. However, the potential for online sexual solicitation and harassment has raised obvious concerns among parents, teachers, and mental health professionals. What risks are children taking when using the internet?

Recent research led by Livingstone (2009) and funded by the European Commission Safer Internet Programme (EC SIP) suggests a rank for young people's online risk taking behaviour. The work draws upon findings from research studies exploring young people's Internet behaviour across Europe and includes the views of thousands of young people across Europe.

The ranking of risk incidence is as follows:

### Ranking of risk incidence

- 1. Providing personal information to strangers (50%)**
- 2. Seeing adult pornography online (40%)**
- 3. Seeing violent or hateful content (30%)**
- 4. Meeting an online contact (10%)**

### Livingstone (2009)

In the UK Ofcom's recent research exploring young people's (aged 16-24) online behaviour suggests that the younger age range (16-19) were much less aware of potential risks in accessing and entering personal information to websites than were the older age range in the sample:

*'Young adults are less likely to make any kind of judgment about a website before entering personal details, less likely to have any concerns about entering personal details online-within the young adult population, it is the attitudes and behaviours of the*

*youngest adults- those aged 16-19- which are the most striking. These adults are the most likely to share information and download content from the Internet, at the same time as being less likely to make any checks or judgments, and more likely to believe that the Internet is regulated'* (Ofcom 2009 ).

This suggests that older children are more likely to engage in risk taking behaviour online and appear less likely to act on advice regarding Internet safety. In 2008 school sample surveys revealed quite a high degree of awareness of the existence of risks and dangers on the internet, although this was not always matched by accurate understanding. Primary-age respondents communicated anxiety about encountering unexpected dangers such as viruses or frightening material. *"The older learners were mostly able to talk quite knowledgeably about how to protect their own safety and identity online, but were less convincing as to whether they manage to act in such sensible ways when online"* (Davies et al 2008).

This finding is supported by research undertaken in the UK by Davidson, Lorenz, Grove-Hills and Martellozzo (2009) on behalf of the National Audit Office. The research included an online survey of 11-16 year olds (n= 1808) and focus groups (n=83) of young people. A substantial proportion of children reported having engaged in high risk behaviour online (defined by degree to which they share information with strangers), 37% had shared an email address; 34% provided information about the school they attended; 23% provided a mobile number; 26% a personal photograph. A significant proportion said they will continue with such behaviour following Internet safety training (particularly 13+), with 36% saying that Internet safety training would make them more careful online. Focus group findings indicated that interacting with strangers (i.e. adding them as ISM or Facebook friends and exchanging messages) is becoming an accepted behaviour not perceived as 'risk-taking'.

Recent research undertaken in Russia (2009) on risk-taking behaviour revealed that more than 50% of young people surveyed gave out personal data without thinking. The difference between the two age groups in terms of the type of personal data was that a larger proportion of 16-17 year olds (23%) appeared to be providing both personal photos and photos of relatives as compared with 11% of 14-15 year olds doing so (Foundation for International Development Research 2009).

Research conducted in Belgium (CRIOC Belgian centre for consumer group information and research 2008) with a large sample of over 2000 young people found that on average, 40% of the sample declared chatting only with people they knew. This means

that 60% were regularly in contact with potentially dangerous strangers, all the more so for younger internet users. On the issue of parental control, only 35% reported using the internet according to the rules laid down by their parents. The researchers concluded that existing laws were inadequate as internet use was not risk-free. There were shortcomings at various levels, particularly in respect of commercial manipulation (e.g., advertising, spam), the exchange of pirated data, the respect of privacy, the dissemination of offensive information and images, and the protection of children. The findings also suggest that one out of four boys and one out of five girls reported having already engaged in cybersex. One-third of the boys and one-eighth of the girls declared having had offline sexual relations with a person they met online. Moreover, 75% of the girls and 80% of the boys admitted to flirting and talking about sex online. Existing in a 'virtual' world may act to break down inhibitions. Indeed, findings suggest that it is not uncommon for girls to pose as older than they actually. The use of a fake identity was also common practice.

Ongoing research funded by the European Commission Safer Internet Programme (Webster & Davidson et al. 2009) exploring online grooming behaviour in 4 European countries suggests that offenders may target socially isolated, vulnerable young people who respond well to attention received from online contacts.

Parents should provide the first line of defence against the dangers related to surfing on the web. Some studies have shown that young people whose parents are involved in and chaperon internet use take fewer risks when surfing. Chat rooms and other forums do sometimes have a code of conduct, filters and moderating systems to regulate offensive content. The code of conduct is a sort of charter that all internet users who frequent a chat room or forum are expected to be familiar with and respect. Otherwise, users can be reprimanded and even excluded temporarily or definitively. The code of conduct generally prohibits discriminatory, racist, hurtful, commercial statements as well as those of a pornographic nature. Filters and moderators ensure compliance with the code of conduct. Text filters automatically block or delete all messages containing obscene terms previously entered in the database. As for the moderator, this is a person who supervises online activities and decides whether or not to censor content deemed inappropriate. However, it should be noted that moderation is not subject to any specific law or regulation. Furthermore, anyone can set up a chat room and supervision is not a legal obligation. Should the moderator or the filters prove ineffective, there are contact points where internet users can report abuse they observe when visiting chat rooms. Generally, moderators will verify e-mail address.

## **Summary Points: Safeguarding Children's Online Experiences**

### **What do we know?**

- **A minority of parents use internet controls or filtering software**
- **Parents are even less aware of safeguarding controls for mobile phones and games consoles**
- **While children are generally aware of how they should behave to stay safe online, they often do not use these strategies. This is particularly true of teenagers.**
- **Young people take fewer online risks when parents are involved in their Internet activities.**

### **Research Gaps?**

- **More research is needed to explore what specific strategies work best in ensuring that young people use the internet safely**
- **There is limited evidence on teachers' awareness and understanding of effective ways of safeguarding from online risks and how to teach children about it.**
- **There is limited research on teenager's use of the Internet and perceptions of risk taking behaviour.**
- **More work should be done to explore what Internet safety approaches work best with different age groups in different cultural and national contexts**

***Source: Adapted from UKCCIS Evaluation, 2010***

## **5.5 Legislation & Policy: Harmful Content and Online Grooming**

### ***5.5.1 The Scale of the Problem***

While the expansion of the Internet and the proliferation of information technology have created new opportunities for those who engage in illegal activities (Quayle and Taylor 2003), the area of digital forensics has grown rapidly as well (Ferraro and Casey 2005). This has helped in the discovery of new forms of criminal activity. As already known sex offenders use the Internet to access indecent images of children, to select victims for abuse and to communicate with other sex offenders. This activity has expanded so much that law enforcement agencies have difficulty, tracking down child victims and

perpetrators involved unless they have the capability of professional digital forensics and intelligence. Successful cyber crime intelligence requires computer skills and modern systems in policing. Digital forensics is the art and science of applying computer science to aid the legal process. It is more than the technological, systematic inspection of electronic systems and their contents for evidence or supportive evidence of a criminal act. Digital forensics requires specialized expertise and tools when applied to intelligence in important areas such as online victimization of children (Davidson and Gottshcalc 2010).

In the UK the National Society for the Prevention of Cruelty to Children have estimated that approximately 20,000 indecent images of children are placed on the Internet each week (NSPCC 2007). The Internet Watch Foundation (IWF) is the IT industry watchdog in the UK. The IWF reported a rise in the number of websites containing indecent images of children from 3,438 in 2004 to 6,000 in 2006. The IWF claimed that over 90 per cent of the websites are hosted outside the UK (many are hosted in the US and Russia), and are therefore extremely difficult to police and control and there is currently no international agreement on regulation of the internet in respect of online grooming and indecent child images<sup>3</sup> The IWF 2008 Annual Report suggest a 10% reduction in websites hosting indecent child images, however the report suggests 'a continuing trend in the severity and commercialisation of the images:

- **58% of child sexual abuse domains traced contain graphic images involving penetration or torture (47% of domains in 2007)**
- **69% of the children appear to be 10 years old or younger; 24% 6 or under, and 4% 2 or under (80% appeared to be 10 or under in 2007)**
- **74% of child sexual abuse domains traced are commercial operations, selling images (80% commercial in 2007)**
- **It is still rare to trace child sexual abuse content to hosts in the UK (under 1%)'**

#### **(IWF 2009)**

There is no doubt that such abuse has a damaging and negative impact upon child victims. It has been claimed that in many instances children are abused and the abuse recorded by members of their own family or people known to them (Klaine, Davis, and Hicks 2001). Many indecent images depict the sexual abuse of children who are victimized both in the creation of the image and in the distribution of the image. It could

---

<sup>3</sup> A breakdown of countries where websites containing child abuse images appear to have been hosted during the period 1996–2006 is provided by the IWF: US 51%; Russia 20%; Japan 5%; Spain 7% and the UK 1.6% (IWF, 2006).

be argued that a child is re-victimised each time their image is accessed, and images on the Internet can form a permanent record of abuse.

In terms of contact sexual abuse, not necessarily related to initial internet contact, the UK children's charity Childline report that of the 13,237 children counselled for sexual abuse in 2007/2008, 8457 were girls (64 percent) but 4780 were boys (36 percent) (NSPCC Press Release, Feb 2009). Boys are no less susceptible to risk of abuse than girls. There is evidence to suggest that this sort of finding is similar in terms of risk of abuse through the internet. An evaluation of a safety internet awareness training initiative in schools revealed that girls appear to be at higher risk than boys because they use social aspects of the internet more (notably instant messaging and social networking sites), and are slightly more willing to share some types of personal information with and to interact with strangers. Girls are far more likely to have had a 'threatening' experience online. However, boys are twice as likely to do nothing in reaction to a 'threatening' experience (Davidson, Lorenz, and Martellozzo 2010).

### ***5.5.2 European and International Legislation***

The 2001 Council of Europe Convention on Cybercrime which was one of the first attempts to harmonise national and international definitions of 'child pornography', and has a specific provision criminalising it (Article 9). Carr and Hilton (2010) suggest that 'the Convention is useful insofar as it contains important procedural and international co-operation measures in dealing with this offence as well as other criminal offences committed by means of a computer. However, this Convention contains a number of optional aspects – for example in relation to age which render it problematic'(p23). The more recent 2007 Council of Europe Convention on the Protection of Children Against Sexual Exploitation and Sexual Abuse goes much further and gives a clearer definition of age as well as strengthening a number of provisions in relation to online abuse and exploitation.

The Committee of Ministers of the Council of Europe formulated Recommendation CM/Rec (2009)5 on "measures to protect children against harmful content and behaviour (and to promote their active participation in the new information and communications environment)<sup>4</sup>". Carr and Hilton (2010) suggest that although this lacks legal teeth it provides another indication of a growing momentum at political level within the international community to mobilise against online child abuse images.

---

<sup>4</sup> <https://wcd.coe.int/ViewDoc.jsp?id=1470045&Site=CM>

Other key international activity in this area includes World Congresses on the Sexual Exploitation of children. Most recently, at the 3<sup>rd</sup> World Congress the 'Call for Action' gave specific attention to the issue of sexual exploitation via the use of the internet, mobiles and other new technology, including calling for the criminalisation of all aspects of 'child pornography' including virtual images as well as the call for ISPs and mobiles to develop codes of conduct in relation to child protection<sup>5</sup>. These high profile international meetings have also resulted in stated commitments to criminalise forms of sexual exploitation and provide access to protection for victims as well as standards for child friendly judicial procedures, a strengthening of victims' rights to legal aid and the development and implementation of national plans of action and focal points to tackle sexual exploitation (Carr and Hilton, 2010).

The Child Online Protection (COP) initiative, started in 2008 by the International Telecommunications Union, represents the first major attempt by a well-established intergovernmental global body to focus on a range of online child protection issues, of which child abuse images is a key part<sup>6</sup>. The ITU has no formal powers in these areas but it is an important part of the United Nations group of organizations, connecting directly with 191 Member States. There is a need for more collaborative international work as initiatives have developed in a piecemeal fashion and impact is therefore limited.

The European Union has introduced a Framework Decision in this area and suggests that: *'to combat child pornography, especially where the original materials are not located within the EU, mechanisms should be put in place to block access from the Union's territory to internet pages identified as containing or disseminating child pornography'* (p5, 2009). A recently published EU (2009) document entitled *'Combating the Sexual Abuse, Sexual Exploitation of Children and Child Pornography'* sets out the shortcomings and vision in protecting young people from sexual abuse. The framework decision outlines the difficulty in protecting young people when there is such widespread variation in national criminal law and law enforcement practice in Europe. The situation is seen as exacerbated by the hidden nature of the offending and compounding issues such as victims' reluctance to report abuse.

The role of information technology in facilitating global abuse and sex offender networks is discussed. The EU suggest that *'developments in information technology have made*

---

<sup>5</sup> [http://ecpat.net/Ei/Updates/WCIII\\_Outcome\\_Document\\_Final.pdf](http://ecpat.net/Ei/Updates/WCIII_Outcome_Document_Final.pdf)

<sup>6</sup> <http://www.itu.int/osg/csd/cybersecurity/gca/cop/index.html> .The objectives of COP are to: • Identify risks and vulnerabilities to children in cyberspace; • Create awareness• Develop practical tools to help minimize risk • Share knowledge and experience.

*these problems more acute by making it easier to produce and distribute child sexual abuse images while offering offenders anonymity and spreading responsibility across jurisdictions. Ease of travel and income differences fuel so-called child sex tourism, resulting often in child sex offenders committing offences abroad with impunity. Beyond difficulties of prosecution, organised crime can make considerable profits with little risk'* (p2).

UK and other national laws provide a distinction between the regulation of adult material and that depicting children in recognition of the vulnerability of minors. However the task of legally defining when childhood ends is complicated and varies across jurisdictions. The *UN Convention on the Rights of the Child* defines a child as a person under the age of 18<sup>7</sup> but given wide variation in the age of consent to sexual relations across countries there is clearly legal disagreement regarding the age at which childhood ends, there is no consensus in international law regarding the age of consent. The *Optional Protocol to the UNCRC on the sale of children, child prostitution and child pornography* does not state what age a child is but as a protocol to the UNCRC itself it would mean 18. The *EU Framework Decision* states that a child is someone under the age of 18. The Council of Europe Convention on Cybercrime also states that a child is someone under the age of 18 but that a State has the right to lower this to 16: *'The age of 18 is an agreed international definition of the age of majority and so there is logic in using this already-agreed age. The difficulty this brings is where this is higher than the age of consent and so it appears to create something of a paradox'* (Gillespie 2009).

### **5.5.3 Online Grooming**

Recent international legislation has sought to protect young people from internet abuse through the introduction of a 'grooming' clause. This new offence category was introduced in the Sexual Offences Act (2003) in England and Wales (this section of the Act also applies to Northern Ireland<sup>8</sup>). Section 15 makes 'meeting a child following sexual grooming' an offence; this applies to the internet, to other technologies such as mobile phones and to the 'real world'. European Union Framework Article 5 refers to online grooming as the '*solicitation of children for sexual purposes*' (p5) and asks that each member state ensure that such conduct is punishable in law. This refers to cases involving children under the age of consent under national law (which varies

---

<sup>7</sup> Article 1

<sup>8</sup> The Sexual Offences Act 2003 (England and Wales) is currently under review in Northern Ireland. Some concerns have been raised regarding a lack of clarity around the age of consent and informed consent. Currently the age of consent is 17 in Northern Ireland (it was raised from 16 to 17 under the Children and Young Persons Act 1950) (Northern Ireland Office, 2006).



considerably across Europe), where an adult arranges to meet for the purposes of sexual abuse via the means of 'an information system' (p5).

'Grooming' involves a process of socialisation through which an offender seeks to interact with a child under the age of 16, possibly sharing their hobbies and interests in an attempt to gain trust in order to prepare them for sexual abuse. The concept of 'grooming' is now also recognised in legislation in the UK. The Sexual Offences Act (2003) in England and Wales, and Northern Ireland and the Protection of Children and Prevention of Sexual Offences Act (2005) in Scotland includes the offence of 'meeting a child following certain preliminary contact' (section 1). 'Preliminary contact' refers to occasions where a person arranges to meet a child who is under 16, having communicated with them on at least one previous occasion (in person, via the internet or via other technologies), with the intention of performing sexual activity on the child. The definition of 'grooming' in UK legislation is provided by the Crown Prosecution Service (CPS) (England and Wales):

*'The offence only applies to adults; there must be communication (a meeting or any other form of communication) on at least two previous occasions; it is not necessary for the communications to be of a sexual nature; the communication can take place anywhere in the world; the offender must either meet the child or travel to the pre-arranged meeting; the meeting or at least part of the journey must take place within the jurisdiction; the person must have an intention to commit any offence within or outside of the UK (which would be an offence in the jurisdiction) under Part 1 of the 2003 Act. This may be evident from the previous communications or other circumstances e.g. an offender travels in possession of ropes, condoms or lubricants etc; the child is under 16 and the adult does not reasonably believe that the child is over 16. (Crown Prosecution Service , 2007).'*

Several countries are beginning to follow the UK in legislating against 'grooming' behaviour. Sexual grooming has also recently been added to the Crimes Amendment Act (2005) in New Zealand. In the US it is an offence to transmit information electronically about a child aged 16 or under, for the purpose of committing a sexual offence<sup>9</sup>. The Australian Criminal Code<sup>10</sup> makes similar restrictions, as does the Canadian Criminal Code.<sup>11</sup> The legislation in the UK differs in that the sexual grooming offence applies both to the new technologies including the Internet and mobile phones, and also to the 'real world'; legislation in other countries addresses only electronic grooming via the internet

---

<sup>9</sup> US Code Title 18, Part 1, Chapter 117, AS 2425.

<sup>10</sup> Australian Criminal Code, s 218A.

<sup>11</sup> Canadian Criminal Code, s 172.1.

and mobile phones. The concept of sexual grooming is well documented in the sex offender literature (Finkelhor 1984), and is now filtering into legislation policy, crime detection and prevention initiatives. A recent report in the Guardian Newspaper suggested that the Child Exploitation and Online Protection Centre in the UK receive an average of 4 phone calls per day from young people planning to meet people with whom they have developed an online, sexual relationship (25/02/2009).

Norway is the only other European country to adopt the grooming legislation. The relevant sections in the General Civil Penal Code ("straffeloven") concerned with sexual offenders in Norway are: (Nicolaisen, 2008): Section 195. Any person who engages in sexual activity with a child who is under 14 years of age shall be liable to imprisonment for a term not exceeding 10 years. If the said activity was sexual intercourse the penalty shall be imprisonment for not less than 2 years, and Section 196. Any person who engages in sexual activity with a child who is under 16 years of age shall be liable to imprisonment for a term not exceeding 5 years. Section 201a is the new grooming section in Norwegian criminal law. This section was included in The General Civil Penal Code in April 2007: *With fines or imprisonment of not more than 1 year is any person liable, who has agreed a meeting with a child who is under 16 years of age, and who with intention of committing an act as mentioned in sections 195, 196 or 200 second section has arrived at the meeting place or a place where the meeting place can be observed.*

In Norwegian law the grooming section refers to *the intention of committing an act* . However, the perpetrator must actually appear for a meeting (sometimes a police trap), an intention to meet is not enough, it is possible that it should be but it is difficult to prove beyond doubt. The legislation is phrased as follows: *"...has arrived at the meeting place or a place where the meeting place can be observed". It is the potential scene of the crime, which is the meeting place where the offence is intended to take place, that the offender has arrived at, or the offender can observe the potential crime scene from where he is located'.*

The crime description is such that it is technology neutral. It is therefore not important how the adult and the child came in contact or agreed to meet. The important issue is that there is an agreement to meet physically. Agreement is to be understood in a wide sense. There is no requirement that there is an explicit agreement to meet. It is sufficient that the offender had a reasonable expectation to meet the child at a specific location within a specific time frame.

The grooming section was introduced in an attempt to protect children at an earlier stage. However, the contact itself is not a crime. There may be good reasons for adults and children to have contact using media such as the Internet. Adult and child may share the same interest in sports or games, and exchange experience and play games on the net. An appointment is defined as place and time where adult and child have agreed to meet. It may be at the adult's location, the child's location or another location to which both have to travel.

#### **5.5.4 Indecent Child Images**

*'Child abuse images are visual representations of a child being sexually abused.*

*The abuse usually takes place in the offline world, although some forms of sexual abuse which involve the capture of images can take place remotely e.g. through the use of web cams. The internet facilitates the mass distribution of the images, often for profit \* add footnote or sentence re informal (non pay per view) networks. This, in turn, creates an incentive for abusers to harm yet more children in order to create new images for sale'*

(Carr and Hilton 2010:1)

Ninety-four of 188 INTERPOL member countries have introduced legislation addressing the creation of pornographic child images. Fifty eight of the ninety four countries have criminalized the possession of child indecent images. Both distribution and possession are now criminal offences in almost all Western countries (<http://www.interpol.int/public/icpo/default.as>).

The scale of the problem is considerable. Many of the child victims appearing in images are amongst the most vulnerable, from poor countries and are repeat victims. The growth in arrests in the UK reflects the increase in the number of images: *'The growth in arrests and prosecutions for offences related to child abuse images in England and Wales has followed a similar trajectory. In 1999 403 persons were cautioned or proceeded against for offences related to child abuse images. In 2007 it was 1,402<sup>12</sup>. In 1996 the Internet Watch Foundation (IWF) processed 615 complaints relating to online abuse images compared with 34,871 in 2007 (IWF 2007)<sup>13</sup>* (Carr and Hilton 2010:2), the UK Internet Watch Foundation has however reported a 10% decrease in websites during 2009.

---

<sup>12</sup> Offending and Criminal Justice Group (RDS), Home Office, Ref: IOS 503-03

<sup>13</sup> [www.iwf.org.uk](http://www.iwf.org.uk)

There is no doubt that such abuse has a damaging and negative impact upon child victims. It has been claimed that in many instances where children are abused, the abuse is recorded by members of their own family or people known to them (Klaine, Davis, and Hicks 2001). Many indecent images depict the sexual abuse of children who are victimised both in the creation of the image and in the distribution of the image. It could be argued that a child is re-victimised each time their image is accessed, and images on the internet can form a permanent record of abuse.

The legislation in Scotland (the Protection of Children and Prevention of Sexual Offences (Scotland) Act 2005, s.16), England and Wales (the Sexual Offences Act 2003 (England and Wales), s.45-46)<sup>6</sup> attempts to curb the production, distribution and possession of indecent images of children on the internet. The age of the child is raised from 16 to under 18 in both acts with certain provisions. The purpose of the legislation is to protect children from abuse in the creation of such images in order to curb circulation.

In the United States the law is similar (Child Online Protection Act 2000 (COPA)), although indecent images of children do not have to be overtly sexual, the possession of suggestive images of children may be prosecuted under the legislation. It is also an offence to simply access images without saving them on a computer. There has been considerable debate in the United States regarding the introduction of COPA; the Act has been returned to the Supreme Court several times on the basis of representations made by the American Civil Liberties Union (ACLU) regarding its restrictiveness. The Sexual Offences Act 2003 does not create any new offences in this category but raises the age from 16 to under 18 by making amendments to the Criminal Justice Act 1991 and the Protection of Children Act 1978. The provisions allow a defence to the charge if : the picture is of a 16 or 17 year old; the 16/17 year old 'consents'; the picture/s of 16/17 year olds are not distributed; the perpetrator and the 16/17 year old are in long term relationship/married/co-habiting. S. 8H 2005 27

The ACLU have argued consistently and fairly effectively that the Act infringes upon civil liberties and that it is possible to accidentally encounter such images online. They also object to the inclusion of the possession of suggestive images, although presumably offence circumstances would be taken into account here. The ACLU has undoubtedly formed a powerful lobby in the United States. No such objections have been voiced in the UK in such an organised manner, although it could be argued that groups such as the IWF and key individuals such as John Carr have campaigned more successfully in the UK for the rights of child victims of internet abuse. In the United States under COPA the making available of material that is harmful to children for commercial purposes on the

Web is also illegal; unless child access has been restricted. It was argued by the ACLU that more effective, less restrictive mechanisms exist to protect children and that educating children and their parents about internet awareness would be a more effective approach (Supreme Court Transcripts, *Ashcroft v ACLU* 2/3/04).

## 5.6 Bahrain- Policy and Legislation

The Kingdom of Bahrain is governed by a bicameral legislature (Shura Council and House of Representatives), with its seat of government in Manama, the capital. It is a member of the United Nations,, UNESCO and the World Trade Organisation. The legal system of Bahrain is based on several sources, including the constitution, customary tribal law (*wrf*), three separate schools of Islamic sharia law, and civil law as embodied in codes, ordinances, and regulations. Sharia law includes the Maliki school of Islamic law (from Imam Malik ibn Anas, an eighth-century Muslim jurist from Medina) and the Shafii school of Islamic law (from Muhammad ibn Idris ash Shafii, a late eighth-century Muslim jurist fromGazza and then transferred to Egypt). Both of these schools are recognized by Sunni Muslims (see Sunni Islam , ch. 1). The third school is the eighth-century Jaafari (from Jaafar ibn Muhammad, also known as Jaafar as Sadiq, the Sixth Imam) school of Twelver Islam, recognized by Shia (see Shia Islam , ch. 1).

According to the Constitution of 2002, the government system is based on the principle of Separation of Powers, Legislative, Executive and Judicial. All functioning in cooperation with each other in accordance with the provisions of the constitution. The Highest power is the King, then comes the Prime Minister and the Crown Prince.

Bahrain has a dual court system, consisting of civil and sharia courts. Sharia courts deal primarily with personal status matters (such as marriage, divorce, and inheritance). Sharia courts are designated to Sunni Shari'a Courts and Shii'te Shari'a Courts which are all located in Manama including the courts of appeal. Appeals beyond the jurisdiction of the sharia Court of Appeal are taken to the Supreme Court of Appeal, which is part of the civil system (see Bahrain: Internal Security , ch. 7).

The Civil Court System is designated to the First instance court of which its decisions may be appealed to the Civil Courts of the lower degree of which its decisions may be appealed to the Civil Courts of a Higher Degree and Civil Courts of Appeal. Decisions made by the Courts of appeal may be appealed against in the court of Cassation which does not look into the substantive matters of a dispute. The Constitutional Court looks into the constitutionality of judgements made by the higher courts only and Laws issued by the Legislative bodies and Regulations issued by the Executive Bodies.

There is currently draft Cyber Crime Law which includes provisions making child pornography a criminal offence, Saudi Arabia introduced similar legislation in 2007<sup>14</sup>. Additionally, there is an ongoing discussion regarding where responsibility for administering the law will lie. There is a recommendation that the draft law is referred to the Central Informatics Organisation and TRA for discussion. Legislation also of relevance includes the legislative Decree (17) of 1976 in relating to Juveniles, and the Legislative Decree (19) of 2004 of Bahrain's accession to the UN Optional Protocols to the Convention on the Rights of the Child on the involvement of children in armed conflict and Rights of the Child on the Sale of Children, Child Prostitution and Child Pornography. Under the current penal code a child is defined as 15 and under. Sexual abuse of boys is considered less serious and sentencing reflects this. The physical abuse of children is not currently recognized in law and when prosecuted sentences tend to be short<sup>15</sup>. This is however addressed in proposed child protection legislation.

**The draft child protection law (Draft Law on the Child) defines child abuse as follows:**

***1. Physical ill-treatment means any act that would lead to intentional physical abuse of children, including fractures, burns, wounds or bruises or internal injuries or the effects of violent shaking or poisoning, or suffocation or drowning, or create artificial condition.***

***2. Intended psychological maltreatment, any act that would lead to damage growth and psychological health of the child such as: verbal abuse and harsh rebuke, attack.***

***3. Refers to sexual abuse, exposing a child to any sexual activity, including the projection of sexual relations or fondling or penetration (Almishqi or anal sex) or the initiation or exposing a child to watch movies or pornography, or use in the production or distribution in any form in any form.***

**Source: Draft Child Protection Law, 2010**

---

<sup>14</sup> The legislation was drawn up by the Kingdom's Commission for Telecommunications and Information Technology, will become law once it is published in the government's official gazette within the next 120 days. The law seeks to protect individuals, companies and organisations from being harmed via the internet. The maximum punishment under the legislation is a prison sentence of ten years and a fine of US\$1.3million, which can be imposed on anyone found guilty of hacking into government networks to steal information related to national security or using the internet in support of terrorism. Creating web sites that defame humanity, advocate drug use or that contain pornographic material can lead to sentences of up to five years in prison and/or a fine of US\$1.3million.

<sup>15</sup> All cases involving physical abuse of children are referred to Public prosecution but none have proceeded.

The draft legislation includes sections addressing Internet luring or grooming (Article 17), the production and distribution of indecent child images ( Article 129 ) and the showing of pornographic images to children (Article 129) , the Chapter will place some responsibility for controlling the access of young people to the Internet with the private sector (restricted access at Internet Cafes for example) . The legislation includes the online grooming of children, defined as follows:

*'luring and exploitation of children via the web "Internet" in matters contrary to public morals, public order or not commensurate with their age, is now a criminal act punishable by imprisonment.'* (Article 17)

The legislation prohibits the showing of pornographic images to children and the use of children in the production and distribution of pornography via the Internet:

*'The showing of sexual relations, or fondling, or penetration (Almishqi, anal), to children in movies or pornography, or the use of these in production in any form, including via the Internet is prohibited'* (Article129)

Article 130 recommends that this be punishable by life imprisonment or a imprisonment term of not less than ten years from (where the child is under 18 years old and has not provided consent) and punishable by imprisonment for not less than seven years nor more than ten years of a female under 15 years of age and has provided consent.

The legislation also includes a section introducing sanctions for the physical and sexual abuse of children perpetrated by strangers and family members, which includes training courses addressing parenting skills and anger management, community service, denial of employment in any work involving children and the possibility of a short term of imprisonment (3 months).

The Chapter introduces the notion of removal of the child to a safe place for the first time in Bahraini legislation:

*'The child exposed to ill-treatment within the vicinity of his family or those who take care, will be removed by the police, check the status of child protection, shelter designated for that purpose, to be submitted to the Attorney General as soon as a decision to approve this procedure, and the Centre for Protection Child asylum to the*

*Syariah Court applied the appropriate version of the rule of the transfer of custody of the child to a foster family to protect them from ill-treatment'. (Article 18)*

If introduced the proposed legislation should have far reaching implications for the development of a comprehensive child protection framework in the Kingdom. The draft legislation has been presented by the Shura Council and is currently under consideration by the Government, a decision regarding implementation of the new legislation is likely to be made in late 2010. The proposed legislation covers a range of child protection concerns including health, education and social issues. The legislation constitutes an attempt to introduce a legislative framework in the child protection area (Source: Interview Member of Shura Council, 6/2010).

There is an increased recognition of children's rights on the part of Gulf countries and the UAE plans to introduce child protection laws that are similar to those in the United States and the United Kingdom. The Ministry of Interior has suggested that it is considering forming a unit to tackle all forms of child sex abuse. Among its priorities would be a new law making it an offence to possess child pornography and the setting up of a sex offender register.

#### **5.6.1 Bahrain: Responsibility for Child Protection and Welfare**

The Kingdom of Bahrain joined the child Rights Agreement for 1989 in accordance with the Decree – Law No. 16 for 1991 on 13<sup>th</sup> February 1992. The Ministry of Social Development has responsibility for child affairs and child welfare via the National Centre for Child Protection.

The Bahrain Centre for Child Protection was opened on 13/05/2007 under the patronage of Social Development Minister, Dr. Fatima Bint Mohammed Al – Bulooshi. The Centre is considered the central body that has responsibility for child protection. The Centre provides and services that relate to the assessment, investigation, therapy, and follow-up of abused and neglected children, in liaison with various concerned Governmental and national bodies.

#### **The Centre objectives are:**

- 1. To work on the provision of child protection against ill- treatment from the family and society.**
- 2. To work on protecting the child from harm during the investigation.**
- 3. To provide psychological, welfare and legal services and to liaise with the concerned bodies.**



4. To rehabilitate the family in order to keep the child in his family environment, where possible.
5. To find an alternative family for the child in case he encounters ill-treatment.
6. To promote the child and society awareness about child protection and rights.
7. To follow the implementation and application of the rules and agreement related to child protection.

*(Source: Ministry of Social Development [www.social.gov.bh](http://www.social.gov.bh))*

The centre receives all notifications concerning child abuse. Providing: Childcare to victims of physical or psychological harm; medical treatment; psychological, social and educational services; coordination of legal and juridical services; child and family rehabilitation.

Under Article 10 of the draft child protection legislation the Child Protection Centre will take the lead in acting as a centre point in working with referred abused children and their families and in undertaking research, compiling data in this area, this remit presumably extends to Internet related abuse also.

*'The Child Protection Centre is the focal point, which holds the evaluation and shelter and follow-up of children who presented to ill-treatment and coordination of services provided to him and his family by the authorities concerned, and proceed all the Centre's functions and powers necessary to protect children from abuse, including:*

- 1 - take all the direct and immediate measures to protect children from ill-treatment.
- 2 - A study of the vulnerability of children to abuse the health, psychological, social, economic and legal.
- 3 - Follow-up cases of children subjected to abuse on a regular basis in the case handed over to their parents or caregivers.
- 4 - Providing alternative care outside the family who exposes children to ill-treatment promptly and temporary, and if the child's life in danger or if he was sexually abused by those who care.
- 5 - to take all action to rehabilitate the child who was subjected to ill treatment and his family to ensure his return to his family situation normal, including treatment and psychological rehabilitation and educational courses, educational and social skills development and skills of self-protection of the child' (Article 10) .

Article 13 sets out the powers and overarching duties of the Centre Board of Directors which will include: the development of plans and programs for dealing with the prevention and protection of children from abuse; coordination of all stakeholders, public and private, on the protection of children from abuse; supervision of the activity centre and its work; provision of advice to the concerned authorities on the protection of children from abuse; development of studies and research on the phenomenon of child abuse.

#### **Summary Points: Bahrain Legislation**

- **There is currently no comprehensive legislative framework that addresses child Internet safety or cybercrime**
- **Legislation is proposed in the cybercrime area– this will address cyberfraud**
- **A legislative framework is proposed in the child protection area, this includes the online ‘luring’ or grooming of children (Article 17) and the use of children in the production of pornographic images ( Article 129)**
- **The National Centre for Child Protection (Ministry of Social Development) will take on an increasingly central role in child protection if the legislation is introduced.**

### **5.7 Internet Safety and Young People: International Approaches and Initiatives**

#### **5.7.1 Protecting children**

It should be imperative, as Calder (2004) rightly suggests, to encourage appropriate and safe use of the Internet by assisting children and young people to feel comfortable navigating the information highway. In fact, *“the most important issue surrounding child abuse and the Internet is child protection, not computer technology”* (Jones, 2003 in Gallagher 2008:45) because technology alone is always fallible and offers no guarantees of child protection. However, if technology is combined with education and awareness amongst children, parents and teachers, and effective inter-agency partnership working, it would be easier to maximise the few available resources and move one step closer to making cyberspace a safe place for young and vulnerable Internet users.

A considerable amount of work has been done internationally to protect children online. The G8 countries have agreed a strategy to protect children from sexual abuse on the Internet. Key aims include: the development of an international database of offenders

and victims to aid victim identification; offender monitoring and the targeting of those profiting from the sale of indecent images of children. Work has also been done with Internet service providers and organizations such the Association for Payment Clearing Services in the UK, and other credit card companies in different countries, in attempting to trace individuals using credit cards to access illegal sites containing indecent images of children.

Organisations like the Family Online Safety Institute (FOSI) have also worked to make the online world safer for young people by identifying and promoting best practices, tools and methods that also respect free speech. FOSI's members include: AOL, AT&T, Blue Coat Systems, BT Retail, Comcast, Facebook, France Telecom, Google, GSM Association, Kingston Communications, Loopt, Microsoft, MySpace, NCTA, Ning, Nominum, Optenet, RuleSpace, Sprint, StreamShield, Symantec, Time Warner Cable, Telefónica, TELMEX, The Wireless Foundation, Verizon, Yahoo!. FOSI hosts an annual international conference to bring together Internet safety advocates from a variety of sectors, including global corporations, government, non-profits, academia and the media, to discuss the current issues of online safety and emerging solutions that will enhance it (<http://www.fosi.org/cms/>).

It would however appear that there is much work to be done in educating Internet service providers, research (2005) undertaken by the Internet Watch Foundation in the UK suggests that 72% (of a sample of 1000 IT senior professionals) were unaware of the implications of amendments to the Sexual Offences Act 2003 upon their industry and only 56% had heard of the IWF. Internet service providers have however taken some action to address child safety online: British Telecom's Operation CleanSweep resulted in the closure of all of its chat rooms, following concerns over sex offender's use of the service to target children. Other providers such as MSN and Yahoo<sup>16</sup> have taken some action to protect children in chat rooms. A Scottish company (Net ID) has launched the world's first virtual ID card which aims to protect children and young people online. The card aims to remove the anonymity of the internet thus preventing paedophiles posing as children in chat rooms to gain their trust. (Lunchtime Scotland Today, 2/8/06).

Many police forces both in the EU and the United States are working to trace Internet sex offenders and their victims. In the UK, National and local High Technology Crime

---

<sup>16</sup> Yahoo were forced into action in 2005 by a New York State Attorney General's Office investigation which found that users were creating chat rooms explicitly for the purpose of grooming children for abuse. Yahoo then agreed to put into place procedures to ensure that the creation of such chat rooms would not continue.

Units currently investigate the grooming of children on the Internet and indecent online images of children. Successful prosecutions have been brought under the acts in Scotland, England and Wales, both for 'grooming' online and for the possession of indecent Internet images on the Internet following Operation Ore. This operation was launched following information provided to the UK police by the FBI in the United States, regarding peer-to-peer technology in sharing indecent images of children. The National Crime Squad (which targets serious and violent crime) has made 2,200 convictions since 2002 under Operation Ore.

Organisations like the Virtual Global Taskforce (VGT) and the Internet Watch Foundation (IWF) are making some headway in attempting to protect children online. VGT is an organization that comprises several international law enforcement agencies from Australia, Canada, the United States, the United Kingdom and Interpol. Through the provision of advice and support to children VGT aims to protect children online and has set up a bogus website to attract online groomers. The Internet Watch Foundation (IWF) is one of the main government watchdogs in this area. Although based in the UK the IWF is a part of the *EUs Safer Internet Plus Programme*. And is part of the International Association of Internet Hotlines (INHOPE) network. As Robbins and Darlington (2003) have pointed out, this programme has four main aims:

- to fight illegal Internet content
- to tackle harmful Internet content
- to promote a safer Internet environment
- to raise awareness about Internet dangers

Whilst the first three of these objectives have until now been largely the province of institutions and organisations, the fourth has immediate implications for the everyday use of the Internet by members of the public and, most significantly, children themselves.

### **5.7.2 Teaching Safety Online**

Measures to protect children include school-based programmes aiming to educate children, parents and teachers about online safety and workshops/programmes run by NGOs and other organisations. Such programmes are now routinely delivered to secondary school children in the UK and other countries such as the USA, New Zealand and Canada (Davidson and Martellozzo 2005).

In Bahrain the Be-free organisation has undertaken workshops on Internet safety and offers advice to parents and children on its website ([http://www.be-free.info/en/How\\_can\\_I\\_protect\\_myself\\_on\\_the\\_Internet.asp](http://www.be-free.info/en/How_can_I_protect_myself_on_the_Internet.asp)). The Be-Free organisation was set up to educate parents, children and teachers about child abuse. **The organisations goals are to:**

- **Build a Smart, Safe and Strong child.**
- **Provide parents and caregivers with skills to build emotionally intelligent children.**
- **Empower children and adults victims of child abuse to regain strength and trust in self and others.**
- **Conduct specialized researches and studies.**
- **Increase society awareness on issues related to child abuse and neglect.**
- **Provide specialized consulting and training for professionals.**


<http://www.befreecenter.org/about-us.aspx>


During 2009 the Be-Free Centre ran a series of workshops with children in schools in Bahrain to raise awareness about Internet safety. The workshops were entitled "*I am a Strong, Smart, and Safe Child...over the Internet*" and provided information about protection skills for children in grades 1 to 3 and 4 to 6. In these workshops, real case studies were discussed that provided examples children's online experience. The following advice is offered to children on the Be-Free website.

Keep these tips in mind when you go online using the internet:

- ✿ Pick a screen name that will attract the kind of friends you would like. Do not use a name that is negative, belittling, or provocative.
- ✿ Only send pictures of yourself or any other member of your family with your parent's permission.
- ✿ Tell your parents if you encounter inappropriate or offensive messages or attachments. Never respond to these messages.
- ✿ Don't tell anyone your exact age, just say you are under 18. Be smart and do not give your name, address, phone number, parent's work address/phone number or the name or location of your school.
- ✿ Do not fill out surveys or register at sites without your parent's

permission.

 Never tell anyone that you are alone or what time you may be alone.

 Never trust or believe any one online. They may be lying in every information they give you even their age, sex, or country.

(BeFree <http://www.befreecenter.org/News/-what-do-children-need-to-be-protected-over-the-internet.aspx>)

Other organisations such as the Bahrain Internet Society (Bahrain Internet Society BIS. <http://www.bis.org.bh/>), an NGO set up in 1996, are planning to run Internet safety and awareness sessions for young people and their parents in the near future and some schools are working to raise awareness amongst parents and pupils. There has however been no systematic attempt to educate young people or adults in Internet safety.

In the USA, the ICAC (Internet Crime Against Children) Task Force has created a program to help both children and parents to understand the importance of the Internet but also the danger that may be encountered whilst using it. The programme has been developed by NetSmartz Workshop. NetSmartz is an interactive, educational safety resource from the National Centre for Missing and Exploited Children (NCMEC) and Boys & Girls Clubs of America (BGCA) that uses age appropriate, 3-D activities to teach children and teens how to be safer when using the Internet. NetSmartz has been implemented in more than 3,000 BGCA Clubs nationally, serving more than 3.3 million young people.

The programme provides parents, children and teachers with an overview of online risks. It argues that in addition to the useful educational information available on the Internet, a great deal of Internet content is not appropriate for children. This content can include nudity or other sexually explicit material; hate or racist websites; promotional material about tobacco, alcohol, or drugs; graphic violence; information about satanic or cult groups; or even recipes for making bombs and explosives at home (Davidson and Gottschalk 2010).

According to ICAC (2000) more than 30 million children in the USA alone use the Internet. A report on the Nation's Youth (2004) suggests that 1 in 4 children on the Internet had an unwanted exposure to sexually explicit pictures that were inappropriate for children to view. Approximately 1 in 5 received a sexual solicitation or approach; 1 in 17 was threatened or harassed; 1 in 33 received an aggressive sexual solicitation (from

someone who asked to meet them somewhere; called them on the telephone; sent them regular mail, money, or gifts).

A similar programme to that of ICAC was designed in the UK in 2002. The Metropolitan Police Safer Surfing Program was delivered by Safer Schools officers, in response to demand from local parents. This Metropolitan Police Program differs from other educational Internet programs in that it is interactive and delivered directly to children in schools. It is unique in this respect. It was designed in 2002 for use with 12- and 14-year-old children as this age group has been identified as active, independent users of the Internet. The program aims (Davidson and Martellozzo 2008b): to encourage safe use of Internet chat rooms and interactive games amongst school children, to outline the potential dangers of talking online to virtual friends via an interactive session, to educate children about strategies for safe use of the Internet via an interactive session, to educate children about strategies for safe use of the Internet via an interactive session using a mnemonic (S - secrets don't keep them; A - attachments don't open them; F - false don't believe them; E - exit don't stay there; R - remember public chat rooms no personal details), to educate children about the dangers of opening attachments coming from unreliable sources as they may contain illegal and damaging material; and to educate parents about safety issues and strategies via educational information and presentations.

In the UK the Child Exploitation and Online Protection Centre (CEOP), a recently launched organisation (April 2006), funded by Government and the communications industry, which includes representatives from the police and other criminal justice agencies. CEOP draws upon expertise from Internet service providers (such as AOL and Microsoft) and children's charities such as the NSPCC, in attempting to confront online abuse (<http://www.ceop.gov.uk>). This centre aims to raise awareness amongst children and parents about the potential dangers of the Internet and to create a database of known offenders. Police officers visit chat rooms posing as children in order to detect grooming behaviour. False websites will be set up to attract sex offenders seeking to groom children. These policing tactics are not new. The National High Technology Crime Unit Scotland and the London Metropolitan Police High Tech Crime Unit (HTCU), for example, have placed undercover officers in teen and other chat rooms likely to attract children since the introduction of the Protection of children and Prevention of Sexual Offences (Scotland) Act 2005 and the Sexual Offences Act 2003 (as have other HTCU's). These officers have learnt to interact as children do online through the use of text language in order to prompt and encourage conversation with child abusers seeking to

groom a child. Several recent convictions have been secured on this basis and an increasing number of online groomers are being arrested under the legislation.

CEOP's ThinkUKnow Programme is now delivered to children throughout the UK. The programme seeks to impart Internet safety advice to children and young people aged 5-16. The programme includes a presentation delivered in schools (usually) and a website with different sections for different age groups, parents, teachers and trainers. Trainers are encouraged to report the number of children trained via a website link (they must go on to the website to do this). Safety advice is also provided on the website. The recent evaluation of CEOP's ThinkuKnow (TUK) internet safety programme (Davidson, Martellozzo & Lorenz, 2010) summarised the findings about risk taking on the internet:

- A high proportion of children reported having engaged in high risk behaviour online (defined by degree to which they share information with and interact with strangers).
- A significant proportion says they will continue with such behaviour (particularly 13+).
- Interacting with strangers (i.e. adding them as ISM or Facebook friends and exchanging messages) is becoming an accepted behaviour not perceived as 'risk-taking'

Other European approaches to child online safety include the Norwegian Child Consent Initiative. The *Child Consent Initiative* is concerned with the protection of personal information about children that is published on the Internet. Some parents tend to publish sensitive information about their children and pictures from vacations and other occasions without considering the potential dangers involved. A principle of *child consent* will imply that parents will have to ask their children and get their permission before publishing material involving them. The principle of child consent is a planned initiative to be included when Norway revises its Child Law ("barnelov"). A fifth initiative stems from Save the Children Norway, which has developed and published chatting rules. There are four important *chatting rules* described in their pamphlet (Redd Barna, 2007):

1. Be anonymous. Never give away your name, address or telephone number,
2. Leave if you do not like the chat. You are in charge!
3. Never meet someone from the chat alone. Bring always an adult the first time.
4. If you are to meet someone from the chat, choose a public place with many people.



Several European countries now have 'red buttons' on social networking sites and other website used by children that can be used to report online abuse. In Norway The Red Police Button was introduced in September 2008. The red button is located on web pages for children where grooming may occur. The red button can be pressed by children and others who experience abuse behaviour on that web site. When the button is pressed, an automatic message is sent to the national criminal police (Kripos) in Norway Kripos is open day and night. When the red button is pressed, the police tip page automatically opens on the screen. Three alternatives emerge on the screen: Sexual exploitation of children ('Seksuell utnytting av barn'), Human trafficking ('Menneskehandel'), and Racial expressions on the Internet ('Rasistiske ytringer på internett'). Facebook has also recently agreed to add a red button in the UK.

In Italy the EASY awareness node in is run by Adisconsum and Save the Children Italia. It is now part of a combined node for hotline and awareness raising activities in Italy, aimed at guaranteeing a relevant increase of Internet safety for minors – both on the side of supporting the fight against illegal/harmful content and online crime and promoting a more responsible, positive and large use of the Web and the new ICTs by minors – thus involving all relevant stakeholders and strengthening synergies with both national and EU policy initiatives. There are three main activities within this project. Firstly, a wide awareness campaign carried out at different levels: an extensive media communication plan; participation in a number of identified events and fairs focusing on new technology (NT); the successful implementation of high visibility and impact events, such as the Internet Safety Weeks which offer a number of awareness raising activities around Italy, meetings in schools with minors and parents, training sessions for teachers, school managers and educators, project presentations for local media and authorities, events for the general public on the main squares where people can debate and deal with NT in a safe and constructive way.

Secondly, the creation of a new Advisory Board acting as a national reference point and a discussion forum with regard to the issues relating to a safer use of NT by children and young people. Thirdly, high quality and well targeted awareness tools and strategies, by actively involving the target groups in order to really meet their continuously evolving needs and expectations. The combined node of easy4.it and stop-it.it has the endorsement of the principal parents and teachers associations as well as Internet and mobile providers such as WIND and AIIP (Association of Italian Internet Providers), the Ministry of Education, Ministry of Communication and the Polizia Postale .

## Literature Review: Summary of Key Points

1. There is little research addressing adult Internet use. Research conducted in the UK by the National Audit Office suggests a correlation between low levels of IT literacy and low levels of confidence in the use of digital media.
2. It is increasingly becoming more common for children to access the internet in their own bedrooms, by mobile phone and without parental supervision.
3. More than half (51 per cent) of teenagers in Europe say they use the internet without any form of supervision from their parents (Cross Tab, 2009), while 23 per cent of parents in the UK with children under the age of 11 report that they allow their children to access the internet without supervision at home (Anti-Bullying Alliance, 2009).
4. There is a growth amongst young people in the use of alternative devices to access online content, particularly mobile phones.
5. Teenagers seem particularly risk averse , many understand key safety messages but still engage in online risk taking behaviour.
6. Not all parents/carers are aware of safeguarding measures
7. Parents/carers have low awareness of the existence and use of access controls for mobile phones and games consoles
8. There is further scope for e-safety provision to be improved in schools, particularly in primary schools and with teenagers.
9. Girls aged 12-15 are significantly more likely than boys of the same age to use social networking sites to communicate with peers.
10. Young people from the most socio-economically disadvantaged groups are less likely to have access to the internet than other groups.
11. Several EU countries have introduced grooming legislation and the European Commission has recently (5/2010) issued a directive to member states to ratify this legislation. Member states may however chose not to follow this directive.
12. The *UN Convention on the Rights of the Child* defines a child as a person under the age of 18 but given wide variation in the age of consent to sexual relations across countries there is clearly legal disagreement

regarding the age at which childhood ends, there is no consensus in international law regarding the age of consent.

13. Ninety-four of 188 INTERPOL member countries have introduced legislation addressing the creation of pornographic child images.
14. There is currently no comprehensive legislative framework that addresses child Internet safety or cybercrime in the Kingdom of Bahrain, however: Legislation is proposed in the cybercrime area – this will address cyberfraud and a legislative framework is proposed in the child protection area, this includes the online 'luring' or grooming of children (Article 17) and the use of children in the production of pornographic images (Article 129)
15. The National Centre for Child Protection (Ministry of Social Development) will take on an increasingly central role in child protection in the Kingdom of Bahrain if the proposed child protection legislation is introduced.
16. The G8 countries have agreed a strategy to protect children from sexual abuse on the Internet. Key aims include: the development of an international database of offenders and victims to aid victim identification; offender monitoring and the targeting of those profiting from the sale of indecent images of children.
17. Some social networking sites now include safety information and some have a red button to enable children to report abuse
18. Measures to protect children include school-based programmes and online advice aiming to educate children, parents and teachers about online safety and workshops/programmes run by NGOs and other organisations. Such programmes are now routinely delivered to secondary school children in the UK and other countries such as the USA, New Zealand and Canada (Davidson & Martellozzo, 2008). Organisations such as BeFree offer safety advice to young people and their parents on websites in the Kingdom Of Bahrain

## **6. Research Methodology**

### **6.1 Introduction**

#### **6.1.1 Research Aims**

The research aimed to:

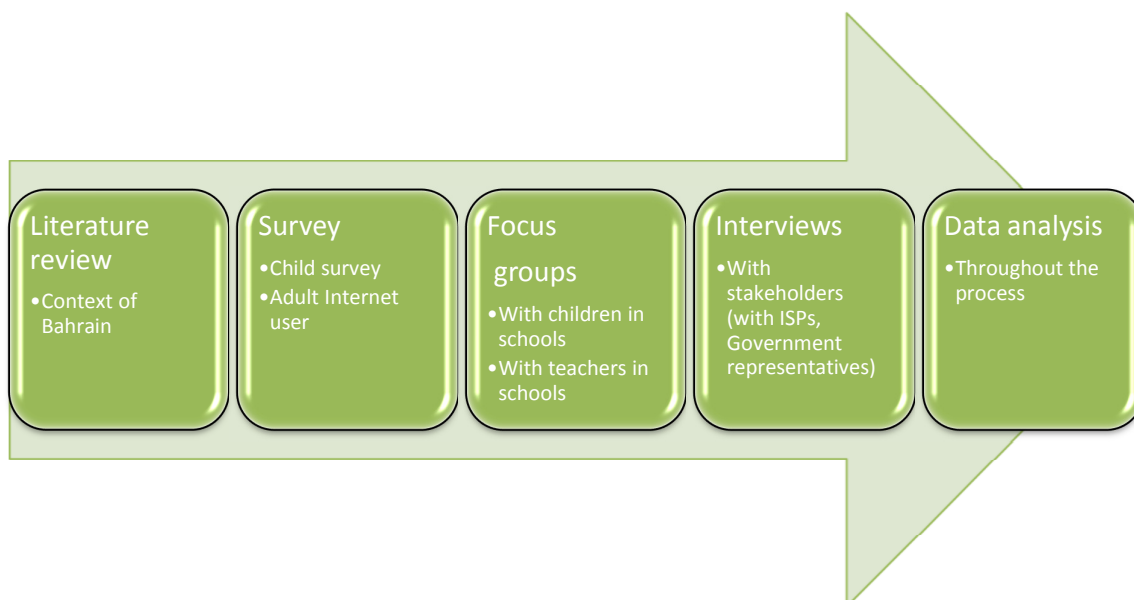
- 1. Identify and review the evidence on risks to children's safety and wellbeing online;**
- 2. Assess the effectiveness and adequacy of existing measures to help safeguard children online;**
- 3. Identify and assess any gaps between the identified risks to the safety of children and the adequacy of the existing measures;**
- 4. Suggest ways to help parents and carers understand and manage the risks;**
- 5. Make recommendations for improvements and additional action;**
- 6. Explore the online safety awareness of the adult population.**

These aims have been met through the use of a mixed methods research strategy. The research consisted of four phases:

- 1) Phase one: Adult survey
- 2) Phase two: Child Survey
- 3) Phase three: focus groups with children
- 4) Phase four: interviews with stakeholders

The research process is summarised in figure 3:

**Figure 3 The research design and the research process**



The fieldwork was conducted from March to June 2010. This section of the report describes the methodological approach approved at the outset of the research by the Telecommunications Regulatory Authority (TRA).

## 6.2 Phase one: Adult Survey

This survey aimed to explore adults' views and experiences about the way in which they use the Internet. The findings from the research will help to inform Internet safety practice and policy throughout the Kingdom of Bahrain.

Survey research comprises a cross-sectional design in relation to which data are collected predominantly by a questionnaire or by structured interview. In this research, an online questionnaire was administered in both English and Arabic<sup>17</sup> (see Appendix 1 and Appendix 2).

The questionnaire was piloted on a small sample of adults before wider use. The final version of the questionnaire was hosted by TRA and marketed by a number of ISPs and other institutions such as the University of Bahrain, who all included a link of the questionnaire on their website. A total of 816 participants completed the online survey.

The survey was standardized in such a way to ensure reliability and validity. This is important so that the results can be generalized to the wider population. However, the

---

<sup>17</sup> The survey was translated by a professional translator working for TRA.

sample was non-random and self selecting; this places some limitations on generalisation.

### 6.3 Phase two: Survey of children in schools

This survey sought children's views and experiences about the way in which they use the Internet and their online experiences. The survey was administered in both English in private schools, and Arabic in public schools (see Appendix 3 and Appendix 4).

Nielsen<sup>18</sup>, a large social research agency administered the survey and collected and analysed the data under the guidance of Prof Davidson and Dr Martellozzo.

The sampling frame consisted of the list of children aged 7-18 attending 8 schools in the private and public sectors, in order to ensure the inclusion of children from all social classes. A total of 2558 children participated in the survey, 1550 of whom were boys and 1008 were girls.

Eight schools were selected for inclusion in the survey on the basis of their demographic mix, they were approached by TRA and Nielsen to secure access, the schools agreed to participate once Ministry of Education permission had been granted. The participating schools are indicated in table 1.

**Table 1**Schools participating to the survey

Name of School
<b>British School of Bahrain</b>
<b>Al Noor International School</b>
<b>Isa Town Middle Boys Intermediate School</b>
<b>Al Hidayah Boys Secondary School</b>
<b>Umm Salamah Middle Girls Intermediate School</b>
<b>Hamad Town Secondary Girls School</b>
<b>St Christopher's School</b>
<b>The Indian School</b>

Most schools were generally willing to cooperate given the importance of the research. Public schools showed less willingness to participate because some pupils were sitting their final exams. However, the public schools total achieved sample size of 1143 and the private school sample was 1415 give a sampling error of  $\pm 2.9\%$  and  $\pm 2.6\%$  at a

---

<sup>18</sup> Nielsen is a global leader in multinational media research and analysis

confidence level of 95%. Therefore, the total sample meets the required standard needed to address the study aims. .

These calculations are indicated in table 2.

**Table 2 Sample size and confidence level**

	Sample Size	Confidence Interval	Confidence Level
Total level	2558	+/- 1.9 %	95%
Total Public Schools	1143	+/- 2.9 %	95%
Total Private Schools	1415	+/- 2.6 %	95%

The participating schools formed a representative sample in terms of the following criteria:

- 1) Private and public sector
- 2) Gender
- 3) Age
- 4) Ethnicity

### **6.3.1 Limitations**

A number of interviews were uncompleted due to the following issues:

- Some students encountered an internet connection problem, consequently the survey saved as uncompleted.
- Some students took a long time to complete the survey and the survey session expired.

Other reasons include:

- Some students decided not to complete the survey.
- Some schools kept the survey open for the students, but by the time students have reached the computer lab, the session had expired.
- Some students completed the majority of the questions, but at the end did not press the final submit link.

However, it is important to note that the total number of uncompleted interviews do not reflect the number of students who did not complete the survey and did not affect the size or robustness of the final sample.

#### **6.4 Phase three: focus groups with children**

Phase three consisted of the collection of qualitative data through a group interview. Focus groups seek to explore the thoughts and experiences of others. This was considered to be the best method of data collection for children aged 7-17. When participants in a group interview share an interest in the discussion topic (such as Internet use) their interaction can provide information about how they relate to the topic and to each other (Morgan 2007).

Each focus group consisted of 5-6 respondents and the discussion was tape-recorded to ensure accuracy in recording, the data collection instrument was an interview guide (see Appendix 5). The aim of this phase of research was to explore young people's (aged 7-17) experience and awareness of Internet use and Internet /other digital media safety.

Given the sensitive and exploratory nature of the research a qualitative approach was adopted but including a sufficiently large, representative sample of children to produce some qualitative data counts. The following methodological approach was employed: Focus group interviews (N 15) were conducted with a representative (by sector: public and private, age and gender) sample of children (5-6 children in each group) focus groups in each sector (30 groups in total). A total of 150 students participated in the focus groups and a total of 30 teachers were also interviewed in both public and private schools.

Prof Davidson and Dr Martellozzo conducted the focus groups with English-speaking children and teachers in a British school in Bahrain. For ethical issues, the focus groups with children and teachers from other non- British schools were carried out in Arabic by local experienced researchers from the University of Bahrain. Two female researchers conducted the focus groups in the girls' schools and two male researchers in the boys' schools. In the Public schools the research was supervised locally by Bahrain University's Dr Khalid Al Mutawah.

#### **6.5 Phase four: stakeholder interviews**

Eighteen semi-structured interviews were conducted on a one-to-one basis with stakeholders including representatives from:

1. Government bodies involved in the social development of children and child wellbeing.
2. Child welfare support agencies, charities and NGOs



3. Internet industry.
4. TRA
5. Bahrain-based Academia

Semi-structured interviews are interviews in which the researcher makes use of a topic guide that includes “a list of topic headings and possibly key questions to ask under these headings” along with “a set of associated prompts” (Robson 2002:278). An interview guide was created to facilitate the interview process (see Appendix 6) and interviews were loosely structured as follows:

1. Introduction and research overview

The interview guide included an introductory statement that explained the purpose of the research.

2. Career

A general set of questions regarding the respondents’ experience working in their field. This section was intended to be exploratory as it seemed particularly important to know about the respondents’ work experience in the field and their perceptions of online safety.

3. Legislation

This section focused on legislation, particularly on online child safety and child protection

4. Innovations

It is clear that the Internet is more than just a medium of communication (Castells 1996; Castells 2004). It constitutes a new virtual reality or cyberworld with its own rules and its own language. It provides a supportive context within which the child is no longer a Bahraini citizen but a citizen of the world. This section included exploratory questions regarding how the Internet has benefited education, social interaction and brought generally significant innovations.

5. Recommendations

The aim of this section was to explore stakeholders’ advice and recommendations to ensure the safety of young people and adults in the digital world.

Although the broad categories that comprise the interview guide were structured to elicit specific information, a common feature of qualitative interviewing is that the categories

should not be mutually exclusive. Recurrent themes, such as the importance of Internet in child development, the widespread problem of lack of awareness for both parents and children, the impact that the social networking sites may have on children, the lack of a strong legal framework, arose at many different points during the interviews. All respondents spoke freely regarding problems they have encountered during their careers, far more so than had been anticipated.

The advantages of interviews are that they enable the interviewer to follow up on and probe responses, motives and feelings and their potential added value is that the recording nonverbal communications may enrich the qualitative aspects of the data (Davis, P. in Jupp, V. 2006).

### **6.6 Access:**

One of the major concerns in research is mainly to do with gaining access at all levels. Fortunately, access was granted when this study was at an embryonic stage. TRA helped the researchers to obtain access at an exceptionally high level for the stakeholder interviews; provided support in accessing schools; hosted and marketed the online survey, together with the ISPs of the Kingdom. Furthermore, the conference on online safety held in Bahrain in April 2010 and sponsored by TRA and the Washington-based Family Online Safety Institute (FOSI) proved to be a vital opportunity for the researchers to present some preliminary findings and network with some of the key stakeholders who participated in this study. This high level of access clearly enhances the validity and quality of data produced in this research.

### **6.7 Ethics**

Careful consideration was given to all relevant ethical aspects of this research to ensure strict adherence to professional codes of conduct, primarily the British Society of Criminology (BSC) Ethical Guide was used to inform ethical design and conduct throughout. In addition reference was made to the British Sociological Association guidelines.

### **6.8 Informed and Voluntary Consent**

Formal consent was obtained at different levels. Firstly, written authorisation for schools to participate in the research was provided by the Ministry of Education represented by King Hamad's Schools of Future Project Directorate, the Information Systems Directorate and the four Education Directorates (Primary, Intermediate, Secondary, Technical and Vocational).

Once permission to conduct the research was obtained, written consent for children to participate in the research was gained from their parents/guardians via Head Teachers before focus group interviews were undertaken. The children's informed consent was also sought. Respondents were provided with a description of the research which clearly described the research aims and process. Informed consent was sought from schools, parents and young people for the survey fieldwork.

Informed consent was also sought from each individual stakeholders. Participation in all stages of the research was on a voluntary basis.

### **6.9 Confidentiality and Anonymity**

A statement regarding confidentiality and anonymity was given to all respondents, with the usual provisos. However provision was made that any child disclosing abuse during the research would be referred to the School head teacher who facilitated the research and helped the researcher to gain access. In the event, this did not occur.

To allay respondent concerns over the confidentiality of their participation given the sensitivity of the research topic, assurances were given regarding safe and confidential data storage. Data is stored in strict adherence with the UK Data Protection Act 1998. Data kept at Kingston University was anonymised and stored by ID number only, and all written records are kept in locked cabinets. Data gathered via the online survey did not include names.

### **6.10 Data Collection**

The survey data collection instruments included two online questionnaires; the focus group and stakeholder interview data collection instrument were interview guides. The instruments were developed on the basis of the research aims, current and recent research in the area.

The survey instrument was validated originally in the UK (Davidson, Lorenz, and Martellozzo 2010) by means of 10 cognitive interviews with children at two participating schools:

- An urban, ethnically mixed comprehensive school
- A very rural, largely white comprehensive school.

Cognitive interviewing aims to uncover possible misunderstandings, inconsistencies, unclear questions or terms, inappropriate response options and incomplete coverage of a particular theme. Specifically it investigates:

- Respondent comprehension of questionnaire wording
- Respondent recall of activities asked about and identification of possible recall problems
- Cognitive judgement processes and shortcuts used by respondents to select their answers
- Issues around responses chosen, e.g. inappropriate response categories or socially desirable responses.

The cognitive interview discussion guide was developed after the survey questions were agreed, as the questions asked in cognitive interviews related to the specific wording of survey questions. As the survey was to be administered online, the cognitive interviews used an online version of the questionnaire for testing purposes.

As a result, it was not necessary to carry out the same exercise in Bahrain, the questionnaire was translated into Arabic. The survey was administered in the ICT suites of participating schools during scheduled ICT or PSHE classes. Students completed the questionnaire online.

Focus groups were facilitated by one researcher and were recorded, the interviews were transcribed and where needed translated by professionals. Analysis was carried out using the thematic qualitative technique, emergent themes were identified and evidence is presented in the form of verbatim quotes. The qualitative data is presented with key findings from the survey data in this report. The interviews findings are reported in a separate section.

## **7. Findings: Adult Survey**

### **7.1 Sample characteristics**

The total survey sample consisted of 816 respondents, aged from 18 to 71. The sample was self selecting and was recruited via ISPs and other organisations such as the University of Bahrain who publicised the survey's link on their website. The survey was hosted by TRA.

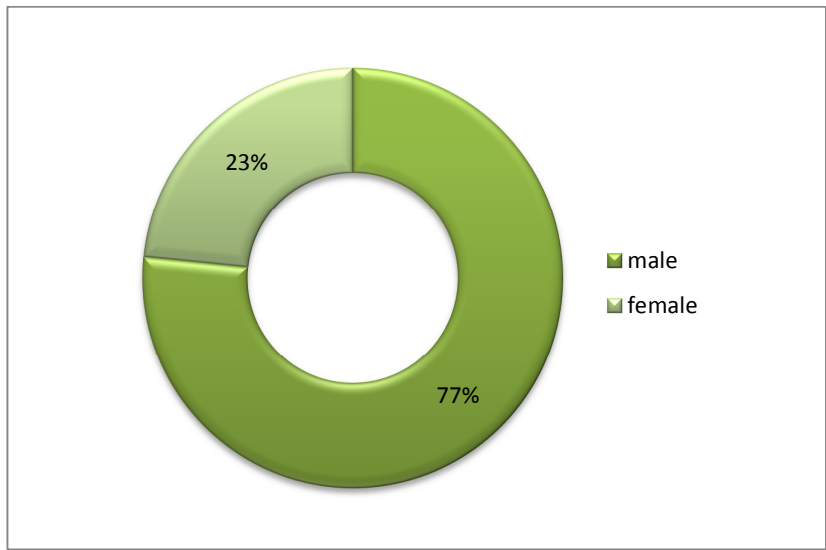
The mean age of the sample is 33.32 years and the breakdown of the respondents' ages is indicated in table 3.

**Table 3 Age of respondents**

Age of Respondents	
18 – 29	42.6%
30 – 39	31.0%
40 – 49	15.9%
50 – 59	8.4%
60 – 71	2.0%
	<hr/>
	100.0%
	<hr/>

The survey sample gender composition is 77% male and 23% female, as shown in table 4.

**Table 4 Gender sample composition**



All respondents stated their nationality:

**Figure 4 Sample nationality**

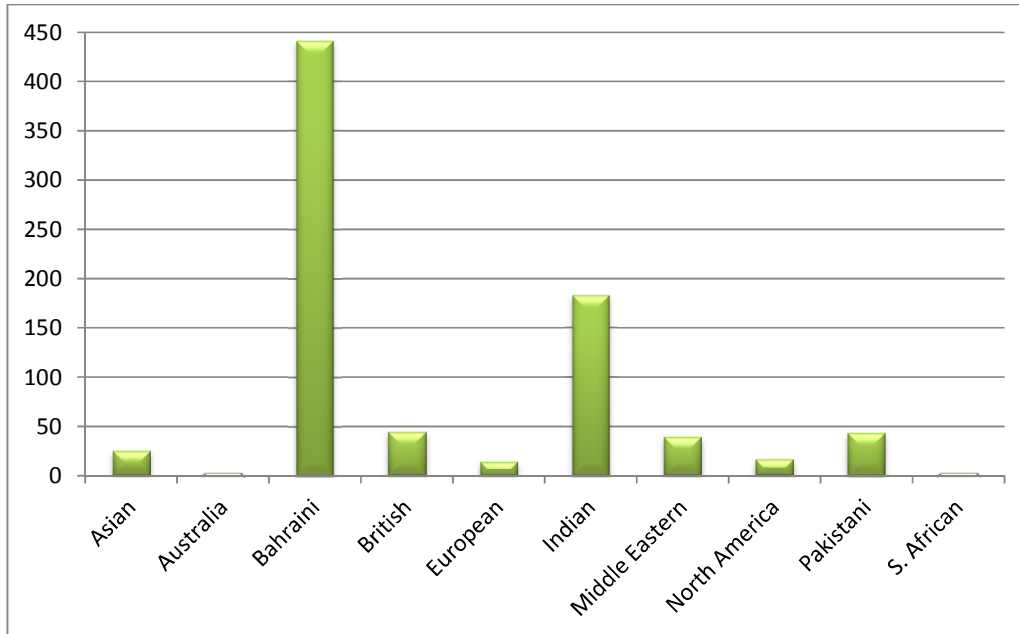


Figure 4 shows that the population that took part in the survey is fairly representative of the general population of Bahrain. According to the Bureau of Near Eastern Affairs (2010) the composition of the population of Bahrain in 2008 (est.) is 1,046,814, including about 517,368 non-nationals with an annual growth rate (2008 est.) as 3.6%. The ethnic composition was Bahraini 63%, Asian 19%, other Arab 10%, Iranian 8%. (<http://www.state.gov/r/pa/ei/bgn/26414.htm>)

In the sample just over half of the respondents are Bahraini (N 441), 183 are from India and the remaining are Asian (N 13), British (N 44), from other Middle Eastern countries (N 7), Pakistani (N 43), North American (N 10), Australian (N 3), South African (N 3) and European (N 2).

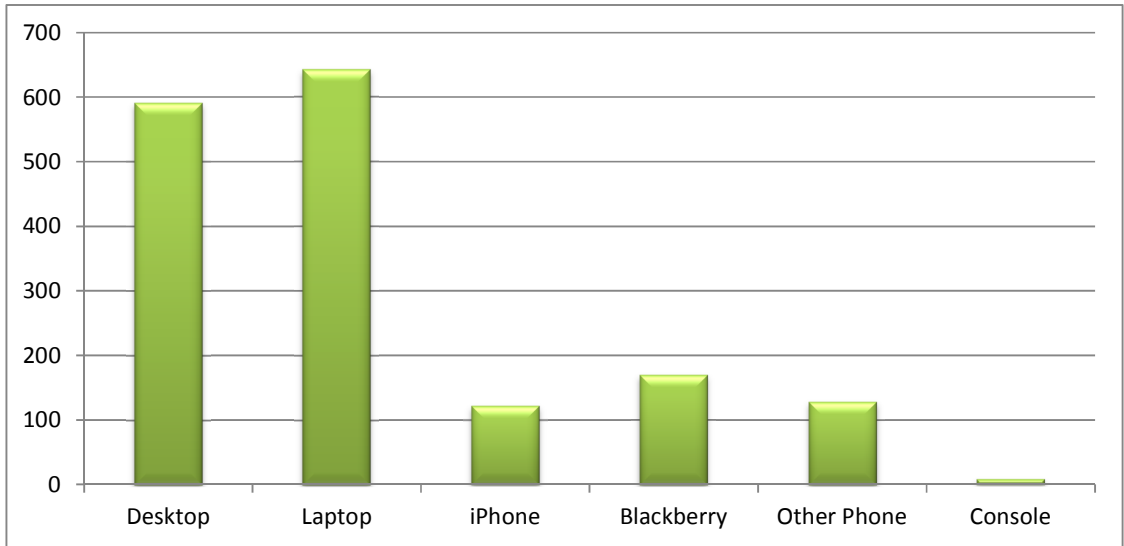
## **7.2 Adult survey findings**

### **7.2.1 How do people connect to the Internet?**

People seem to be more and more mobile, particularly in Bahrain where the population is so diverse. 643 respondents connect to the Internet via a laptop and 591 via a desktop. However, it is clear that the use of iPhones (122), Blackberry (169) and other mobile

devices (128) are becoming increasingly more popular. From figure 5, it is possible to notice that many respondents make use of both portable computers and mobile Internet devices.

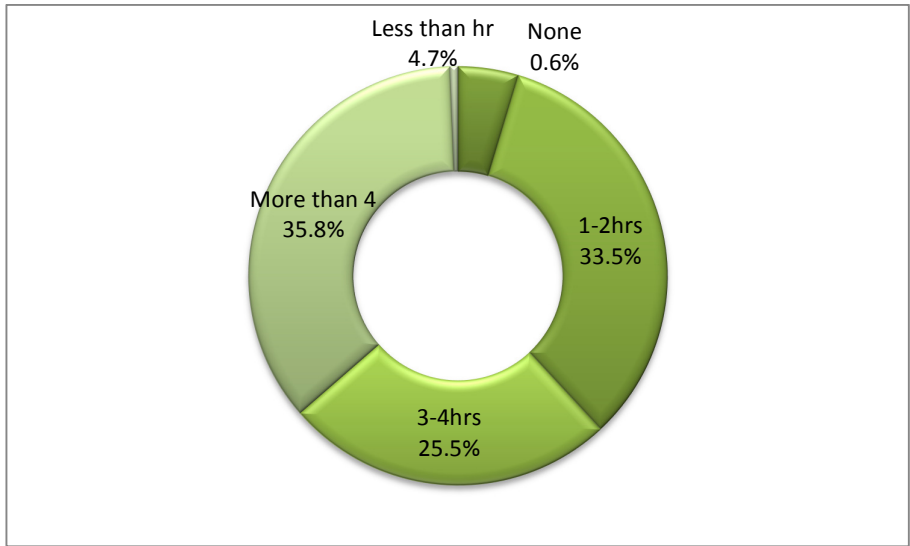
**Figure 5** How people connect to the Internet



**7.2.2 Time spent online**

In the online survey, the majority of people claimed that they spend more than 3 hours online per day (70.3%), which includes time spent at work and at home.

**Figure 6** Time spent online

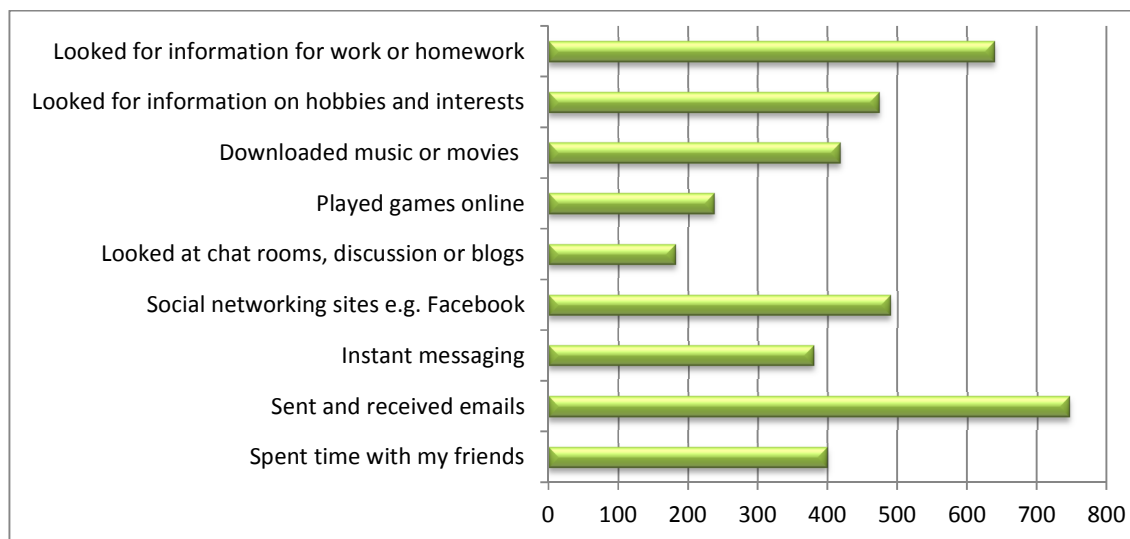


As figure 6 shows, the Internet is part of everybody's life. The great majority of respondents (67.7%) claimed that they spend more than 4 hours on line per day.

### 7.2.3 Online activities

The people who participated in the survey use the internet for a variety of reasons (these are indicated figure 7). The most common reason cited are to: send and receive email (91.4%), look for information for work and homework (78.3%), use Social Networking Sites (SNS) (60.0%), and look for information on hobbies and interests (58.1%) respectively.

**Figure 7 Online activities**



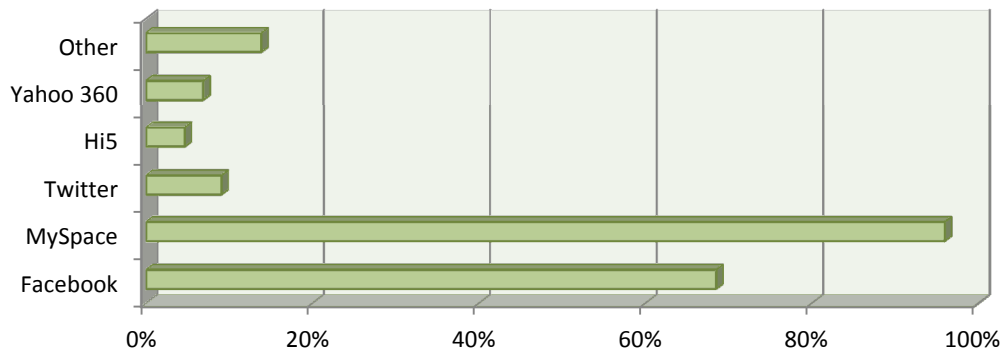
Clearly the Internet, SNS and games are very popular amongst adults and offer a range of opportunities for development but also fun and learning. However, there are concerns over material that might be deemed as potentially inappropriate. This ranges from content (e.g. violence) through to contact and conduct of young people and adults in the digital world (Byron 2008). As a result, a number of questions on safety issues have been included in the survey and are presented later in this report.

### 7.2.4 Use of social networking sites

As shown in figure 8, 100% of respondents use social networking sites with the most popular being MySpace (96%) and Facebook (69%).



**Figure 8 Use of social networking sites**



These findings have been validated by other research (Davidson, Lorenz, and Martellozzo 2010), which shows that instant messaging, online games and doing homework are the most popular online activities.

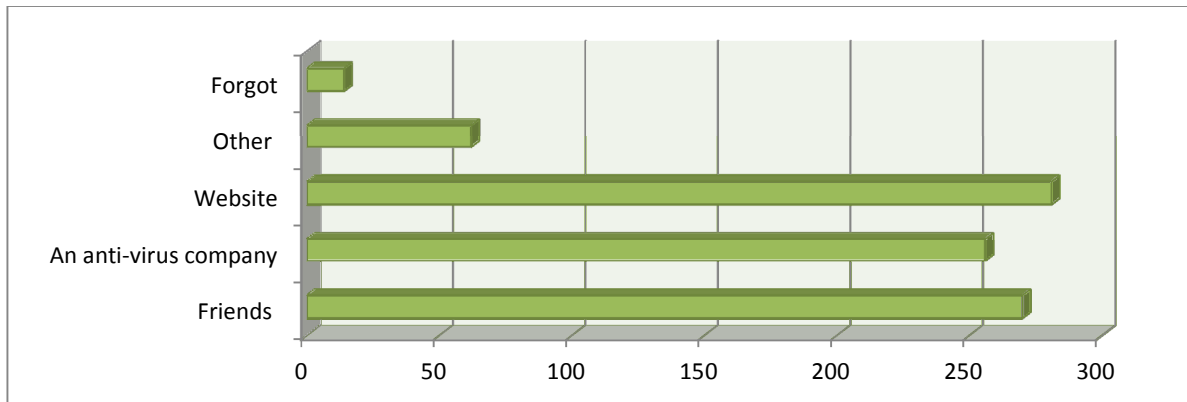
#### ***7.2.5 Internet safety advice received***

60% of the people who participated in the survey say they have had some sort of Internet safety advice. This number is not particularly reassuring when compared to the amount of online experience respondents claim to have (the great majority has over 6 years' online experience). That is to say, adults were aware of online threats, but other research has shown that the extent of their awareness is often strongly correlated with their confidence or experience in using the Internet (NAO, 2010).

The top three sources of advice come from websites, friends or anti-virus companies. Furthermore, when asked if they know about online safety, 44% of respondents claimed to have no knowledge of Internet safety at all. This is of concern considering that the great majority of respondents spend more than 3 hours online per day.

### 7.2.6 Source of advice:

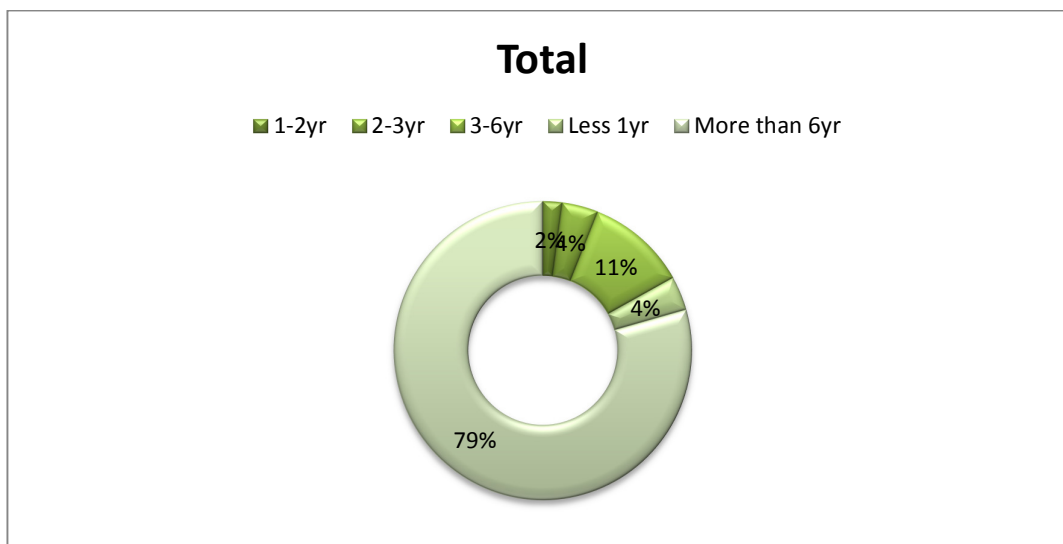
Figure 9 Source of advice



The great majority (79%) of the respondents have more than 6 years' online experience. Only 30 people (4%) claimed to have less than one year's experience. This shows that the population of Bahrain has a rather high level of experience. However, it cannot be assumed that internet safety awareness increases with experience. The results demonstrate that this is not the case.

### 7.2.7 Online experience

Figure 10 Online experience



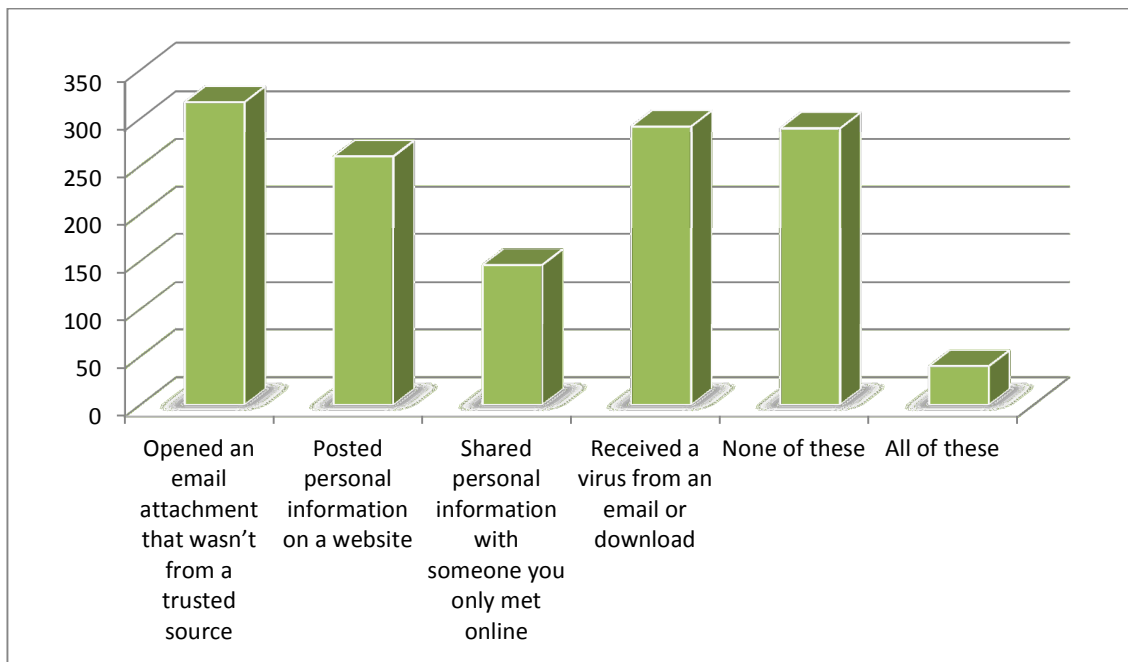
Indeed, when the findings of people with online experience are compared with risk-taking behaviour it becomes clear that the two are not necessarily related. Despite the fact that people have fairly good experience, risk taking behaviour is surprisingly high.

### ***7.2.8 Risk taking behaviour and online negative experience***

This section of the report details the extent to which adults take risks when online, if they had negative experiences, and the extent to which they know how to react to such experiences.

As figure 11 shows, adults seem to take a great number of risks when online at some point in their lives. The most common risk taken is that of opening email attachments that do not come from reliable sources (317), receiving a virus from an email or download (292), posting personal information on a website (260) and sharing personal information with someone they have only met online (146). A total of 290 respondents claimed they did not take any of the risks listed in figure 11.

**Figure 11 Risk taken**

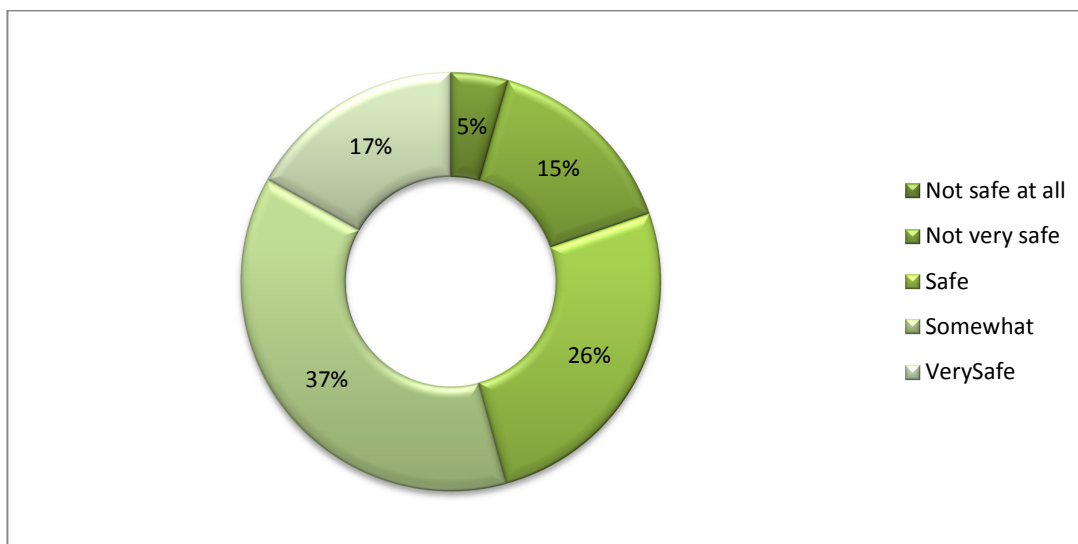


Research conducted by Davidson, Lorenz and Martellozzo (2010) found that people increase their willingness to share personal information depending on whether they have met that person face to face, or whether they only know them online. As there is likely to be far less risk associated with the former than the latter, the analysis in this section focuses largely on sharing of information with strangers. Therefore, the questionnaire asked about sharing of personal information with someone they have only met online and 146 respondents (17.9%) admitted they have done so.

To the question 'have you ever received unwanted messages or material (spam, pornography, indecent messages) from people you know?' the majority claimed that they did (54%). Of these, 21% claimed they did not know how to remove unwanted messages and material from their computer.

Furthermore, despite the fact that the majority of people have received unwanted material, the great majority claimed they feel safe online. As figure 12 suggests, 80% of respondents feel they are somewhat safe to very safe.

**Figure 12 Level of safety**



### **7.2.9 Personal information shared with people online**

From the data set, it is difficult to calculate the overall extent to which people have shared personal details online with people they have met only online. However, it is possible to claim that of the 142 people who have responded that they share personal information, 56% have received internet safety advice.

### **7.3 Adult Survey : Summary of key findings**

- The findings show that Bahrain's adult population internet use is very high and that mobile devices such as iPhones and Blackberrys are becoming increasingly popular.
- The survey shows that many adults have been exposed to some negative online experiences. However, the majority do not have the necessary knowledge to avoid or resolve them.
- Lack of awareness is also highlighted by the high number of adults taking online risks such as opening email attachments that do not come from reliable sources (317), posting personal information on a website (260) and sharing personal information with someone they have only met online (146).
- These results raise a number of concerns:
  - First of all, it shows the need to teach adults and parents to be aware of the risks they and ultimately their children can be exposed to online.

- Secondly, it shows the need for people to be able to depend upon reliable information sources about online safety.
- When asked where they learnt about safety, most people were found to rely on various sources which were not necessarily reliable (e.g. friends, the internet, websites).
- However, according to research conducted by the UK's National Audit Office (2010) on the Get Safe Online website, people who are less confident about Internet use are those who are less knowledgeable about internet security. Most of the less confident users liked to be able to rely on a reassuring and friendly website.
- It can be argued that people who can consult a reliable website will become more confident about their ability to be safe online and expanded the range of activities they carried out online.
- It can also be argued that people who receive internet safety training may be able to transfer their knowledge to others, particularly their children, and further appreciate the extraordinary opportunities that the internet and other technologies offer.

## 8. Findings: Child Survey and Focus Groups

This section presents findings from the online child survey conducted in schools with a stratified sample (by age, gender, religion and school sector) of 2558 respondents aged 11-18 , the qualitative focus groups (29) also conducted in schools with respondents aged 7-18 and a small number of interviews conducted with teachers (30). The findings from the survey are largely validated by the child focus group findings and data are presented under key headings: Online behaviour; online activities; parental supervision and online safety; behaviour on social networking sites and posting personal information; risk taking and unpleasant online experience; online safety training and advice. The findings from the teacher interviews are presented at the end of the section along with a summary of key findings. Key themes are presented in this section.

### 8.1 Online Child Survey Sample

This survey sought children's views and experiences about the way in which they use the Internet, their online experience and knowledge about safety issues. Eight schools were selected for inclusion in the survey on the basis of their demographic mix. The participating schools included:

**Table 5 Schools participating in the survey**

Name of School
British School of Bahrain
Al Noor International School
Isa Town Middle Boys Intermediate School
Al Hidayah Boys Secondary School
Umm Salamah Middle Girls Intermediate School
Hamad Town Secondary Girls School
St Christopher's School
The Indian School

Most schools were generally willing to participate, however public schools showed less willingness to participate because some pupils were sitting their final exams. The public schools achieved a total sample size of 1143 and the private school sample was 1415. Therefore, the total sample was 2558 which meets the required standard needed to address the study aims (see the methodology chapter for a more detailed sample description). The participating schools formed a representative sample in terms of the following criteria: Private and public sector (social class); gender; age; ethnicity.

### **8.1.2 Sample Characteristics: Online Survey**

The gender split of the sample was skewed towards males, 61% of the sample was male and 39% female, it proved difficult to secure survey participation in some female public schools. The largest group of respondents were Bahraini comprising 63% in total. 80% (2044) of the sample stated that they were Muslim, 13% Christian, 3% Hindu and 4% selected 'other religion'.

The majority of the sample fell in to the 11-13 (44%) and 14-16 year (45%) age groups. A considerably smaller number of 17-18 year olds (11%) participated in the study (Table 6). The majority of the respondents were Muslim (80%), comprising the largest respondent group from both school sectors. The second largest group were Christians (13%), unsurprisingly all of whom were in the private school sector (Table 6), the sample was split almost equally between private (55%) and public school (45%) respondents. Boys were however over represented in the public school data (70%) but not significantly in the private school data (53%).

**Table 6 Age and Gender**

	11-13 years	14-16 years	17-18 years
<b>Male</b>	621	785	143
	56%	69%	47%
<b>Female</b>	495	353	160
	44%	31%	53%
<b>Total</b>	1116(44)	1138(45)	303(11)
	100%	100%	100%

**Table 7 School Sector and Religion**

	Muslim	Christian	Hindu	Other
<b>Public</b>	1127	5	4	7
	99%	0	0	1%
<b>Private</b>	917	340	60	97
	65%	24%	4%	7%
<b>Total</b>	2044	345	64	104
	80%	13%	3%	4%

## 8.2 Focus Group Sample

The aim of the qualitative interviews was to explore young people's experience and awareness of Internet use and Internet /other digital media safety.

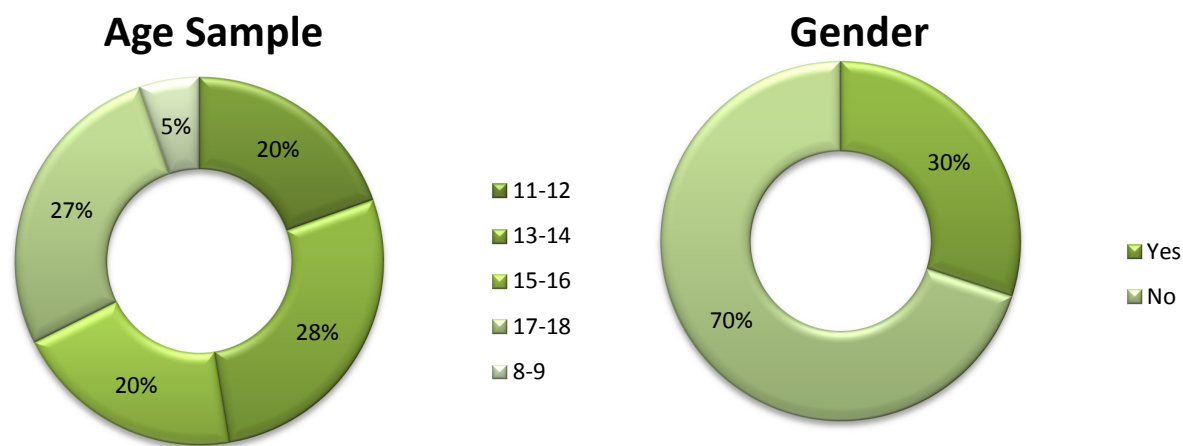
### 8.2.1 Sample Characteristics: Child Focus Group Sample

The focus groups sample consisted of 133 young people across the Kingdom of Bahrain aged 8-18. The sample gender composition is 68 girls and 65 boys (Figure 13). The data from the focus groups is presented by school category (private, public boys and public



girls). General themes are included along with qualitative counts, a smaller number of private school children participated in the focus groups and it was therefore not viable to produce counts by gender for this group.

**Figure 13 Focus Group Sample Composition: Age and Gender**



It is important to stress that the extent to which the findings from this element of the research can be generalised is limited given the small sample size. As a result, the focus group findings have been compared to those from the survey to increase the validity of the data.

Seven schools were selected for inclusion in the focus groups on the basis of their demographic mix. The participating schools included:

**Figure 14 Schools participating in the focus groups**

Name of School
British School of Bahrain
Al Noor International School
Isa Town Middle Boys Intermediate School
Al Hidayah Boys Secondary School
Umm Salamah Middle Girls Intermediate School
Hamad Town Secondary Girls School
The Indian School

Most schools were generally willing to participate. The public schools achieved a total sample size of 103 (50 boys and 53 girls) and the private school sample totalled 30.

### 8.3 Child Survey and Focus Groups Findings

#### 8.3.1 Online Behaviour

The survey data demonstrates that the amount of time spent online varied little by gender but there was some variation by age, with 39% of 11-14s spending 4 or more hours online each day compared to 32% of 14-16s and 23% of 17-18s, the mean average amount of time spent online each day was approximately 2.5-3 hours (with a low standard deviation of 1.61). The mean time spent on line every day did not vary significantly by private and public school sector (Table 8) or by nationality (Table 9), children at private schools spent a mean average of 2.42 hours online every day compared to children in the public school sector who spent a mean average of 2.56 hours online each day.

**Table 8 Time Spent Online x School Sector**

	Private Schools	Public Schools
<b>Less than an hour</b> <b>[0.5 hr]</b>	205	175
	14%	15%
<b>One to Two hours</b> <b>[1.5 hrs]</b>	532	340
	38%	30%
<b>Three to Four hours</b> <b>[3.5 hrs]</b>	290	177
	21%	15%
<b>More than four hours</b> <b>[5 hrs]</b>	219	226
	15%	20%
<b>Total (where response)</b>	1246	918
	100%	100%
<b>Mean [In Hrs]</b>	2.48	2.58

<b>S.D</b>	1.61	1.66
------------	------	------

**Table 9 Time Spent Online x Nationality**

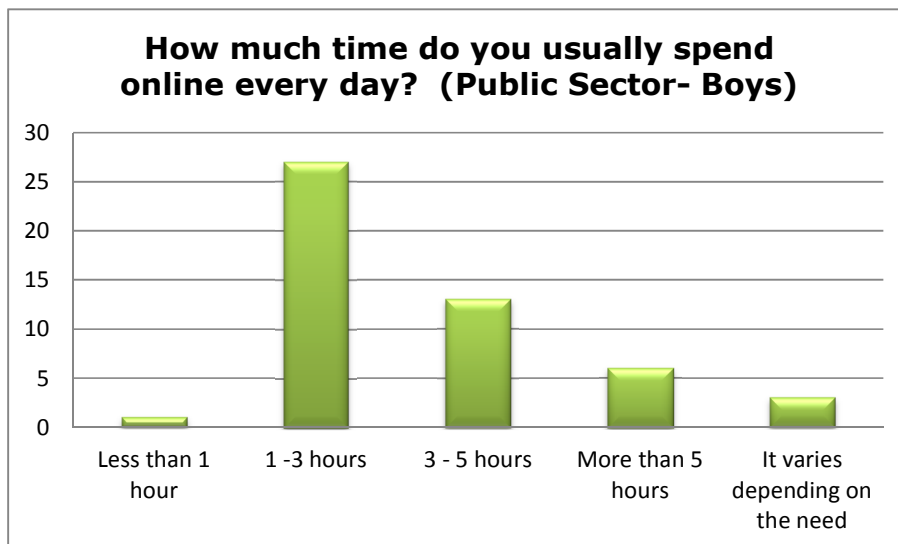
	Total	Nationals	Expat Arabs	Expat Asians	Others
<b>Less than an hour [0.5 hr]</b>	380	228	21	60	71
	15%	14%	14%	21%	14%
<b>One to Two hours [1.5 hrs]</b>	872	504	63	103	202
	34%	31%	41%	37%	40%
<b>Three to Four hours [3.5 hrs]</b>	467	289	35	48	95
	18%	18%	23%	17%	19%
<b>More than four hours [5 hrs]</b>	445	313	19	34	79
	17%	19%	12%	12%	16%
<b>Total</b>	2557	1615	155	281	506
	100%	100%	100%	100%	100%
<b>Mean [In Hrs]</b>	2.48	2.58	2.34	2.13	2.38
<b>S.D</b>	1.61	1.66	1.47	1.53	1.55

The findings from the focus groups support the survey data. All children, from both the public and private school sectors use the Internet every day and spend an average of 3.5 hours online. Young people's daily time spent online is indicated at Figures 15, 16 and 17.

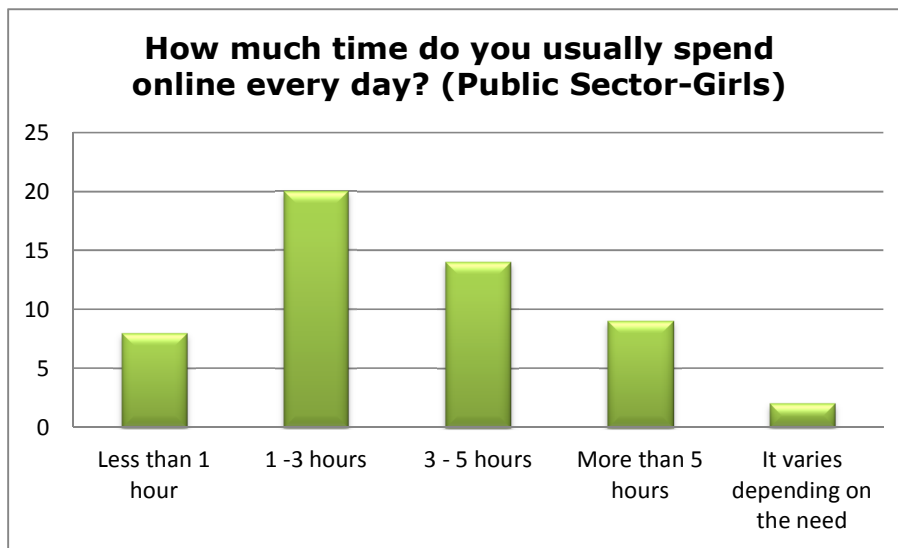
**Figure 15 Time Spent Online: Private School Sector**



**Figure 16 Time Spent Online: Public School Sector (Boys)**



**Figure 17 Time Spent Online: Public School Sector (Girls)**

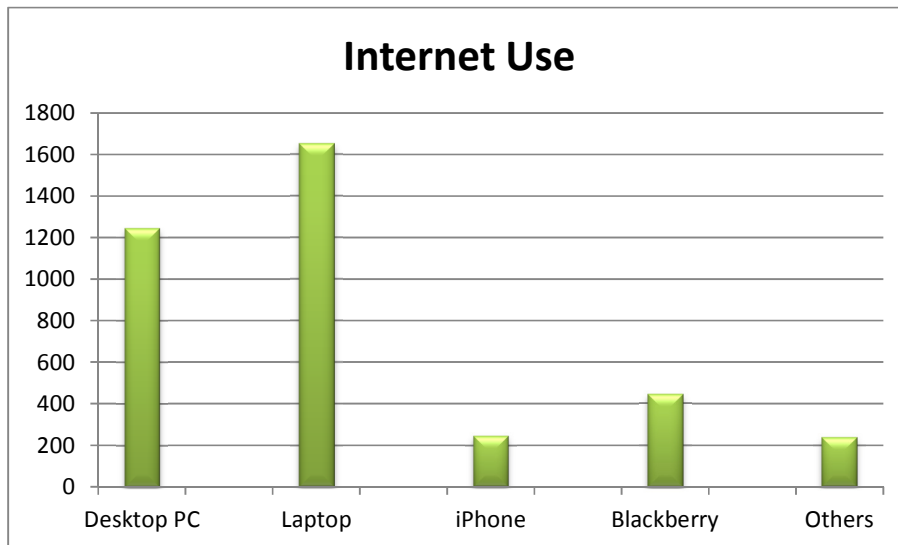


However, it is interesting to note that the majority of the respondents from the private school sector use the internet more than 5 hours a day, whilst public sector respondents tended to use the internet every day for an average of 2 hours. This may indicate that children going to public schools have a lower level of Internet access than those who attend private schools. This finding is consistent with data regarding young people's online activity from Europe (Livingstone and Haddon 2009).

Survey data indicates that the majority of respondents accessed the Internet predominantly via a desktop PC (49%) or via a laptop (65%), 27% accessed the Internet via an iPhone or Blackberry device. There were no significant gender or age differences regarding means of access, children in the younger age group (28% of 11-13 year olds) were slightly more likely to access the Internet via mobile phones than children in the older age group (26% of 14-16 year olds) (Figure 18).

This finding is supported by the qualitative data which shows that, the majority of young people have at least one mobile device, for example iPhone or Blackberry that allows them to connect to the Internet anytime, particularly where a wireless free network is available.

**Figure 18 Internet Access**



#### **8.4 Online Activities**

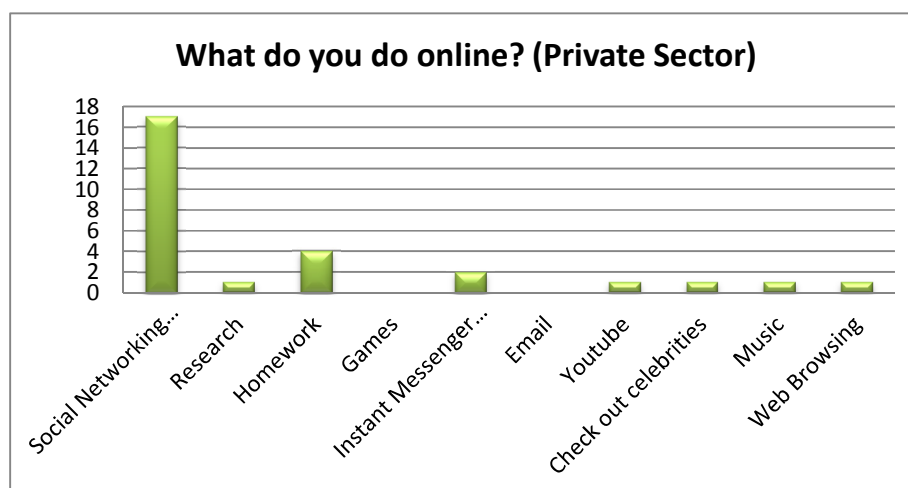
Survey data suggests that online activities also varied little across groups with most children using the Internet to communicate with friends (62%), send emails (44%) do research (43%), download music and films (48%), play games (44%) and for instant messaging (32%). There were no significant gender differences in terms of online communication: boys were just as likely as girls to use the internet to communicate with friends (61% and 62% respectively). Girls were more likely to use instant messaging (40% compared to 26% of boys) and were less likely than boys to play online games (36% of girls compared to 50% of boys). There were no significant differences in online activity by age group, but the older groups were slightly more likely to communicate with friends and to send emails (Table 10).

**Table 10 Online Activities x Gender and Age**

	Male	Female	11-13	14-16	17-18
<b>Spent time with friends</b>	949	624	626	731	216
	61%	62%	56%	64%	71%
<b>Sent emails</b>	632	419	488	480	163
	41%	50%	44%	42%	54%
<b>Instant messaging</b>	400	406	370	332	104
	26%	40%	33%	29%	34%
<b>Updated profiles</b>	651	505	532	490	47
	42%	50%	48%	43%	16%
<b>Posted in chat rooms</b>	188	107	124	87	31
	12%	11%	11%	8%	10%
<b>Played games</b>	767	359	593	423	110
	50%	36%	53%	47%	36%
<b>Research</b>	591	498	492	445	152
	38%	49%	44%	39%	50%

Generally, it can be said that the majority of the young people who participated in the qualitative study use Social Networking Sites (SNS). The most common are Facebook, Bebo, MSN and online games. A higher number of private sector respondents use social networking sites (Figure 19) than public sector, 45% of the public sector do not own an account on such a site.

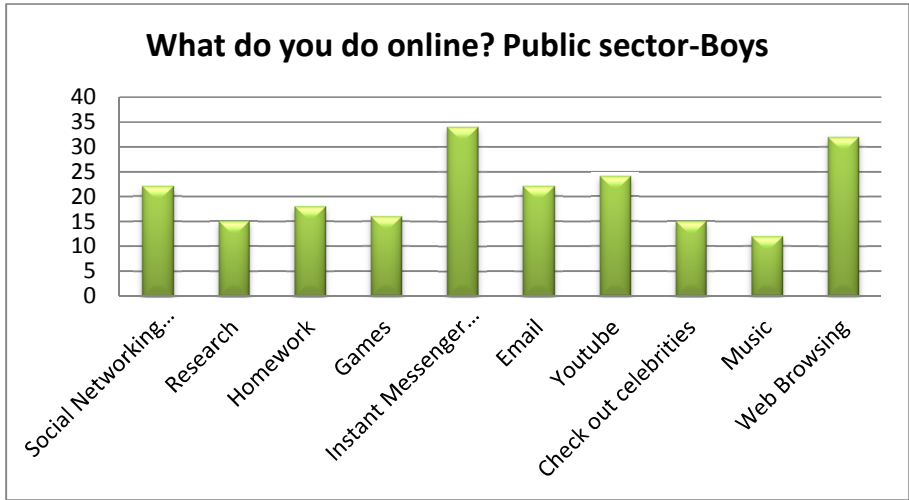
**Figure 19 Online Activities (Private School Sector)**



Furthermore, what also emerged from the qualitative data is that the majority of the private sector respondents used the internet for social networking whereas the public sector respondents used the internet on a wider basis for games, YouTube and homework and music, for example. Moreover, as the data below indicates, girls from the public sector are bigger users of social networking sties and messenger than boys from the same sector.

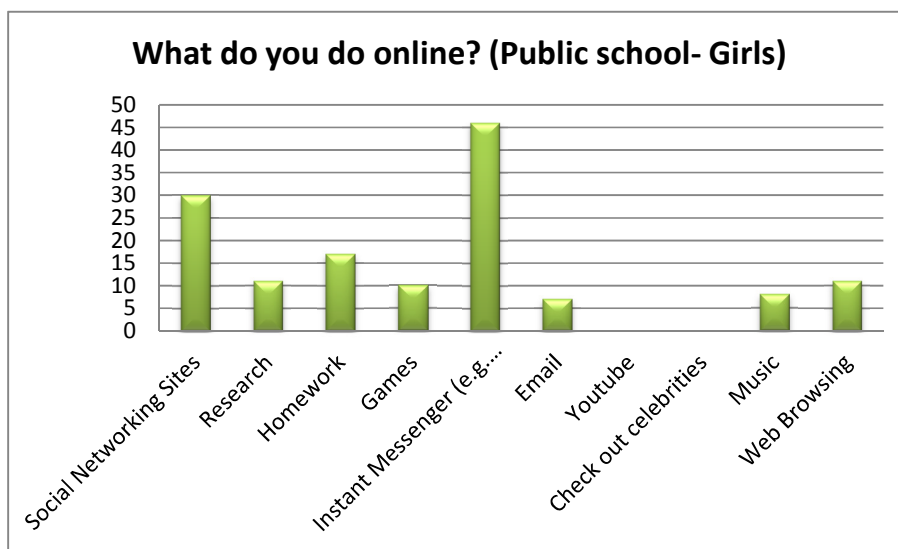
Girls from the public sector are more likely to use the internet for socialising. While boys are more likely to play games online and investigate things they’re interested in (Figure 20), girls are significantly more likely to use instant messaging, send and receive emails and visit social networking sites, chat rooms or blogs (Figure 21).

**Figure 20 Online Activities Public School Sector (Boys)**



**Figure 21 Online Activities Public School Sector (Girls)**





This potentially puts girls at higher risk of coming to harm online, as they engage in online activities that enable grooming or bullying to take place more frequently than boys. This finding is consistent with other research conducted in the United Kingdom (Davidson, Lorenz, and Martellozzo 2010), however the survey data indicates that girls are more likely to take action in response to such an approach.

This is a very important finding which was validated by other data in this report (see the interviews with stakeholder's findings for example). Furthermore, findings from the focus groups suggest that young people are very attracted to SNS and having a long list of friends. When this question was asked, it was clear that there is a competition amongst some children regarding the highest number of friends.

As this pupil claimed:

*"It is almost like a competition who has the most friends so you keep adding" (FG15)*

#### **8.4.1 Parental Supervision & Online Safety**

The majority of respondents claimed that they were allowed unsupervised access to the Internet (85% of males and 90% of females) (Table 11). Approximately half of the sample (48%) claimed that their parents 'always' knew what they were doing online (Table 12). There was little variation by gender, age, religion, nationality, private or public school sector. The majority claimed that their parents sometimes or never knew what they were doing online (52%).

**Table 11 Allowed Unsupervised (by an adult) Internet Access: Gender**

	Gender		Age		
	Male	Female	11-13 years	14-16 years	17-18 years
<b>Yes</b>	1312	910	987	973	262
	85%	90%	88%	86%	86%
<b>No</b>	237	98	129	165	41
	15%	10%	12%	14%	14%
<b>Total</b>	1549	1008	1116	1138	303
	100%	100%	100%	100%	100%

**Table 12 Parental Knowledge about Child's Online Activity x Gender & Age**

		Gender		Age		
		Male	Female	11-13 years	14-16 years	17-18 years
	<b>Total</b>					
<b>Always Know</b>	1222	682	540	594	501	127
	48%	44%	54%	53%	44%	42%
<b>Sometimes know</b>	1146	722	424	457	537	152
	45%	47%	42%	41%	47%	50%
<b>Never know</b>	189	145	44	65	100	24
	7%	9%	4%	6%	9%	8%
<b>Total</b>	2557	1549	1008	1116	1138	303
	100%	100%	100%	100%	100%	100%

The focus group findings indicate that when the children were asked whether they tell their parents about their online activities, a large number of young people from the private sector claim that they do not inform their parents what they do online (Figure 22), whereas the majority of the public sector do (Figure 23 and 24).

Figure 22 Online Activities Discussed with Parents: Private Sector

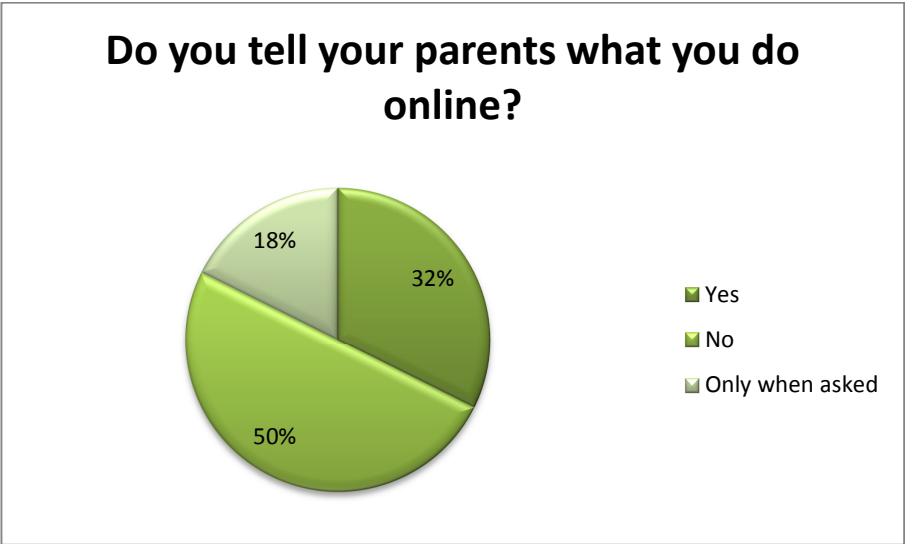


Figure 23 Online Activities Discussed with Parents: Public School Sector (Boys)

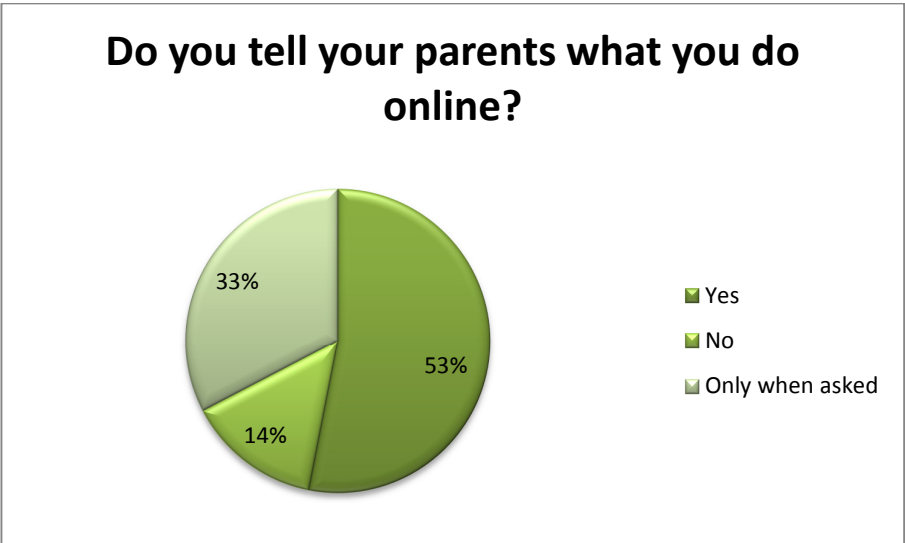
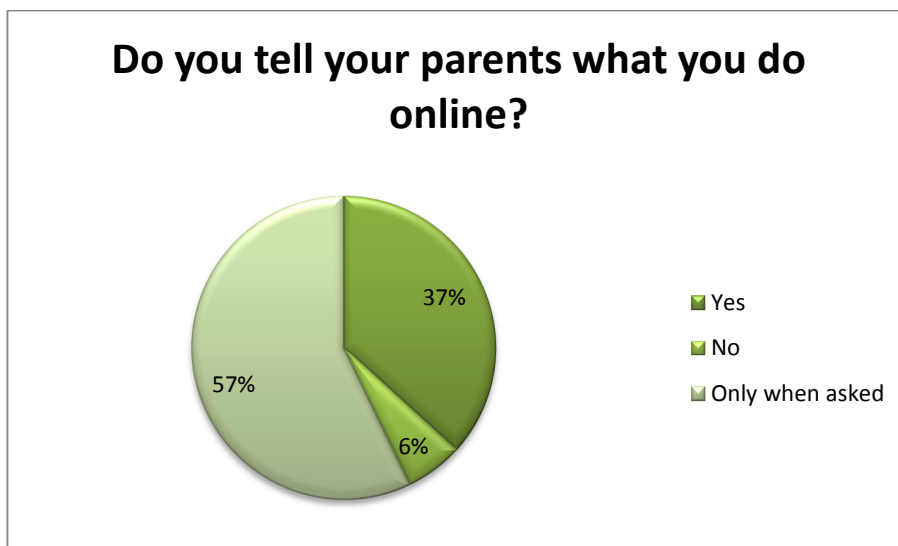


Figure 24 Online Activities Discussed with Parents: Public School Sector (Girls)



Some of the respondents claimed:

*'My parents ask what I do online but I lie anyway' (Child 1)*

*'I don't tell my parent everything I do, but I don't do anything wrong' (Child 2)*

There is an element of confidence evident from these young people's quotes. Children feel generally confident and safe when they use the internet and this sense of security is fostered by the very nature of the internet where people feel physically disconnected from the real world and as a result safer. This finding is confirmed by the survey data.

To the question "do your parents ask what you do online?" the majority of children suggested that parents do not enquire what they are doing, this applied across both public and private sectors (Figures 25, 26, 27).

*'It is a big mistake being friends with your parents on Facebook. My mum is a friend of mine on Facebook and she is always checking on me and my friends' (Child 3)*

*'I only tell my parents if they ask me, otherwise I keep it to myself' (Child 4)*

*"No ,they know that I take care of myself"( FG1)*

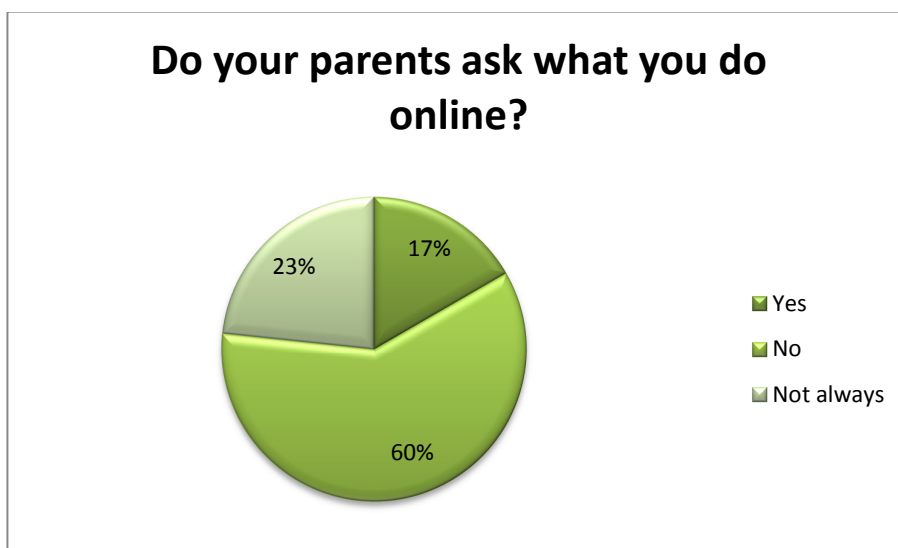
*"I discuss things with my dad"(FG4)*

*"My parents very rarely check; they leave me alone to do what I need to do"*  
(FG6)

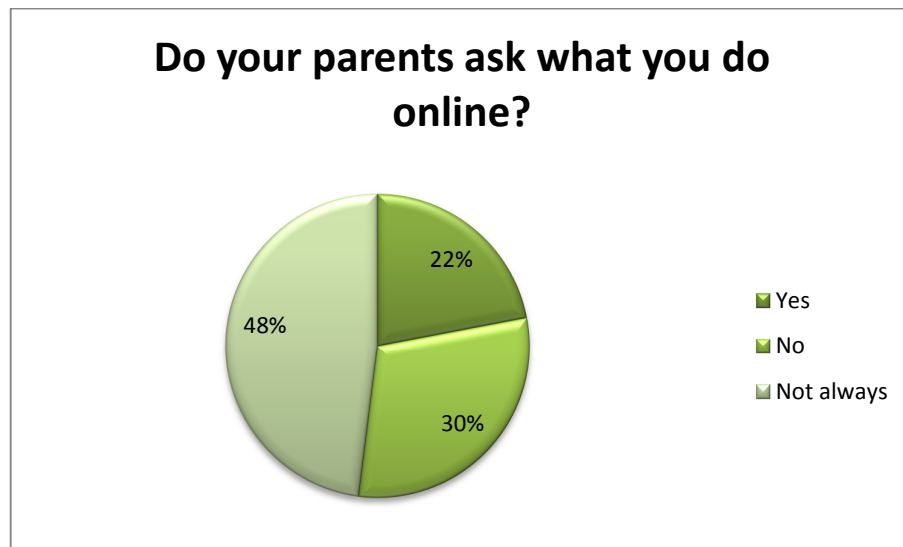
*"They don't really ask but I don't hide anything from them"* (FG6)

As the quotes above highlight, children are not keen to share their online activities with their parents; they enjoy the privacy and freedom that the Internet affords. Those that share their information with their parents, do not do so voluntarily but because their parents ask.

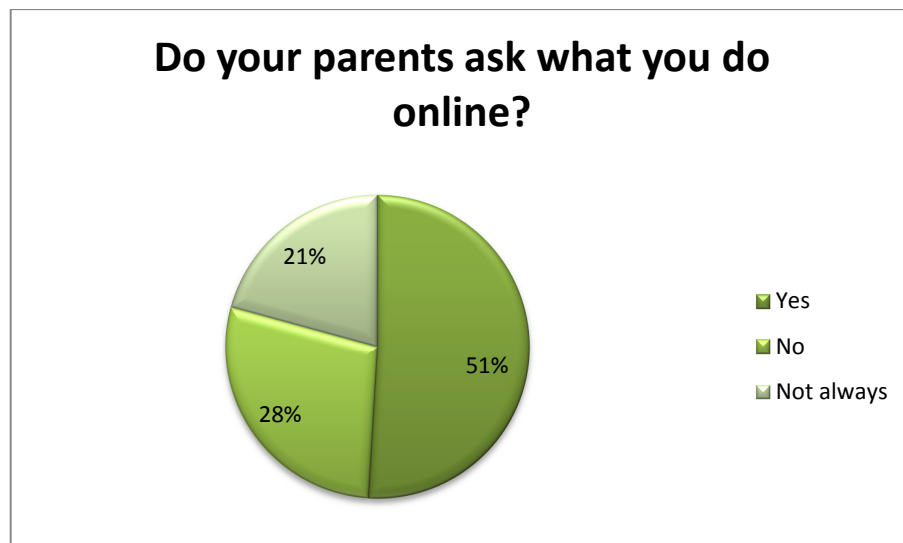
**Figure 25 Do Parents Ask What Children Do Online? Private School Sector**



**Figure 26 Do Parents Ask What Children Do Online? Public School Sector (Boys)**



**Figure 27 Do Parents Ask What Children Do Online? Public School Sector (Girls)**



It is interesting to note however, that the girls' studying in public schools appear to be the most supervised group. More than half of the girls' parents enquire of their online activities.

Pupils were asked where they keep their computer in the house. The majority of children were allowed to keep a computer in a private place such as their bedroom (60%) rather than a common area such as the living room (24%).

*"We have many computers so they are everywhere in the house" (FG1)*

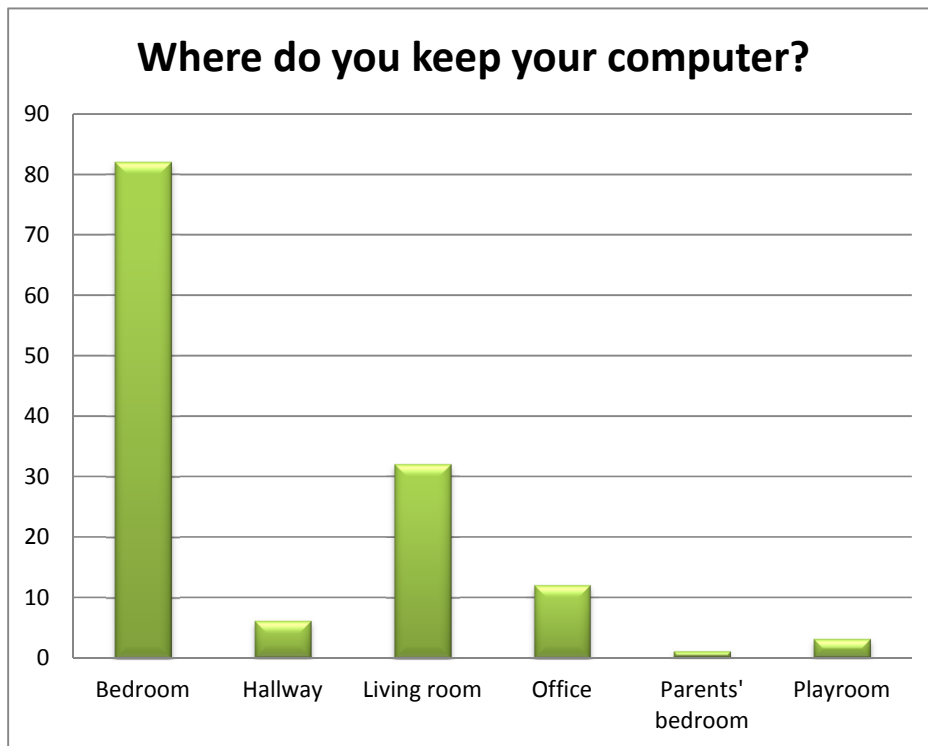
*"I have my laptop in my room. Everyone in the house has a laptop" (FG4)*

*"I keep mine in my bedroom" (FG5)*

*"I have my laptop in the bed room and the computer in the Majlis" (FG6)*

The total number of responses have been summarised in Figure 28.

**Figure 28 Location of Computer**



To the question "what do you know about staying safe online?" all children from both public and private sectors raised some valuable messages:

*"I have software which protects me against all viruses and software that blocks anything" (FG1)*

*"Not to use unprotected programs and avoid suspicious sites" (FG2)*

*"I don't log into any site I don't know, because there are mails which have viruses" (FG4)*

*"I should not answer any person I don't know in the messenger" (FG5)*

*"Not to log in chat programs and not to talk to a person I don't know" (FG6)*

*"This is the first time I have heard about it" (FG8)*

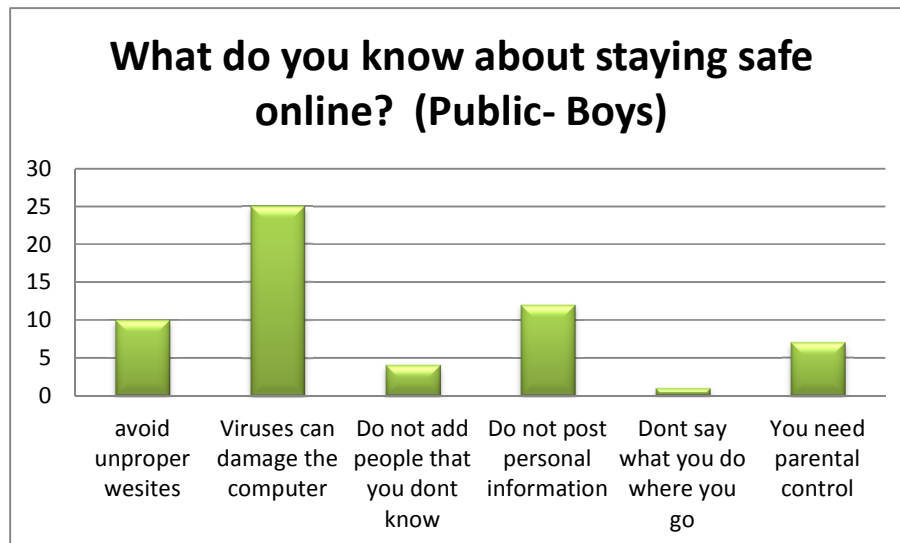
*"Viruses are the most fearful thing" (FG13)*

**The key themes are summarised below:**

- 1) Viruses can damage your computer**
- 2) Do not add people you don't know to your social networking sites**
- 3) Don't say what you do and where you go to people you don't know**
- 4) Avoid certain websites**
- 5) Parental control is important**

However, findings suggest that girls from the public sector are more aware of some of the risks they may face online, such as posting personal information, posting what they do and where they go, than boys (Figure 29). As illustrated in Figure 29, boys' major concern is viruses that may damage their computer.

**Figure 29 Knowledge About Online Safety: Public School Sector (Boys)**

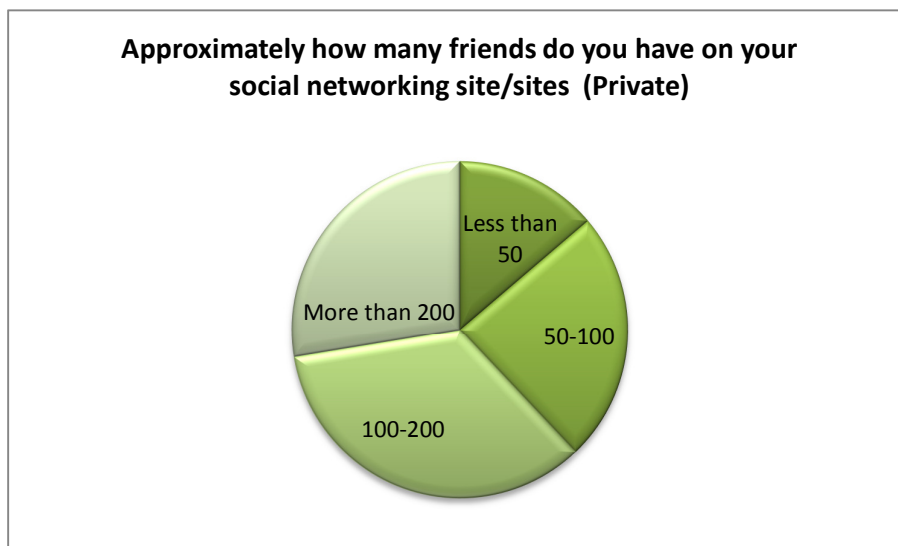




## 8.5 Behaviour on Social Networking Sites and Posting Personal Information

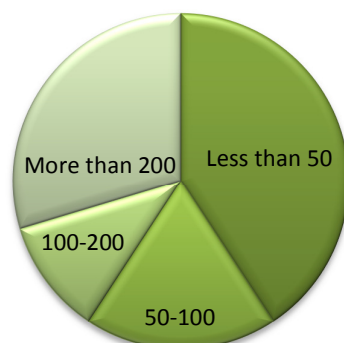
As discussed earlier in this report, the great majority of children use SNS to interact with friends and family and to make new friends. The qualitative findings indicated that the majority of the respondents used more than one form of SNS and had more than one profile. All children from both the private and public sector are extremely popular on SNS. As the graphs below shows, the qualitative data indicates that the great majority have more than 50 friends who have access to their profile. When this issue was probed during interviews, it was found that young people liked to have a large list of people in their SNS, even if they did not know all of them (Figures 30, 31, 32).

**Figure 30 Friends on Social Networking Sites: Private School Sector**



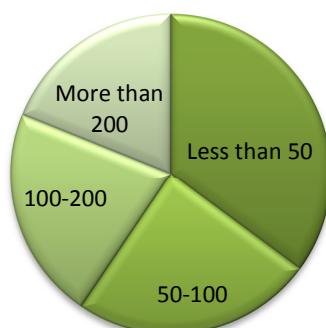
**Figure 31 Friends on Social Networking Sites**

**Approximately how many friends do you have on your social networking site/sites (Public- Boys)**



**Figure 32 Friends on Social Networking Sites: Public School Sector (Girls)**

**Approximately how many friends do you have on your social networking site/sites (Public- Girls)**



When asked the question “what information do you include in the profile?” it emerged that the majority of the public sector share more detailed information such as personal pictures, current school they attend than the private sector respondents and have less awareness about privacy settings on SNS.

Some children from the private school claimed:

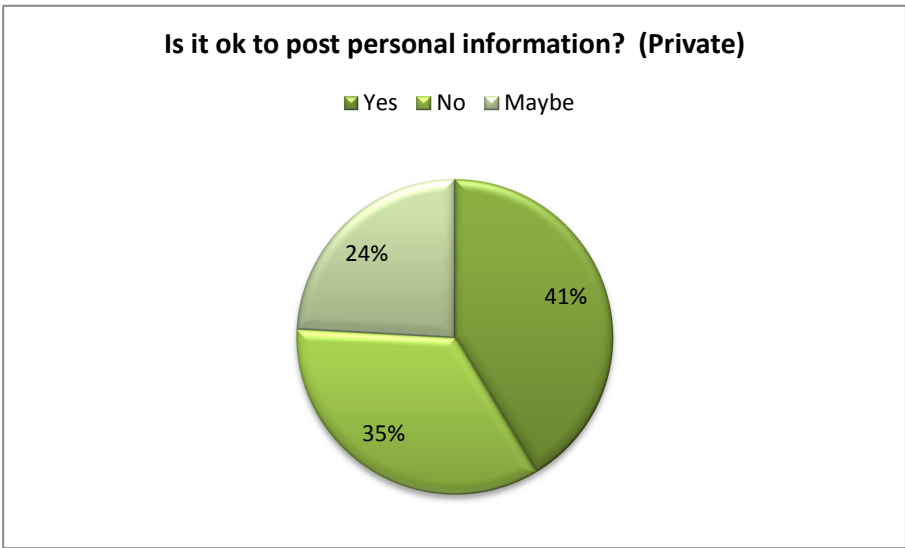
*‘I put my real name and family name and the e-mail and not the number. I put a photo of me and my birth date and nationality.’ (Child 13)*

*'I have included my name, email, date of birth, school name, photo, everything of me' (Child 12)*

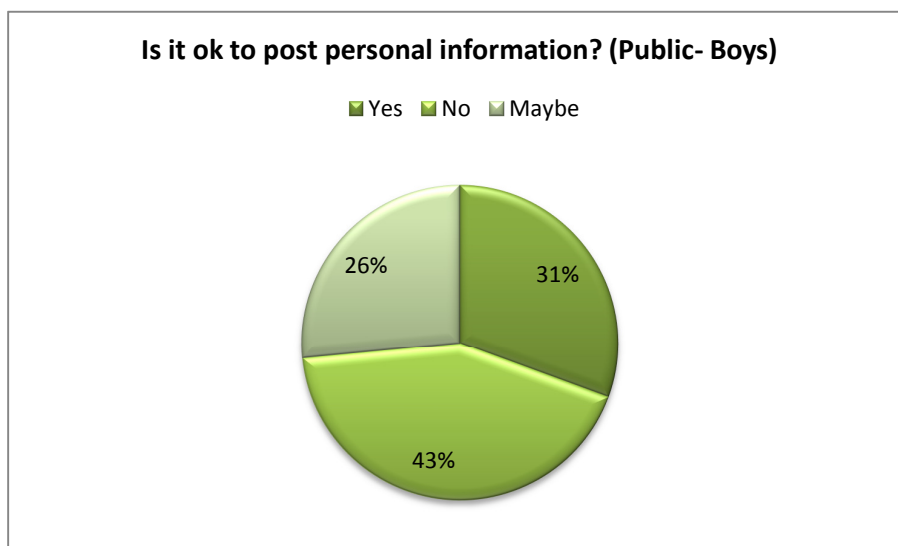
*'I only put my email, date of birth and the school but I don't put my personal email' (Child 5)*

The percentage of the children that would post personal information on their public profile is indicated at Figures 33, 34 and 35.

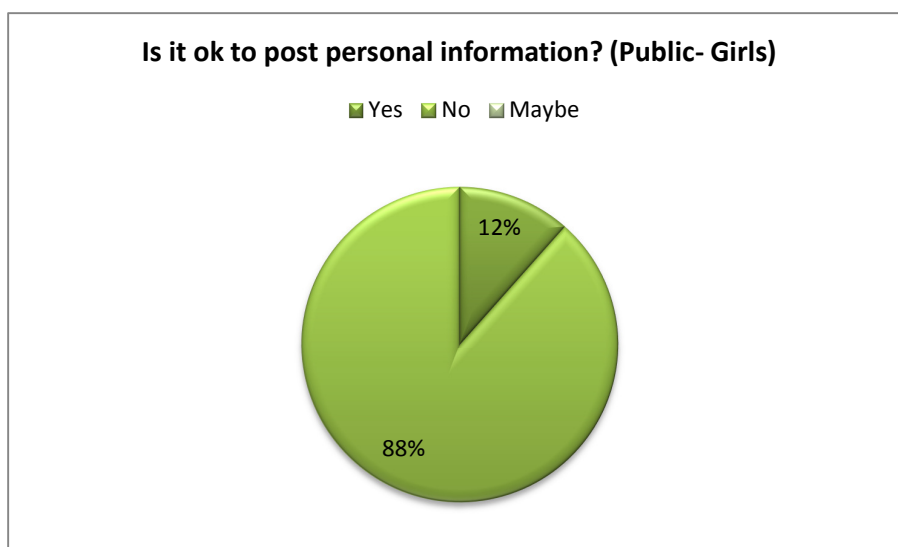
**Figure 33 Posting Personal Information Private School Sector**



**Figure 34 Posting Personal Information: Public School Sector (Boys)**

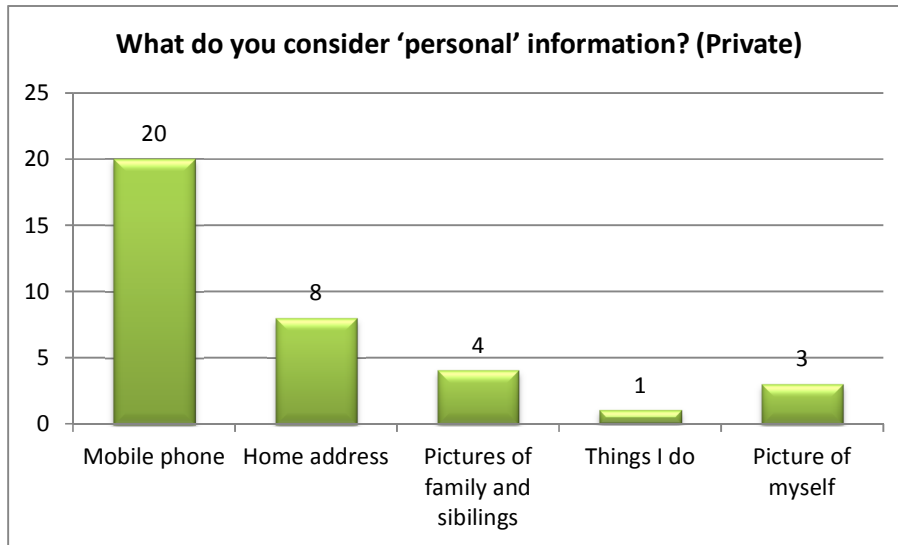


**Figure 35 Posting Personal Information: Public School Sector (Girls)**

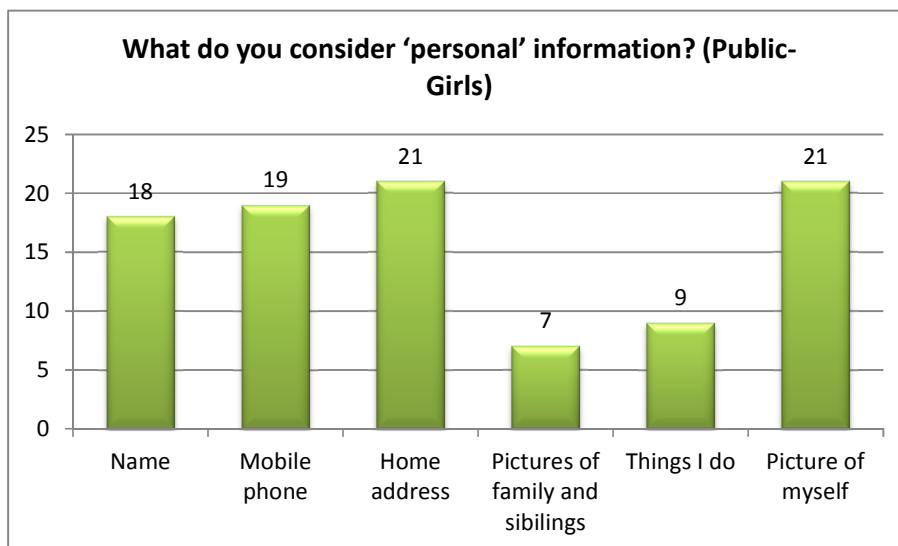


The qualitative data indicates that girls from private sector schools are more conservative in posting personal information than boys. 88% of girls would not post personal information; whereas 31% of the boys said that they would and 26% that they might. This finding was contradicted by the survey findings which indicated that girls attending public schools were highly risk taking. Overall, it can be argued that in both private and public sector schools there is a lack of awareness regarding what is considered personal information and what is not. The data presented at Figures 36, 37 and 38 indicate what young people regard as personal information.

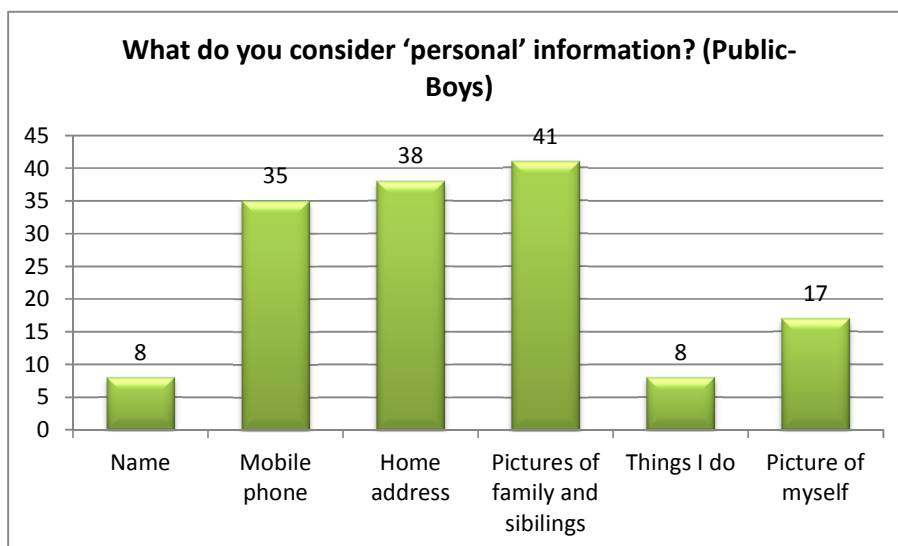
**Figure 36 What is considered to be 'personal information'? (Private School Sector)**



**Figure 37 What is considered to be 'personal information'? (Public School Sector- Girls)**



**Figure 38 What is considered to be 'personal information'? (Public School Sector-Boys)**



The qualitative data indicates that most children would freely post on their SNS profile what they do or where they are everyday. A small number for each sector consider posting what they do as personal information whereas none of the young people interviewed considered that posting where they are to be posting personal information. Furthermore, a significant number of young people had their public profile set to public and did not know how to set it to private. When this issue was probed, it was clear that there was less awareness amongst public school children. This is indeed concerning. Mobile devices such as iPhones and Blackberries allow people to update their status every minute of the day making them constantly traceable and possibly vulnerable.

Amongst the things that young people are not aware of is the lack of understanding of the risk posed by wide internet accessibility available through mobile phones. This issue should be reinforced more in schools. It is imperative to teach people that using the internet on mobile phones can be as 'high risk' as being online at their computer at home. It appears that young people associate the term 'online' strictly with the computer. They do not associate the term 'online' to apply when they use a mobile phone to check, for example, their Facebook page or to chat on MSN.

### **8.6 Risk Taking and Unpleasant Online Experience**

Findings from children' interviews show that the great majority of children across both sectors add people that they have never met before to their lists. These numbers, indicated at Figures 39, 40 and 41, are particularly high for both the private sector (76%) and for girls studying in private schools (76%).

Figure 39 Online Strangers Added to Social Networking Sites: Private School Sector

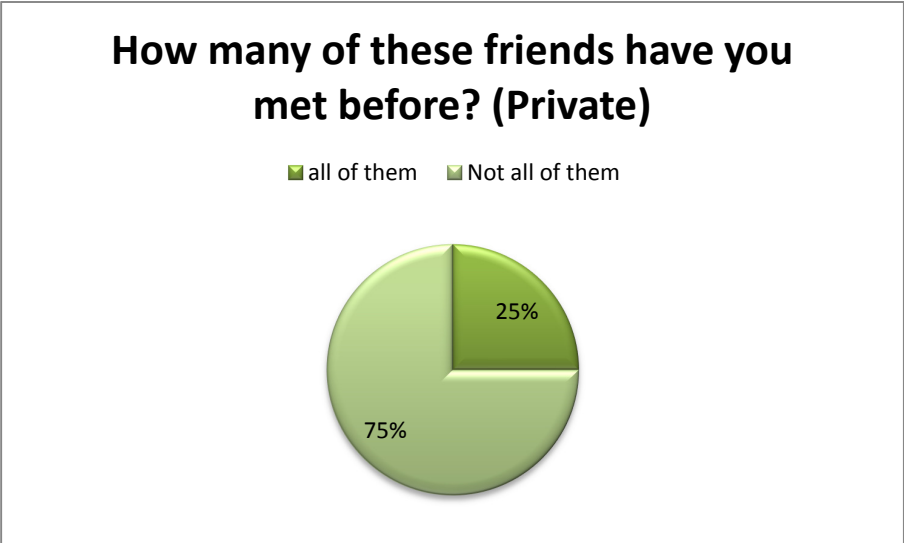
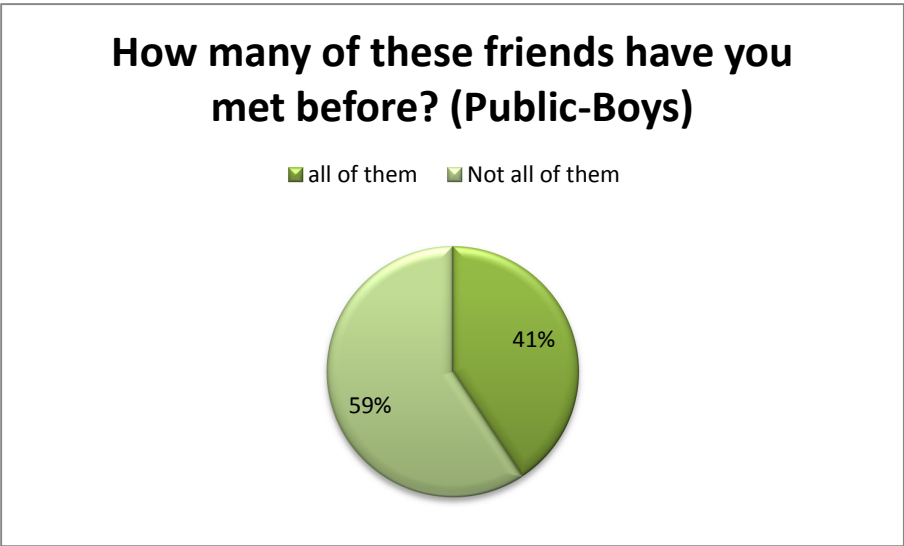
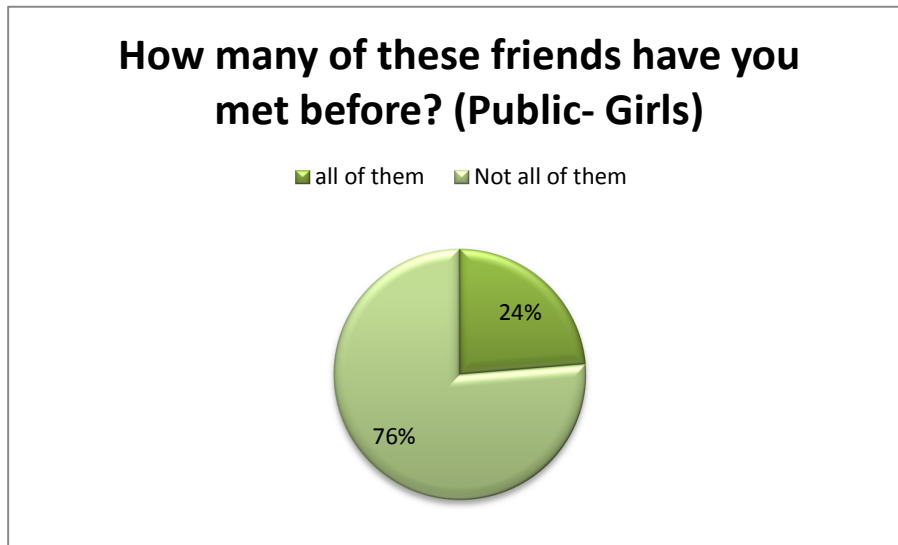


Figure 40 Online Strangers Added to Social Networking Sites: Public School Sector (Boys)



**Figure 41 Online Strangers Added to Social Networking Sites: Public School Sector (Girls)**



Some of the children's responses are indicated below:

*"All of them I know and I met" (FG10)*

*"I know some of them and some I don't know" (FG2)*

*"I know half of them" (FG4)*

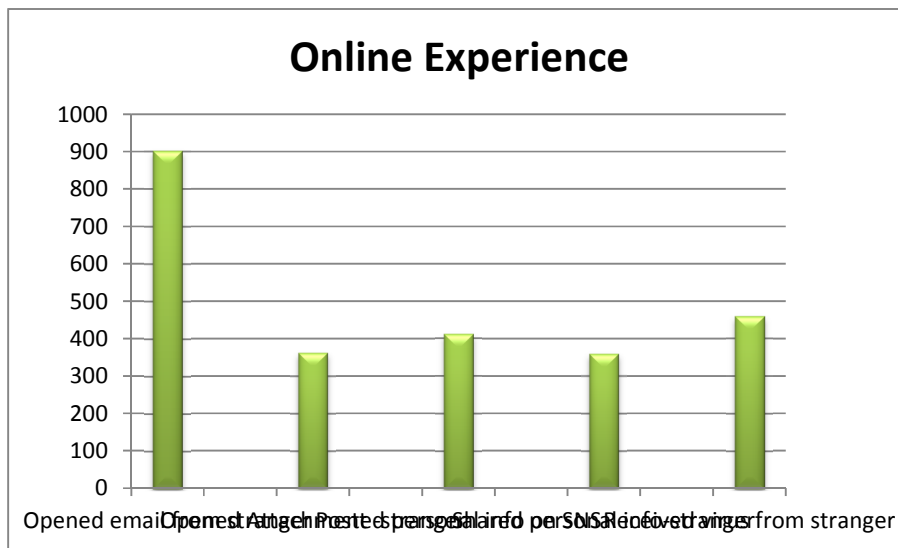
*"Most of them are from my school, but I do not know some of them and I know most of them" (FG5)*

*"Three and the rest I don't know them" (FG6)*

The survey data shows that a minority of children admitted having opened an email (35%) or an attachment (14%) from someone they didn't know, 16% had shared personal information with a stranger. These data are indicated at Figure 42.



**Figure 42 Online Experience**



The survey data indicates that generally older children in the 14-16 and 17-18 age groups took the most risks in terms of online safety, they were more likely to have shared personal information with a stranger (22% of 17-18s compared to 11% of 11-13s) and to have opened an email attachment from an unknown source (21% of 17-18s compared to only 10% of 11-13s) than were children in the 11-13 age group (Table 6). There appears to be a relationship between the sharing of personal information and the willingness to meet online strangers: those children sharing personal information were more likely to have met online strangers. This finding was established using a multi-linear crosstabulation analysis between questions exploring the sharing of personal information and meeting online with strangers. The survey data demonstrates that public school girls were *significantly* more likely to post personal information and to meet with online strangers than private school girls (Standard error of 6.2%, p value 0.34, t value 0.96, 5% level of significance) .

**Table 13 Online Risk Taking x Age**

	Age		
	11-13 years	14-16 years	17-18 years
	N(%)	N(%)	N(%)
<b>Opened email someone don't know</b>	303(27)	452(40)	147(46)
<b>Opened email attachment someone don't know</b>	109(10)	189(17)	64(21)
<b>Posted personal info on website</b>	154(14)	197(18)	60(20)
<b>Shared personal information with online stranger</b>	118(11)	174(15)	67(22)
<b>Total (age group)</b>	1116	1138	303

This data was supported by the qualitative findings. Some of the children claimed:

"I accepted someone I didn't know on Facebook and he phoned me, it was an adult man's voice, I just hung up and didn't tell my parents" (FG 9)

"My friend was friends with someone on Facebook who was a 50 years old" (FG 12)

"I was approached by someone and was chatting with him about travelling, I reported him to Facebook" (FG 5)

This finding is also consistent with data from a recent UK study (Davidson, Lorenz, and Martellozzo 2010). This data validates other data which suggests that online risk taking behaviour increases with age (Livingstone and Haddon 2009) regardless of nationality, religion (although a larger group of Muslim (15%) children (Livingstone and Haddon 2009) had shared personal data with online strangers than Christian (8%) and Hindu children (8%), however some of the religious sub categories are very small and the data may not be valid), and gender. Children attending public schools were more likely to have opened emails (42% compared to 30% of private school children) and email

attachments (17% compared to 12% of private school children) from an unknown source and to have shared personal information with online strangers (17% compared to 12%). This data is validated by the qualitative data which indicated that there is a lower level of internet safety awareness amongst public school children.

Respondents were asked if they had been made to feel 'uncomfortable' online, 36% (925) reported that they had been made to feel 'uncomfortable'. The proportion feeling 'uncomfortable' increased with age: 30% of 11-13s; 40% of 14-16s and 44% of 17-18s. There was a gender difference, girls (43%) were more likely to have felt 'uncomfortable' than boys (32%). There were no significant differences by nationality or religion, however a large proportion of girls in the public school sector (55% and 57% of girls in 2 public sector schools compared to the baseline of 43% of girls across the sample) reported feeling more 'uncomfortable' online than boys from both sectors and girls from the private school sector.

Respondents were asked to identify the nature of the online approach that caused discomfort (Table 14, Figure 43). Of the 925 (36%) who claimed to have felt uncomfortable 732(79%) described cyber bullying behaviour including posting something unpleasant or sending an unpleasant email, 213(23%) had been asked to do something they didn't want to. There were no significant differences in such experience by gender or age. The data indicates that experience of unpleasant online behaviour increases with age and is more prevalent amongst girls. The majority of the respondents took positive action in responding to unpleasant contacts, 64% blocked them, 40% would close the window. However less children would confide in either a friend (20% would), a relative (15% would) or a teacher (5% would). Girls were more likely to confide in friends and relatives than boys and there was no difference in action taken by age group.

Figure 43 Source of Unpleasant Online Experience

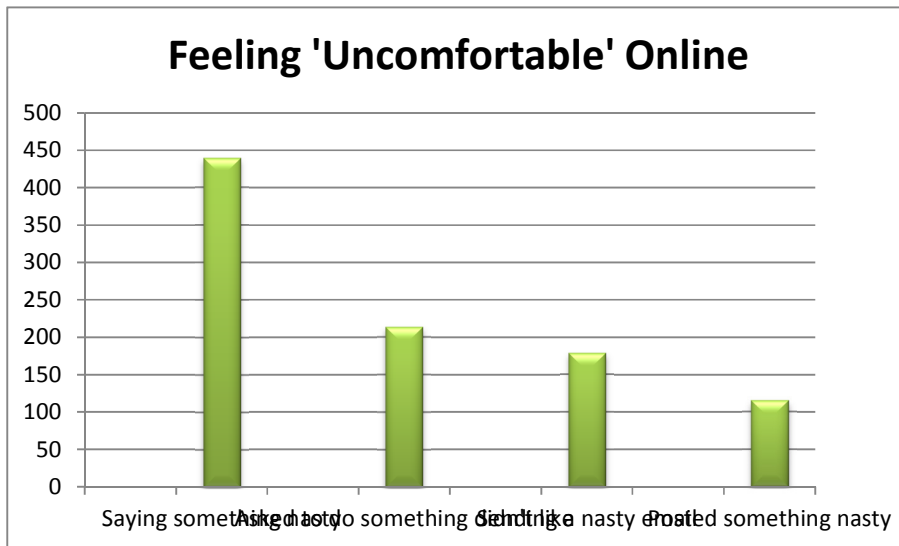


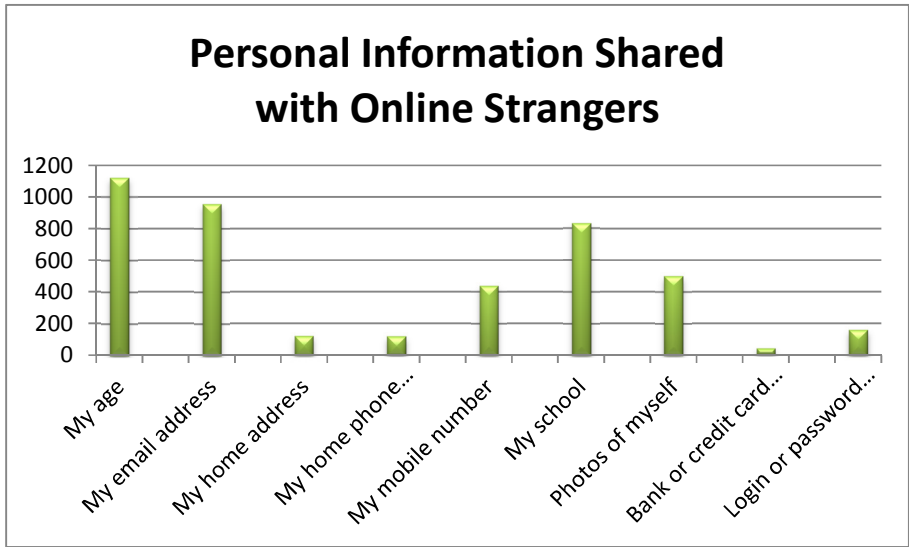
Table 14 Feeling Uncomfortable Online x Gender

	Total	Male	Female
<b>Unweighted Base: All who have felt uncomfortable</b>	925	32%	43%
<b>Saying something nasty</b>	439	203	236
	47%	41%	55%
<b>Asking me to do something I didn't want to</b>	213	115	98
	23%	23%	23%
<b>Sending a nasty email</b>	178	92	86
	19%	19%	20%
<b>Posting something about me on a social networking site</b>	115	68	47
	12%	14%	11%
<b>Other</b>	362	204	158
	39%	41%	37%

Respondents were asked to identify the type of personal information they had shared with online strangers 49% had shared their real name, 37% had shared their email address, 5% their home address and 17% their mobile number, 2% had shared their (presumably parents?) bank or credit card details (Figure 44).

Boys seemed more likely generally to have shared personal information than girls and 11-13s were less likely to have shared personal information than the 14-16s and the 17-18s, however is it of concern that 35% of 11-13s had met with an online stranger. Children attending public schools (particularly girls) were more likely to have shared some personal information with online strangers than were those attending private schools (42% of children attending public schools had shared their email address compared to 34% at private schools for example).

**Figure 44**Personal Information Shared with Strangers



The qualitative interviews support these findings. Some of the children claimed:

*"If he is ok I will add him"* (FG1)

*"Sometimes I add a girl and I feel uncomfortable then I delete her because I feel he may be a boy"* (FG4)

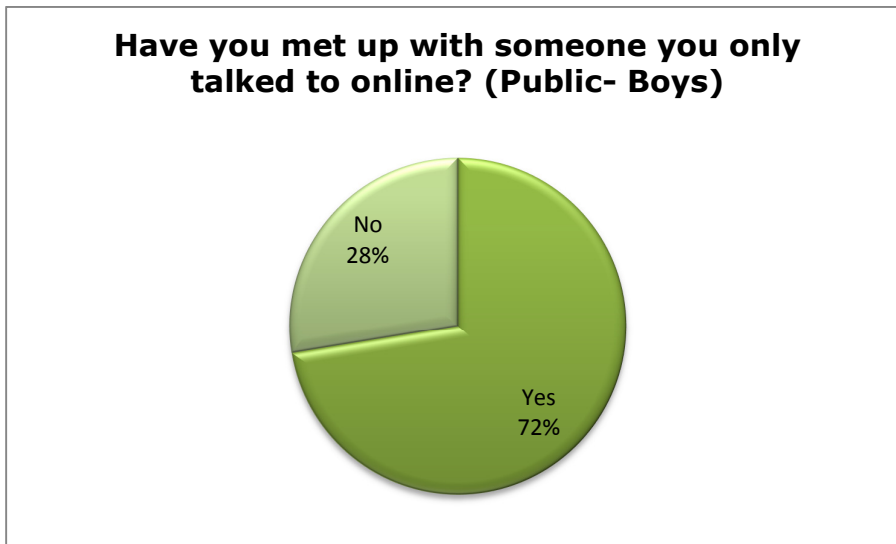
*"Yes, I access some sites to download but it takes you to chat sites. I find strange people talking strange things"* (FG4)

*"Yes in the messenger if they are ok I leave them or I delete them, I don't accept boys"*  
(FG5)

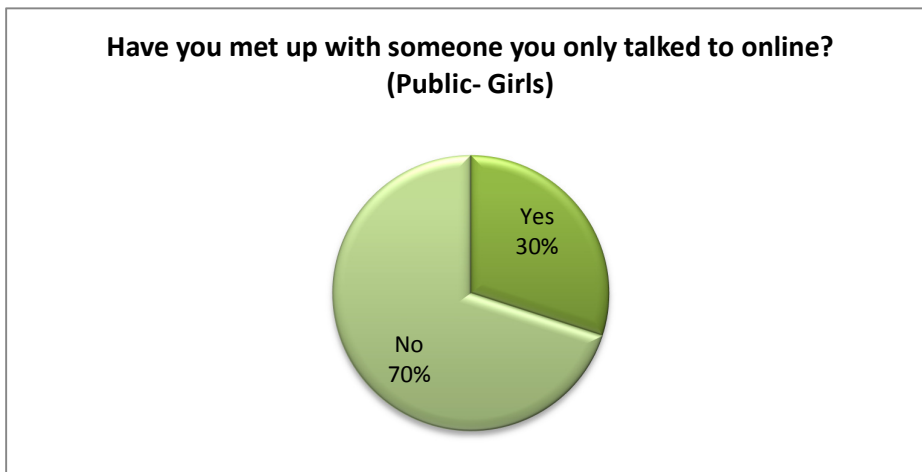
The survey data indicates that 43% (1090) of children had met with an online contact who they had not met before in person. There was a gender difference as boys were generally more likely to meet (49% had) than girls (32% had).

This finding is supported by the qualitative data. When boys were interviewed, 72% admitted that they had met with someone they only interacted with online (Figures 45 and 46).

**Figure 45 Meeting Online Strangers-Public School Sector (Boys)**



**Figure 46 Meeting Online Strangers: Public School Sector (Girls)**



Interestingly, none of the children from the private school sector claimed that they had met with someone that they had only interacted with online, this contradicts the survey data but children may be more truthful when completing an anonymous survey. Further probing revealed some concerning issues:

*"[When she turned up to the meeting], she was one year older" (FG6)*

*"Once [I met] someone. I knew her for a long time [online] and she then asked to meet her and she insisted on meeting me and later I discovered he was a boy not a girl" (FG7)*

*"I have one girl but I haven't met her yet" (FG7)*

*"On Friday, I am going to meet a girl who is going to attend a birthday party of my cousin" (FG7)*

*"I got acquainted with a person but I didn't meet him" (FG8)*

The survey data indicates much higher proportions of children meeting with online contacts when compared to recent studies in Europe (10%) (Livingstone and Haddon 2009) and the UK (7%) (Davidson, Lorenz, and Martellozzo 2010). The meeting rate peaked with the 14-16 age group being most likely to meet with an online contact (49% had) compared to 35% for the 11-13s and 47% for the 17-18s (Table 15). However, when the data was analysed by school sector and age, girls from the public school sector were the group identified as most likely to meet an online stranger (5% level of significance).

**Table 15** Number of Children Who Have Met Online Strangers x Gender and Age

Gender		Age		
Male	Female	11-13 years	14-16 years	17-18 years
1549	1008	1116	1138	303
764	326	388	559	143
49%	32%	35%	49%	47%
785	682	728	579	160
51%	68%	65%	51%	53%
1549	1008	1116	1138	303

<b>100%</b>	100%	100%	100%	100%
-------------	------	------	------	------

Muslims were more likely to meet a stranger than children from any other religious group (46%) (Table 16), and children attending public schools were more likely to meet strangers (54%) than children attending private schools (34%). However, the data doesn't indicate if the online strangers were adults or children, or explain the context in which such meetings occurred. Contacts may have been friends of friends for example. Given that Bahrain has a comparatively small population, there may be a greater tendency to meet peers in this way than exists elsewhere. It is however clear that young people's willingness to meet and their level of trust is high. This finding is validated by the focus group data which indicated that a high proportion of children in the public school sector had met online contacts (over 70%).

**Table 16 Number of Children Who have Met Online Strangers x Religion**

	<b>Religion</b>			
	<b>Muslim</b>	<b>Christian</b>	<b>Hindu</b>	<b>Others</b>
<b>Have met</b>	948	92	13	37
	46%	27%	20%	36%
<b>Haven't met</b>	1096	253	51	67
	54%	73%	80%	64%
	2044	345	64	104
	100%	100%	100%	100%

## 8.7 Online Safety Training and Advice

The qualitative data suggests there is currently more teaching of internet safety (72%) in the private sector schools but this appears to be patchy and unstructured. This data is supported by the survey findings. Furthermore, it is clear from the qualitative data that the majority of internet safety advice is provided by parents (56% in private schools; 33% in private schools for boys; 56% in private schools for girls). However, none of the young people mentioned awareness being systematically taught in schools (Figures 47, 48 and 49).



Figure 47 Source of Advice Private Sector Schools

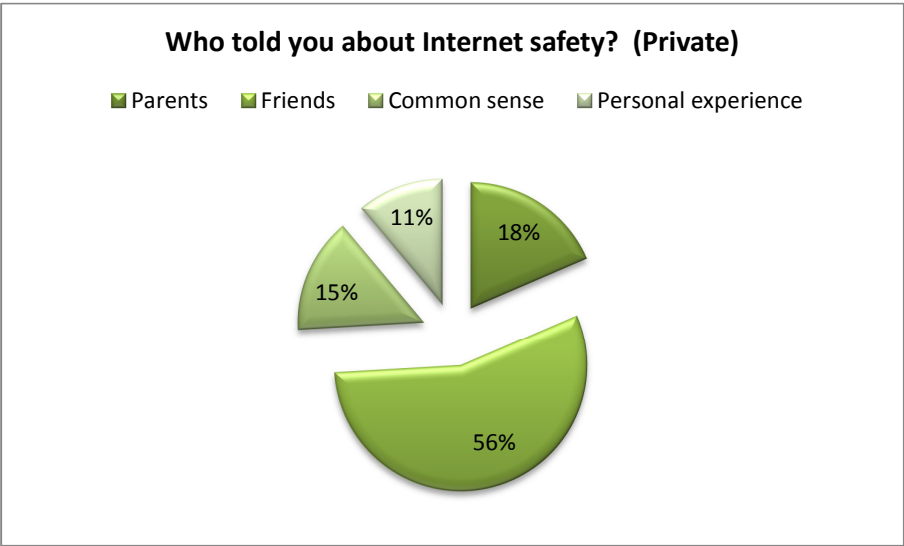
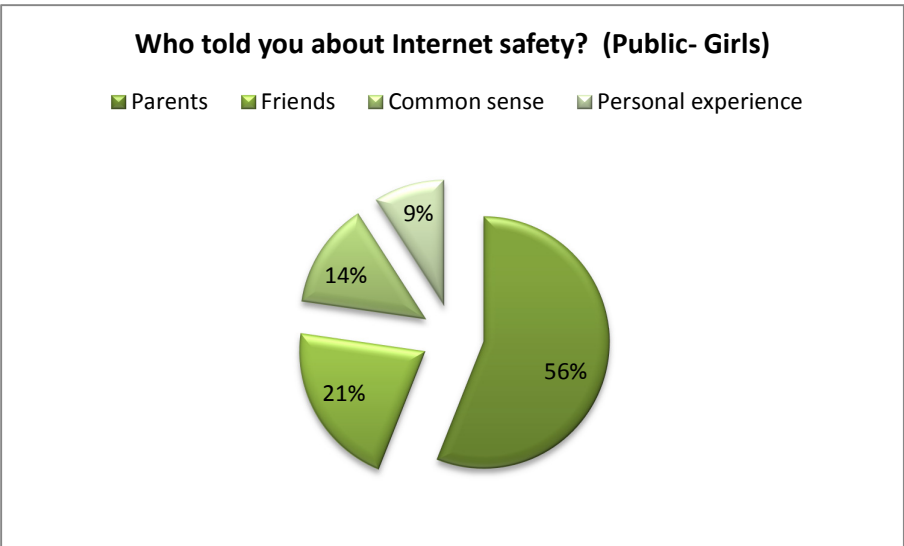
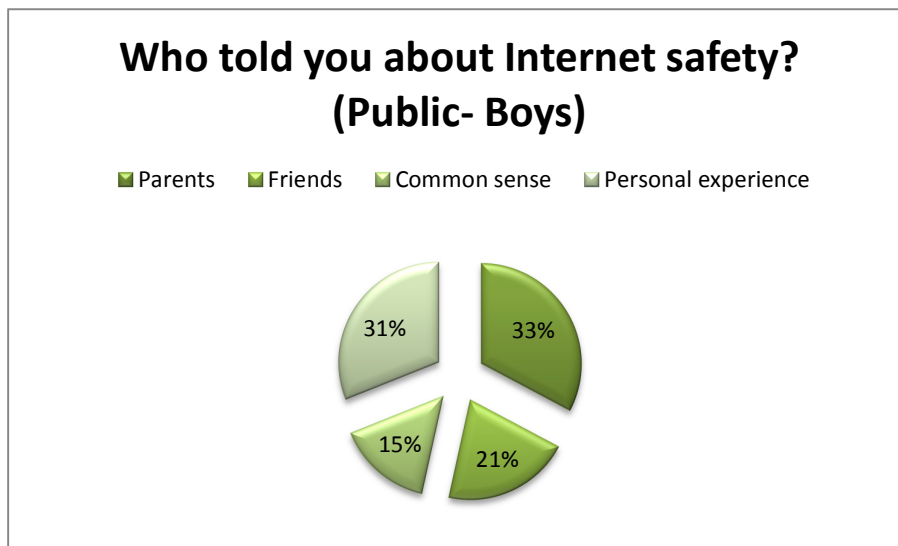


Figure 48 Source of Advice Public Sector Schools (Girls)



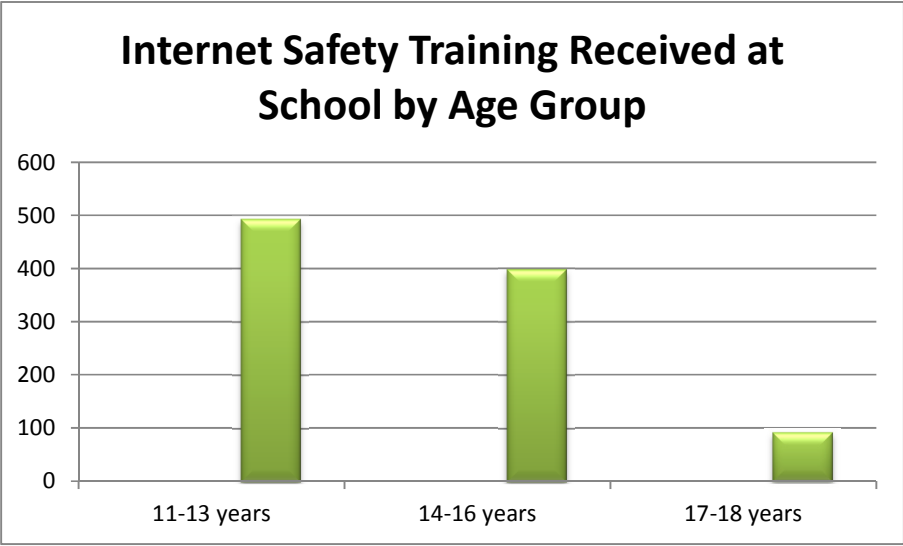
**Figure 49 Source of Advice: Public Sector Schools (Girls)**



The survey data suggests that the majority of children had not received internet safety training at school (62%), a slightly larger proportion of the 11-13 year age group (44%) had received some training at school compared to the 14-16(35%) and 17+ age groups (30%) (Figure 50). A slightly greater proportion of children attending private schools (40%) claimed to have received training, compared to only 36% attending public schools.

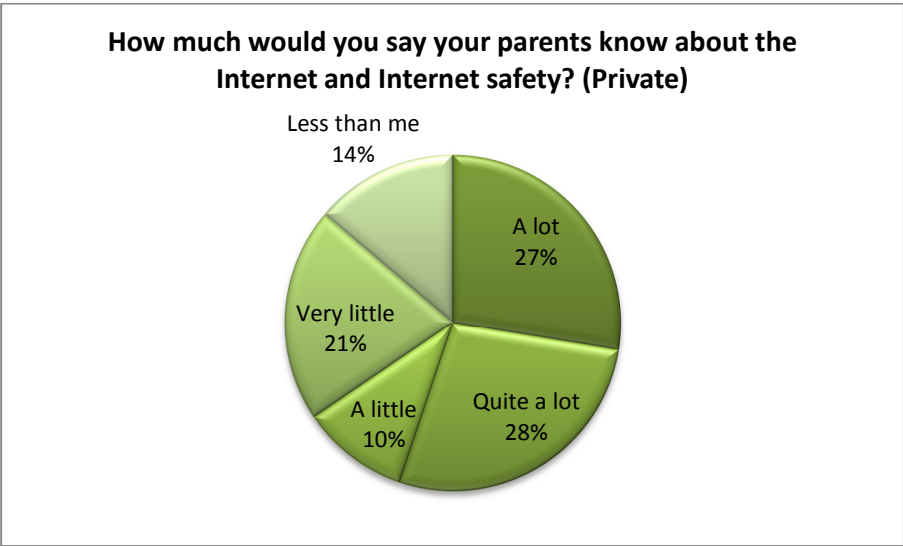
The survey data suggests that the amount of systematic schools training received was very low and there was wide variation in the public school group across schools, with only 22% of children in one school having received any form of training.

**Figure 50 Internet Safety Training Received at School by Age Group**

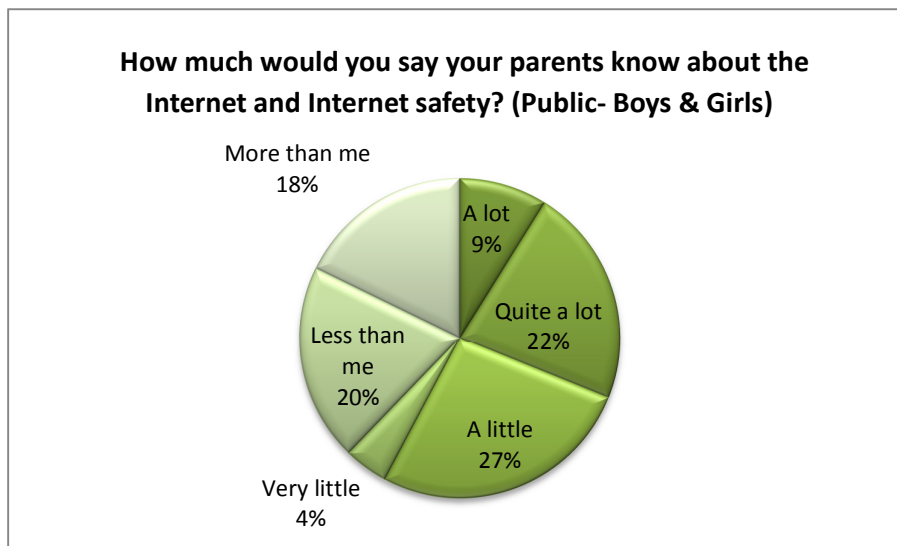


During the focus groups Children were asked to discuss the extent of their parents' knowledge on internet safety and the results are interesting (Figures 51 and 52).

**Figure 51 Parental Knowledge: Private Sector Schools**



**Figure 52 Parental Knowledge: Public Sector Schools (Boys and Girls)**



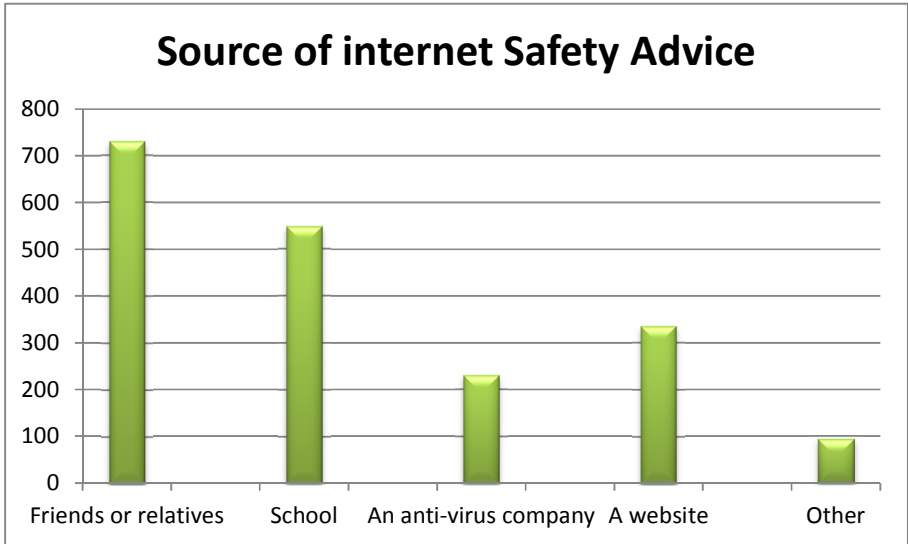
Considering that children learn about internet safety from their parents, it is interesting to note that almost half of all the children interviewed do not consider their parents to be particularly knowledgeable. The focus group data indicates that children in private schools consider their parents to have little knowledge (10%), very little knowledge (21%) or less knowledgeable than young people (14%). In the public schools, parents appear to be ranked even lower; little knowledge (27%), very little knowledge (4%) or less knowledgeable than the respondents (20%).

The survey findings suggest that a large proportion of children were allowed unsupervised access to the internet (87%) and there was little significant variation by nationality, religion, age or gender. There was however a difference in the data from private and public school sectors. Children attending private schools appeared to have much less supervised online access than those attending public schools, 7% of private school children were supervised online by parents compared to 21% of those attending public schools.

Half of the survey sample (50%) had received some form of internet safety advice or had actively sought internet safety advice. There was little variation by age, gender, nationality, private and public school sector on this general point. However, the majority had received advice from their families (57%). Some (42%) had received advice from school (Table 17 and Figure 53). There was no variation in the source of advice received by age or gender, children attending public schools were less likely to have received training at school (34%) than children attending private schools(49%). Despite not having received any formal training the majority of the sample (80%) felt that they had

knew enough about staying safe online. This finding was consistent by age, gender, nationality and private/public school sector, however Muslims were slightly less confident about their safety knowledge (78%) than Christians (90%), Hindus(84%) and the 'other religion' group (86%).

Figure 53 Source of Internet Safety Advice

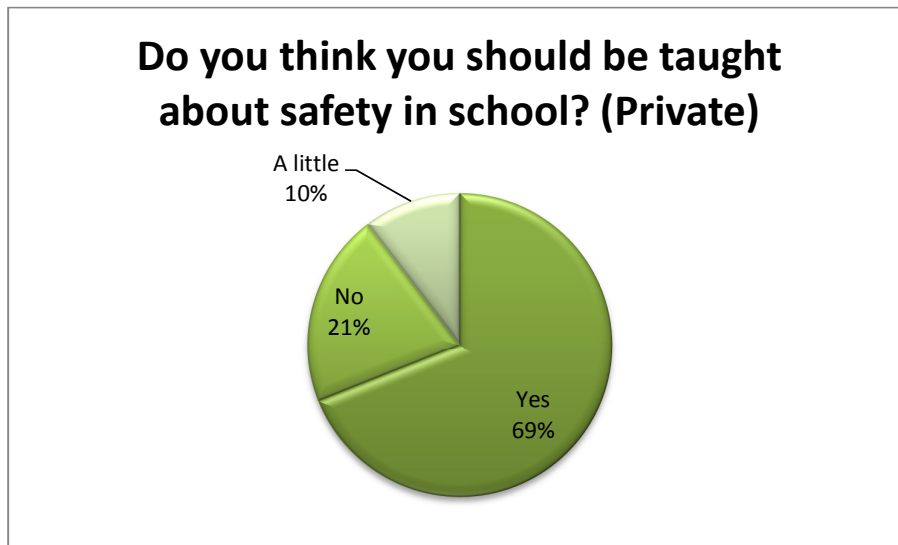


**Table 17 Source of Internet Safety Advice**

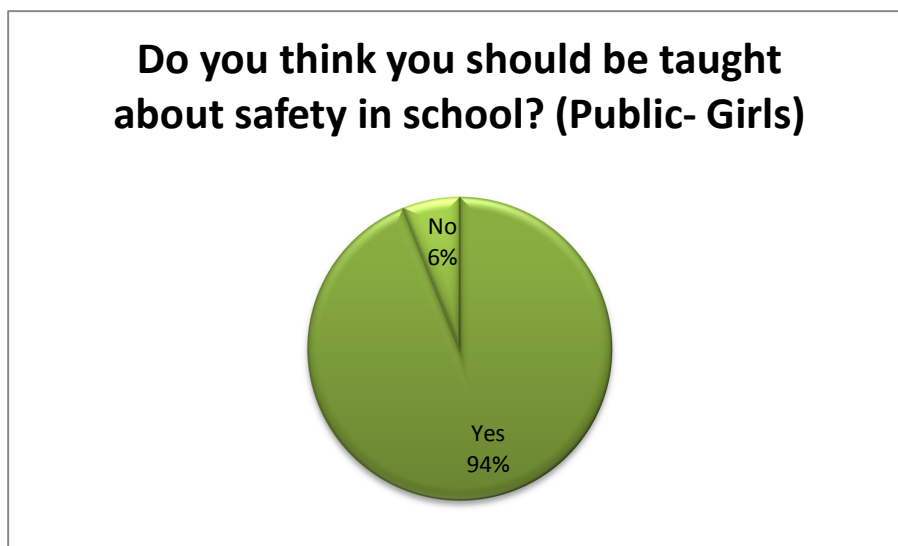
<b>Source of Advice</b>	
	<b>Total (N &amp; %)</b>
<b>Unweighted Base: Those who have received or looked for advice about internet safety</b>	1291
<b>Friends or relatives</b>	730
	57%
<b>School</b>	548
	42%
<b>An anti-virus company</b>	230
	18%
<b>A website</b>	335
	26%
<b>Other</b>	94
	7%
<b>ANY MENTION</b>	1214
	94%
<b>Can't remember</b>	75
	6%
<b>No Answer</b>	2
	0
<b>Total</b>	2014
	156%

The qualitative data suggests that when students were asked whether they should be taught about safety in school, a clear majority welcomed the idea (69%), in both the private and public school sectors (Figures 54 and 55).

**Figure 54 Is School Safety Training needed? Private Sector Schools**



**Figure 55 Is School Safety Training needed? Public Sector Schools (Boys)**



The qualitative data suggests that a clear majority in both sectors believe that internet safety should be taught as part of their curriculum. As a result, students were asked to provide recommendations on what a safety lesson should look like. This student claimed:

“They should use students from year 10-11 for internet safety” (FG 18)

"People should show us how things work; how for example to put a password" (FG 8)

"It should be practical so we don't just sit there and listen" (FG 4)

Young people's recommendations are summarised below:

- 1) It should be interactive and fun
- 2) It should be colourful and contain a lot of pictures or characters
- 3) It should not be taught by teachers but by other students
- 4) It should be practical

## 9. Teachers Interview Findings

### 9.1 Sample Characteristics: Focus Group with Teachers

A small group of thirty teachers with responsibility for ICT (Information Computing Technology), PSHE (Personal, Social and Health Education) and head teachers were interviewed. Five focus groups were carried out at the schools participating in the qualitative research. All teachers were asked to share their perceptions of young people's, teachers and parents' awareness of internet safety and to provide recommendations.

It is important to stress that the extent to which the findings from this element of the research can be generalised is limited given the small sample size, however it is interesting to note the similarities between the findings presented here and those presented in the previous sections.

### 9.2 Young People's Awareness of Internet Safety and Online Behaviour

The majority of teachers believed that young people have a good general understanding of how to use the internet but need more awareness of online safety. This perspective was supported by the fact that all young people, when asked questions regarding safety messages, identified some useful messages but are still confused regarding what they should and should not post on their profiles, and many had met with online strangers. The majority of teachers felt that young people believe themselves to be very knowledgeable.

*"They think they know a lot, but in reality they get themselves in a lot of trouble. We have had a number of incidents where children have cyber-bullied other children, have*



*publicly humiliated one teacher; have stolen another child's identity. I cannot begin to tell you."* (FG1- Private School)

It is important to note that cyberbullying is "when a child, preteen or teen is tormented, threatened, harassed, humiliated, embarrassed or otherwise targeted by another child, preteen or teen using the internet, interactive and digital technologies or mobile phones" cyberstalking (kidscape.org.uk/cyberbullying). Cyberbullying seems to be a problem, particularly in the private school sector and the consequences of such acts can be extremely damaging to the victimised child. Therefore, internet awareness should encompass training on cyberbullying and on ethical practice in using technology.

The other important issue that needs to be raised is that children feel secure and anonymous when online. As discussed elsewhere in this report, children (and adults) behave in a way that they would not in the real world:

*"We have had cases of Islamic girls that took their veil off in front of the webcam and took photographs of themselves. Then they were deeply upset when their pictures were made public. You can see how their parents felt."* (FG3- Private School)

Children should be made aware that everything they do online is a permanent record of their actions, which may be used against them. This is what can be defined as the digital footprint. On the internet a digital foot print is the word used to describe the evidence or "footprints" that people leave online. This is information transmitted online, e-mails and attachments, uploading videos or digital images and any other form of transmission of information; all of which leaves traces of personal information about that particular person, available to others online.

### **9.3 Safety training in Schools**

All teachers suggested that schools do not have clear policies regarding safe internet practice and therefore internet safety is either not taught at all, and when it is taught, this is not done systematically. To the question, "Do you teach students the sensitivity of personal information which should not be posted on the net" some teachers answered as follows:

*"Very little"* (FG4- Public School)

*"We give them, within the project, general guidelines about the use of the internet" (FG2- Public School)*

*"We do at the beginning of the year but the messages is never formally reinforce throughout the year" (FG1- Private School)*

*"In the beginning we don't allow them to use the internet unless there is a work and we try our best to teach them not to give your information to anybody. Don't log in any site and your email until you become safe" (FG3: Public School)*

These findings support children's responses which suggest that they do not receive any formal or structured training in schools. Furthermore, in schools children learn about how to protect their computers from viruses and from hackers but do not learn basic awareness tips on how to stay safe online.

*"Through the internet curriculum we have a subject on how to protect your pc from hackers and internet hazards" (FG2- Public School)*

This claim reinforces the survey and interview findings with children which show that a significant number of respondents perceive of internet safety as virus's protection for the computer rather than as online risk taking behaviour.

#### **9.4 Training for teachers and parents**

All respondents felt that there is a generation knowledge gap. The level of awareness amongst parents is generally very low and that this problem needs to be addressed. Some parents, particularly younger parents, are computer literate and use social networking groups or use MSN regularly. However, many feel alienated from the digital world and instead of becoming more involved and attempting to learn more they avoid the problem. Most parents think they understand the problem and know enough to supervise their children. These findings reflect what was raised by children during the focus groups.

Thus some teachers recommended a wider internet safety campaign that would also reach children's homes.

*"We should make awareness from the house. Many generations and parents now don't understand Facebook. Much of the awareness must be made by parents. A father should monitor his child and establish a background for him. The school, the house and the society must complement each other" (FG4- Public School).*

*"We should make a five-year plan and we create religious and legal restraint in order to create a knowledgeable generation. I always tell students to make use of the internet and learn new things every day" (FG3- Public School).*

Many respondents would like to see internet safety education made a priority for parents as well. Overall all respondents felt that parents do not become involved in their children's use of the internet and do not supervise their children properly online. It is interesting that these perceptions are generally substantiated by the children's responses.

### **9.5 Teachers' Recommendations:**

The majority of the teachers claimed that they would benefit from some internet safety training so each school could teach the same messages and there would not be disparity across schools. Currently, Internet safety training is delivered in a piecemeal fashion by each school; however the message should reach each child in the same manner.

This finding reflects those from the children's interviews which suggest that children studying in private schools are more aware of internet risks than those studying in public schools.

*"They [children] definitely need awareness" (FG5- Public School)*

*"Yes they need [awareness]. They make mistakes even after we guide them" (FG3- Public school)*

*"Students need awareness from entering the school until they graduate so that and when they enter the university they are ready and aware of internet safety and they do not suddenly become open-minded in respect to such things" (FG5- Public school)*

*"The students like lectures especially if they are given by a person from outside the school who affects the students more. Some of them implement the guidelines when we instruct them about risks. But we need more than one way" (FG2- Public School)*

*"We can make use of social specialists and improve them to make the situation sustainable". (FG5: Public School)*

The way this should be delivered is summarised below:

- 1) Regular lessons on internet awareness by social specialist.
- 2) Practical training session in labs.
- 3) Awareness campaigns in schools through leaflets, poster and emails.
- 4) The introduction of awareness programme in the school curriculum.

However, as other stakeholders have recommended, young people should also be made aware of what is both allowed and not allowed and make them responsible if they do something that can hurt others. These recommendations have also been reinforced by some teachers:

*"Students must know that some actions are legally accountable. One time a teacher disconnected the phone of a student but his father intervened in his favour protesting that it is his private phone. So the father had a role in this" (FG4)*

The great majority of teachers were against blocking sites.

*"Even blocked sites by the country are hacked by students and we cannot prevent such sites 100%. Blocking pornographic sites is of no use if the student is not convinced" (FG6- Public School)*

*"I conclude now that all schools depend on the Ministry of Education and the filtering protection provided by Batelco and the prevention of accessing Pornographic and non-educational sites" (FG6-Public School)*

It is also important to remember that it cannot always be assumed that young people make the choice to visit sites that are unsuitable.

*"The girls sometimes see pornographic pictures" (FG3- Public Schools)*

It is not hard for a determined webmaster to "disguise" a web-site to catch innocent visitors.

## 9.6 Child Survey: Summary of Key Findings

1. The mean average time spent online each day was 2.5 – 3 hours.
2. The majority claimed that their parents 'sometimes' or 'never' knew what they were doing online (52%).
3. Older children in the 14-16 and 17-18 age groups took the most risks in terms of online safety; they were more likely to have shared personal information with a stranger and to have opened an email attachment from an unknown source than were children in the 11-13 age group. This finding is consistent with data from a recent UK study (Davidson, Lorenz, and Martellozzo 2010). Girls attending public schools were more risk taking than those attending private schools.
4. The proportion feeling 'uncomfortable' online increased with age. There was a gender difference, girls were more likely to have felt 'uncomfortable' than boys.
5. Of the 925 (36%) who claimed to have felt uncomfortable the majority (79%) described cyber bullying behaviour including posting something unpleasant or the sending of an unpleasant email, (23%) had been asked to do something they didn't want to.
6. The majority of the respondents took positive action in responding to unpleasant contact either by blocking them or by closing the window. However few children would confide in either a friend (20% would), a relative (15% would) or a teacher(5% would).
7. A large proportion of children (43%, 1090) had met with an online contact who they had not met in person before. This data indicates much higher proportions of children meeting with online contacts when compared to recent studies in Europe -10% (Livingstone and Haddon 2009) and the UK - 7% (Davidson, Lorenz, and Martellozzo 2010).

8. There was a relationship between the tendency to share personal information and the willingness to meet with online strangers. This group of young people are the most risk taking and are probably most at risk.
9. There was a gender difference as boys were more likely to meet than girls.
10. Muslims were more likely to meet a stranger than any other religious group (46% had) and children attending public schools were more likely to meet contacts (54% had) than children attending private schools (34% had).
11. The majority of children had not received internet safety training at school (62% hadn't).
12. A large proportion of respondents were allowed unsupervised access to the internet (87%) and there was little significant variation by nationality, religion, age or gender.
13. Where children had received internet safety training advice the source tended to be family or friends.
14. The majority felt they knew enough about staying safe online. However, this was not evidenced by the online behaviour of many children who divulged personal information and who met online strangers.

## **9.7 Child Focus Groups: Summary of Key Findings**

- 1) All children, both from the public and private school sector use the internet every day and spend an average of 3.5 hours online.**
- 2) The great majority of the respondents use social networking sites.**
- 3) The majority of young people from the public sector have at least one mobile device, like for example iPhone or Blackberry.**
- 4) Most respondents have a personal laptop or computer in their bedroom; many public school respondents have PCs in the family dining room.**
- 5) Girls from the public sector are more likely to use the internet for socialising. While boys are more likely to play games online and investigate things they're interested in.**
- 6) A large number of young people from the private sector claim that they do not inform their parents of what they do online, whereas the majority of the public sector claimed to.**
- 7) The majority of respondents do not to share their online activities with their parents; they enjoy the privacy and freedom that the Internet affords.**
- 8) A majority of the respondents are not asked by their parents what they do online.**
- 9) Respondents are generally aware of the dangers of posting personal information on the internet, but willingly post such information on 'trusted' social networking sites such as Facebook. This is particularly the case for the public school sector.**
- 10) A limited number of respondents understand internet safety as a personal safety issue. Most children, particularly boys tend to refer to virus protection rather than personal information.**
- 11) A large number of the boys in the public school sector had met with someone they had only met online (online stranger).**
- 12) None of the respondents from the private school sector claimed that have never met with someone they only interacted with online.**

- 13) Respondents generally set their profiles to private and are aware not to add people they do not know- there is less awareness however amongst public school children.
- 14) Respondents receive awareness internet safety messages through family and friends but no formal or structured training in schools.
- 15) The great majority of respondents encourage formal internet safety training programmes in schools.



## 9.8 Teachers Focus Groups: Summary of Key Findings

- 1) All teachers felt that internet safety should be regularly addressed in schools because the internet is part of every child's life.
- 2) Cyber-bullying is a serious phenomenon that needs to be addressed. Teachers commented that the boundary between home and school is increasingly blurred due to the Internet and that problems on the Internet tend to spill into school life.
- 3) Children say and do things online that they would not otherwise say and do in the real world.
- 4) A number of teachers have been humiliated online by their pupils.
- 5) The ethics of using computer technology should be addressed in schools and at home.
- 6) All teachers stressed the importance of delivering awareness messages.
- 7) All teachers felt that awareness messages are not delivered in a systematic manner across schools.
- 8) The great majority of teachers feel that there is a knowledge gap between children, parents and teachers.
- 9) All teachers felt that parents play a key role as well in educating children about online safety.
- 10) However, some parents feel intimidated by their children's knowledge as they are more internet savvy than they are.
- 11) A large number of parents do not supervise their children's Internet use at home
- 12) The majority of teachers felt that parents should also be included in an 'education campaign'.

## 10. Findings: Stakeholder Interviews

### 10.1 Sample Characteristics

A group of 18 stakeholders were interviewed during the last stage of the research. Key players involved in the development of children's education and the wellbeing of children within the Kingdom were purposely selected to take part in the study including representatives from:

- a) Child welfare support agencies, charities and Non Governmental Organisations (NGO)
- b) Ministries of Health, Education and Development
- c) Internet industry
- d) TRA
- e) Bahrain-based Academia

All stakeholders were asked to share their perceptions of young people's and adults' awareness of Internet safety and were asked to share their views regarding what should be done to address Internet safety in the future. Child welfare support agencies such as the Bahrain Centre for Child Protection and key Ministries were asked to share both their knowledge and experience on what kind of problems children face online, and were asked to make recommendations on how these problems might be effectively addressed.

The extent to which the findings from this element of the research can be generalised is limited given the small sample size. Nevertheless, it is interesting to note that these findings support those presented in the previous sections. It is important to stress that the level of access was extremely high and, as a result, the researchers were able to gather the views and recommendations of key influential stakeholders from the Kingdom.

### 10.2 Nature and role of the organisations

The organisations participating in the study showed great interest in the research and recognised the importance of the project and supported the aim to provide a safe environment for Internet users, particularly children. The participating organisations were as follows:

#### 10.2.1 Ministry of Education

Two representatives from the Ministry of Education (MOE) discussed their educational mission. This is *"to ensure the provision of evidence-based education at all levels based*

*on efficient use of ministry resources (schools, libraries, e-services) and encouragement of personal responsibility for education” (Ministry of Education 2005). As the main providers of educational services in Bahrain, one of the respondents claimed that*

*“it is one of our responsibilities is to provide a safe environment online and offline. We work hard to improve the education process” (R4)*

The MOE’s new strategy focuses on developing the education system in Bahrain specifically:

1. Educational gain
2. Quality and educational excellence
3. Service development
4. New investment in the educational infrastructure in Bahrain
5. Partnership working
6. Community involvement
7. Organization and management
8. Human Resources
9. Education, research and development
10. Financial Management
11. Information and communication technology

### **10.2.2 Ministry of health**

Two representatives from the Ministry of Health (MOH) were interviewed. Both respondents are actively involved in child protection and are members of the Child Protection Committee (CPC) which seeks to protect children suffering from abuse and neglect.

*“From a medical perspective we examine them from the medical point but now we work closely with psychologists and social workers to explore all the other issues related to the abuse. We meet regularly we can discuss the case and think about what is best for them. Most of the cases are referred to us from the Bahrain centre. We receive call from the hospital, schools, local health sectors, police stations. We are basically the centre for all of these children in need. We provide counselling for children and parent to avoid this from happening again. We also provide training for anger management, lectures in schools but we feel that we need more people doing this” (R 9 Ministry of Health).*

The Child Protection Committee (CPC) was formed in 1991 by the Ministry of Health (MOH) and is responsible for assessing and providing treatment for all cases of child abuse and neglect referred to Salmaniya Medical Complex (SMC). CPC includes paediatricians, child psychiatrists, social workers and community nurses. In addition, the Committee consults the MOH’s legal advisor when needed. A child protection plan was

developed by the Committee in 1998 and was supported by WHO. The action plan covered three main activities: 1) intervention 2) education and training and 3) policies and legislation. Professional guidelines for health providers were developed and child protection seminars and workshops were provided for medical students, paediatricians, primary care physicians and community nurses.

### ***10.2.3 Ministry of Social Development***

Representatives of the Ministry of Social development also showed great interest in the research. The aim of the ministry is to provide the best services to the child in different areas such as protection, welfare in addition to cultural, educational, social and recreational development.

One of their most recent achievements in child protection is the Centre for Child protection which opened in 2007 under the patronage of Minister Dr Fatima Bint Mohammed Al –Bulooshi. The Centre has a central responsibility for child protection and has responsibility for the assessment and care of children suffering physical, mental, sexual, emotional abuse and neglect. The Centre is staffed by psychologists and social workers. The centre provides support for abused children and their families, legal advice and rehabilitation programmes.

### ***10.2.4 Shura Council***

Two members of the Shura council were interviewed. Both stakeholders showed great interest in future involvement in this research. The Chair of the Shura Council's Committee for Women and Children Affairs provided some useful insights regarding the current situation of Bahrain. She was in favour of a stronger legislative framework focusing on the protection of women and children. During the interviews, it was affirmed that many hours were spent debating child protection and many consultative meetings were held with the relevant agencies and bodies in order to draft the new legislation.

### ***10.2.5 Bahrain University***

The University of Bahrain (UOB) has played a key role in this research and showed great interest in future collaborative work. The UOB was founded in 1986 with a mission to excellence in teaching and learning, innovative research, the dissemination of knowledge and building partnership with the community. In 2009 the UOB proposed the Future of the Internet Unit as the Internet is revolutionizing the way of accessing information and how the world is communicating. The Unit was initially established under the Information

technology Centre, where it offers research, consultants and training services to Bahrain's society.

The unit's objective is to bring academics from different disciplines together to enrich the future of the internet in Bahrain. Academics from IT background, sociologists, pedagogues, engineers, and criminologists can now work together to investigate the current status of Internet safety in Bahrain, propose solutions and work in cooperation with the government to implement these solutions.

From an academic perspective the Unit can offer research that investigates how internet users access the internet safely and securely. Currently Dr Khalid Al-Mutawah and his team are conducting a study on victims' patterns of Internet bullying focusing upon the users of social network sites like facebook. Furthermore, Dr Al-Mutawah and his team's aim is to establish collaborative research with the international community, local authorities and non-government organizations (NGOs) to exchange data, expertise and share knowledge associated with safe internet and online child abuse.

The Unit also provides training and workshops to:

1. Educate a variety of Internet users about the proper usage of the Internet.
2. Educate judges, lawyers and policeman about cybercrime, abuses on the Internet and accessing illegal contents.
3. Educate teachers in schools about the best practices of surfing the Internet safely, data privacy, and abuses on the Internet. This can be implemented through Bahrain Teacher College (BTC) that was founded in 2008 at University of Bahrain to train future teachers of schools in Kingdom of Bahrain.

In addition to research and training, the Unit is willing to collaborate with local authorities, NGOs and international communities to establish policies and procedures that ensure a safe future Internet for local users.

#### **10.2.6 Bahrain Internet Society (NGO)**

A member of the Bahrain Internet Society (BIS) was interviewed. BIS is a non-profit organisation that was set up in 1996 that reports to the Ministry of Information. BIS strives to serve the community of Bahrain by spreading awareness on the benefits of Internet and Information and Communication technologies (ICT).

BIS also strives to engage in ICT Development towards e-Bahrain. To achieve this objective, BIS is:

1. Conducting hands-on training for citizens on Internet and Computers fundamental.
2. Conducting generic and specialized seminars, workshops and forums to improve e-content and to help people to develop skills. One of the major concerns is around e-content.
3. Organizing awards to encourage the innovative and effective use of technology.
4. Providing advisory to entities on technology related matters
5. Promoting awareness- particularly to women so they can then teach their children
6. Creating awareness through workshops and presentations
7. Training for university students- we then give them a certificate

#### **10.2.7 Bahraini Society for Child Development (NGO)**

The Bahrain Society for Child Development (BSCD) also participated in this study. BSCD was founded in July 1991, and "since its inception has been able to occupy much space in the community of Bahrain through its noble mission and its giving fruitful and sincere intentions to support and develop one of the most important segments of society, a Bahraini Child" (<http://www.fsd.org.qa/common/ngo/ngo/2125.html>).

*"We take care of children particularly children with difficulties. We organise a number of workshops for the children teaching them how to handle the technology- basic things like excel, word etc. We also organise seminars and engage a lot with the media" (R 7, BSCD)*

*"Children come to us for training. We work closely with doctors and other specialists like speech therapists. We organise workshops to teach them how to use the Internet" (R 7, BSCD)*

Some of the society's work involves working closely with parents, who contact the society for advice.

### **10.3 Background and Legislative /Policy Overview**

Stakeholders suggested that there is no legislative framework that either seeks to protect children from Internet related or other forms of abuse, or that seeks to protect adults from cybercrime (other than basic e-transaction legislation passed in 2002). However, legislation is proposed in both areas (see section 5.6 for a description of the proposed legislation).

Stakeholders suggested that the proposed child protection legislation (including Clause 17 on internet 'luring') should be enacted and implemented with the agreement of key

organisations and government departments such as the Ministry for Social development and the Ministry of the Interior.

All stakeholders felt that there is a need for a legislative framework that protects children from abuse in both the real world (the family, school and society in general) and cyber space (internet grooming, abuse, cyber-bullying).

*"There is not any overarching information. Being in this industry I have never come across any legislation. The only regulation I am aware of is the filtering system on the Internet and people have to accept that. For example nobody can access gambling website as it is against Islamic culture" (R 3, ISP)*

*"As a member of the Shura Council we are proposing a new Chapter especially to include a clause on Internet abuse (Clause 17). Now we have nothing that covers the issue of internet abuse. So we need more legislation to support our goal to protect these children" (R8, Shura Council)*

*"What we have is not enough. The only thing that we have is the criminal law and the cyber crime act that is currently been discussed is also too general. This chapter will be important for the children here in Bahrain" (R8, Shura Council)*

The new chapter will include the grooming offence (referred to as 'luring'). The legislation is currently under discussion until later this year. Stakeholders suggested that this legislation is necessary:

*"Currently nobody who commits an offence online would be criminalised because we don't have the legislation. Very important as it recognises the problem". (R8, Shura Council)*

The proposed cybercrime legislation should be enacted but it was suggested that the process of developing such laws should be a consultative one involving a range of organisations:

*"There is not proper legislation to protect the public. We have had a number of problems with fraud and cybercrime. Currently a draft has been written. This has been taken to parliament but the answer has not been heard yet. This is an important draft for us and should be taken seriously" (R1, NGO)*

*"Bahrain lacks any legislation that protects individuals from cybercrimes. The formation of cybercrime laws should be a consultative process including stakeholders such as NGOs, TRA and academics" (R1, NGO).*

Stakeholders suggested that key organisations should work collaboratively to ensure that should draft legislation be enacted, it is implemented effectively. It was recommended that an organisation such as an e-Government forum or committee be formed.

*"Therefore there is a need for an e-government forum that involves representatives from different stakeholder groups including ministries, ISPs, NGOs, teachers and parents. All should have a voice in keeping with the Bahraini principle of openness and tolerance" (R2, ISP)*

Stakeholders suggested that there would be a need to train prosecutors and police officers if the draft child protection legislation is introduced, in order to ensure effective implementation.

*"Training for law enforcement and judges is very important. It is the first time here that law enforcement is mentioned. In other words, if we develop legislation there is a need to also develop everything that comes with it" (R8, Shura Council)*

Stakeholders were opposed to blanket blocking of the Internet and attempts to further control Internet usage, they advocated educational awareness training for parents and children. Some ISPs suggested that in the spirit of openness the community should be directly involved in discussions about blocking.

*"Blanket blocking is limiting and does not provide a good solution, the government should enter into a dialogue with ISPs to discuss what should and should not be blocked. Further blocking or limiting young people's internet usage is not a good solution to safety issues. It is very important to include families and the community in discussions about safety and blocking, at the moment this doesn't happen". (R2,ISP)*

*"I feel the government should provide information to society and explain why they enforce filters. People need to understand why decisions are made and not just accept. People would appreciate what they are doing; there should be a process of consultation". (R3, ISP)*

*"We are strongly resisting the temptation of stopping children from sites or more dramatically from the Internet. We have Human Rights and children as well have the right to use such a useful tool. Our children have the right to be part of the digital global community- what we call digital citizenship. This is one of our targets. We want Bahraini to have critical thinking skills and of being a global citizen with a national affiliation. We have to keep our culture, our religion but there is no way to prevent the coming technological problems". (R 4, Ministry of Education)*

It is clear that stakeholders suggested that the government should engage more not only with ISPs but also with society. It was strongly recommended that blocking or filtering material does not provide a sustainable solution, particularly as the risk to children and adults on the Internet is also a people problem and not only a technology



related problem (Martellozzo 2010). As argued by Jones (2003), those who endanger children and adults are people and not computers. Indeed, "the most important issue surrounding 'Child abuse and the internet' is child protection" (Jones 2003:41). Thus, promoting education for parents and children is essential.

### **10.3.1 Further Gaps in the Law**

Further gaps in the current Bahrani legislation were identified, particularly around the definition of a 'child':

*"There is a gap in the law. A child is defined a person under 16 but children that is between 16 and 17 aren't protected because they are not considered as children. They wouldn't even be put in a juvenile centre and not dealt with the juvenile law. This is a serious problem. We have been working on a new law that for the past 4 years but this has been bouncing back and forth" (R 11, Ministry of Health).*

This stakeholder was concerned regarding the treatment that children or young adults above the age of 16 receive. It is clear that notions of childhood have been gradually discovered, identified and constructed throughout the centuries and that, despite all these attempts at constituting childhood as a clearly bounded social category, it still remains fluid and contested across different countries and legal jurisdictions.

Punishment, on the other hand, was characterised as sometimes very harsh:

*"If a man has sex with an underage girl, he can get a life imprisonment. Even if they say that there is consent, this would not be taken into consideration. For boys the sentence is less than life imprisonment" (R 11, Ministry of Health).*

However, as highlighted by the stakeholder below, the law has some further significant gaps which need to be urgently addressed. Bahrani law currently does neither define nor recognise physical abuse (however the proposed legislation does recognise physical abuse):

*"In the law there is not such a thing as physical abuse which is very bad. No definition, nothing. And the only thing that there is in the law is if someone hurt somebody he would be penalised for that for example 30, 40 Dinars. And the sentences are usually very light, depending on how much damage they have caused. As for children, there is no definition of child abuse and despite the fact that there are children who have been hurt badly -we have children who died, we have shaken baby syndrome, who have children who are mentally retarded or with convulsion, children with severe disabilities. We have taken these cases to public prosecution but none of these cases are prosecuted and the parents are punished. None. None of them" (R 11, Ministry of Health)*

*"I have been working in child protection for many years and I have a lot of experience in the field. We refer every single case to public prosecution. We have a police woman working for us, so every case will go. But many of these folders will be just kept and will*

*not even reach the court. And those that reach the court, they won't be prosecuted, very rarely. This is for physical abuse." (R 11, Ministry of Health)*

Stakeholders also suggested that it is also hard to secure a prosecution for sexual abuse that occurs within families as evidence is needed:

*"If you don't get a father saying "Yes, I did it" then, it will be just the word of the child against that of the adult. And even when there is evidence, the father will deny" (R 11, Ministry of Health)*

Stakeholders expressed frustration regarding the current lack of willingness to prosecute such cases. According to Al-Mahroosa et al. (2005) there is no mandatory referral law in Bahrain, but there is a professional requirement for health professionals to refer abused children to the Child Protection Committee. However, there are currently no such requirements for other professionals, such as teachers or social workers, to report abuse (Fadheela Al-Mahroosa, Fouad Abdulla, Susan Kamal, and Al-Ansarib 2005).

It can be argued that every society has a moral obligation to protect children because they constitute a particularly vulnerable group (Fortin 2003; Unicef 1989). However, in many countries such as Bahrain, the legal context to support child protection is sometimes absent. Therefore, the definition of childhood is vital, as this provides some general guideline as to who is a child, when a child becomes an adult and, more importantly, when children acquire fundamental rights and when they lose certain protection measures. Children require 'tailor-made' rights because they '*need special care and attention that adults do not*' (Unicef 1989). Stakeholders did however recognise that the proposed legislation would provide a child protection framework but expressed some concern that it may not be enforced fully.

#### **10.4 Current Approach to Internet Safety**

The great majority of stakeholders believed that very little has been done to educate adults and children about internet safety. It appears that a significant number of consumers are mainly concerned with data protection and confidentiality issues rather than child protection. Furthermore, as previous findings have shown, there is a large knowledge gap between young people and adults regarding the use of the Internet and online safety. Where parents are aware of the risks they often do not know how to help their children to stay safe when navigating on line.

*"In Bahrain the younger generation is adopting the Internet very quickly and there is an increasing digital divide between young people and their parents" (R1, NGO)*

*"Even if we say: 'we know a lot about computer and the Internet', the reality is that they [children] know more than us. We don't have to use the Internet like they are doing. So this gap will always continue to grow. Children are clever, they are curious and they will always invest more time than we do in exploring the way and the quicker way to get to information. We cannot control them. Well, in my experience I cannot control my son" (R7, NGO)*

*"It is difficult for parents to control their children because they know more than their parents. It has to come from the children as well, what we can call the 'the police within'. We need to educate children on how to stay safe; on what it is appropriate to see; to search and to download" (R 5, Shura Council)*

*"I Can foresee a problem with lower social class where there is a knowledge gap between young people and their parents about Internet usage. We need to think carefully about how to raise this with such people" (R6, Ministry of Social Development)*

Generally, it can be argued that all respondents felt that the level of awareness amongst parents is often very low and that this problem needs to be addressed. Some parents, particularly younger ones, may be computer literate and may use social networking groups or IM services regularly. However, many do feel alienated from the digital world and instead of becoming more involved and attempting to learn more they avoid the problem; these findings reflect research findings from other countries discussed in the literature review (Byron 2008; Davidson, Lorenz, and Martellozzo 2010).

It is clear from the stakeholder interviews, interviews with teachers and from the adult survey that parents cannot control their children's activities all the time, and this is not a realistic expectation given widespread use of mobile phone Internet technology amongst young people. However, parents need to be made aware of the risks their children may be facing when online and need to know how to educate them on safety issues. Furthermore, parents need to know how to help them to appreciate that they have to be responsible for their own online actions.

### **10.5 The context of Internet safety**

The use of the internet has grown exponentially in the past ten years. According to Internet world statistics (<http://www.internetworldstats.com/>), internet usage in Bahrain has grown from 40,000 in 2000 to 402,900 in 2009. These numbers are supported by this research which shows that social networking sites are very popular amongst teenagers and adults and that such sites represent the new playground for children.

*"What triggered the importance of the subject to me is that just Facebook alone we had 146.000 Bahraini under 18 using Facebook. If you see the Bahraini population of nearly 1 million, it is rather concerning that such a high number is online because we have 14, 15 and even 13 year old children using Facebook" (R 1 NGO)*

The majority of stakeholders that participated in this study were supportive of the use of social networking sites and IM services as they allow children to interact in a fun way with their friends.

However, they also expressed some concern:

*"We sell Internet products and are aware of the dangers that children are exposed to. There are filters in place to block youngsters to visit harmful websites. But youngsters are tech-savvy enough and have tools that allow them to access these websites. The problem with the IT world is that there is nothing in place that prevents access because of the easiness of the IT structure". (R 3, ISP)*

Furthermore stakeholders suggested that it is widely accepted in Bahrain and many Islamic countries that Islamic organisations and groups should be trusted. Therefore, groups that are established in social networks under an Islamic title tend to encourage participation on the part of children and adults. One stakeholder suggested that the culture in Bahrain and in many Arabic countries encourages unquestioning respect of Islamic initiatives. It was suggested that this often misleads people and leads them to encounter difficult or dangerous situations. As highlighted by one stakeholder from the University of Bahrain, these methods may also be used by people with an interest in children:

*"I assume that some unhealthy adults use Islamic symbols to attract children online. This is an area that I am currently investigating" (R 10, University of Bahrain)*

This problem was highlighted also by other stakeholders:

*"There is an issue of trust here as well. People in Bahrain tend to trust people quite easily but what we need to remind ourselves is that half of the population in Bahrain is foreign; and the majority are workers with a very low level of education. It is a very mobile nation. I come from a country where it is less relaxed than here because of the nature of the country. When I first moved here I couldn't relax; my children were running around the mall and I would try to control them. When I saw that people around me were relaxed then I also relaxed and in this way you lose the sense of awareness." (R3, ISP)*

*"We need a religious message which is common to all religions: Islamic, Jewish, Christian etc. "Love the other and learn to say no". In this country you will find nobody says no as it is not part of our culture" (R 5, Shura Council)*

The majority of the stakeholders from ISPs who participated in this study were in favour of protecting internet users in Bahrain and of promoting education to make children and their parents more aware of the dangers that may be encountered online. As this respondent suggested, this strategy should fit with ISP's values:

*"We can promote education by developing programmes; remind people of the dangers via brochures. This would be excellent for us also from the business point of view. So we can let people know that we are an ISP with a responsibility in the sense that we provide the Internet with a manual of also how to use it. This would really help us to position ourselves and uplift our values. We have a responsibility to contribute" (R 3, ISP).*

*"The use of the Internet is indispensable but it should be done with caution" (R 5, Shura Council)*

Furthermore, one of the issues that emerged is that of anonymity. A stakeholder shared some interesting insights and claimed that the main problem with children's use of the Internet is based on them feeling secure about their usage:

*"Because they use the Internet from home they feel they are secure and they lose the sense of danger. We teach them not to talk to strangers but because they speak to people via the computer, they feel they are safe. But it is not always the case" (R 7, NGO)*

It can be argued that the main difference between the real world and cyberspace is anonymity. Although it can be exciting and fun for children to go online and form new friendships, what should not be underestimated is that by affording anonymity the Internet allows anyone to be whoever they want to be, at any time and in any place (Davidson and Martellozzo 2008). Therefore, children may find that their virtual friends are not who they say they are on their online profile. While some children may feel confident with Internet use and may feel secure online, they still need adult help to make wise decisions.

However it should be emphasised that "just like the offline world, no amount of effort to reduce potential risks to children will eliminate those risks completely" (Byron 2008:5). In other words, it is not realistic to expect to make the Internet completely safe, but appropriate, culturally specific educational guidance directed at both children and their parents should serve to raise awareness.

### **10.6 Problems faced online**

One of the key issues raised by representatives of the Ministry of Health was that a number of young female teenagers (during 2009 and increasing in 2010) are interacting with teenage boys online, via Instant Messenger (IM) or social networking sites such as Facebook and Twitter. This social interaction has been hidden from parents as it is considered culturally unacceptable by some parents. As a representative of the Ministry of Social Development suggests:

*"Parents would not approve of this behaviour. It is a cultural issue" (R 6, MOSD)*

When the interaction is discovered, some feel threatened by their parents' reaction and some have been subjected to severe physical punishment on the part of their parents. Unfortunately a number of these interactions have resulted in the attempted suicide of the girls (there were seven such cases in April 2010). Although most of the interactions have occurred between young people, a minority have been perpetrated by adult males, although no meeting has taken place:

*"There have been cases where the interaction took place between the child and an adult but in these cases, the meeting did not take place" (R9, Ministry of Health)*

*"They would start to chat with friends via mobile or computers. They would then build a friendship and sometimes meet with them. Thank God they didn't reach the stage of sexual abuse or physical. The age is different. Sometimes it would be amongst children of the same age and sometimes the difference would be of two to three years- say for example she would be 12-13 and he would be 17-18" (R 9, MOH)*

One respondent suggested that given cultural constraints placed upon some girls, interacting with and meeting strange boys is unacceptable and girls are more controlled by their parents:

*"Girls shouldn't go out with a boy. This is not accepted in our society" (R 9, MOH)*

*"We have had cases that the children were assaulted by parents to the degree that they were admitted to the hospital. They would arrive to us with multiple bruises and severe injuries. Sometimes they are beaten up badly with the stick. Even if the parents know that the online relationship was innocent, even if she was just talking they would punish her. They would be punished not necessarily by the father but also by the uncles, the brothers" (R 9)*

From a review of the Child Protection Committee records, Psychiatric Hospital records, and Salmaniya Medical Complex computer database, 150 cases with the diagnosis of child abuse and neglect were identified for the period from June 1991 to July 2001 (Fadheela Al-Mahroosa, Fouad Abdulla, Susan Kamalb, and Al-Ansarib 2005). Furthermore, according to a statement by the social development minister, more than 135 children suffered abuse in Bahrain in 2009. The records shows that: "27 children did not receive any care, eight were abused psychologically, 32 abused physically and 70 abused sexually" (Gulf News 30/03/2010).

It is clear from the stakeholders' comments that the sexual and physical abuse of children occurs within Bahraini families, and is perpetrated by strangers, as it does in all other societies. There is evidence that the cultural context produces specific sometimes violent responses on the part of some parents to situations that are perceived to be unacceptable. Stakeholders have suggested that there is much work to be done in

raising awareness and educating parents regarding Internet use, but also in respect of appropriate responses to children. It was suggested that inventive ways of communicating with all sectors of the population be developed to achieve this end.

### 10.7 Stakeholder Recommendations

1. All stakeholders felt that there is an urgent need for a legislative framework that protects children from abuse in both the real world (the family, school and society in general) and in cyber space (internet grooming, abuse, cyber-bullying).
2. Stakeholders suggested that the proposed child protection legislation (including Clause 17 on internet 'luring') should be *enacted and implemented* with the agreement of key organisations and government departments such as the Ministry for Social development and the Ministry of the Interior.
3. Stakeholders suggested that key organisations should work collaboratively to ensure that should draft legislation be enacted, an action plan be developed to facilitate implementation. It was recommended that an organisation such as an e- Safety Forum or Council be formed to facilitate this process. The Council/Forum should include representatives from key Ministries, ISPs, NGOs, TRA and from the community.
4. Stakeholders suggested that there would be a need to train prosecutors and police officers if the draft child protection legislation is introduced, in order to ensure effective implementation.
5. Stakeholders were opposed to blanket blocking of the Internet and attempts to further control Internet usage. Some ISPs suggested that in the spirit of openness the community should be directly involved in discussions about blocking.
6. Stakeholders advocated the development of systematic approach to educational awareness training for children to be delivered in schools, possibly as part of the national curriculum, organised by the Ministry of Education with input from other ministries (Social Development for example) and organisations such as TRA and the ISPs . It was

recognised that different programmes should be developed to suit the public and private school sectors.

7. Stakeholders pointed to the existence of a digital divide between some parents and children that is particularly marked amongst lower social class groups where there is little computer literacy amongst parents. It was suggested that basic awareness training be provided along with basic computer literacy workshops.
8. Stakeholders suggested that there is much work to be done in raising awareness and educating parents regarding not only Internet safety issues, but also appropriate responses to children. It was suggested that inventive ways of communicating with all sectors of the population be developed to discourage the use of extreme physical punishment. It was suggested that NGO's and representatives from the Ministry of Social Development work with local communities via community groups and Mosques, for example, to this end.
9. Some stakeholders suggested that the media including television, newspapers and the radio should be used to raise awareness. However, the messages should be simple, short and easy to understand, aimed also at those who are new to the internet and technology in general:

*"The radio and television should be used. In our culture we watch television a lot and listen to the radio. People from Bahrain are prepared to listen. And of course newspapers are important. Although we think that nobody is reading, I believe that parents do. So I would include messages there as well" (R 7)*

*For those people that cannot read and write or cannot use computers, particularly the older generations we can use the visual more. We should create simple leaflets and leave them at the GP or hospitals for example, where everybody goes eventually" (R 7)*



## 10.8 Summary of key Findings

- The insights provided by the stakeholders are of great value particularly as research of this kind has not been conducted in the Middle East before.
- Stakeholder's insights have proved to be of great value because of the lack of the literature and research in this subject area. Child abuse reports for example, began to appear in the medical literature of the Arabian Gulf region only at the end of the 1980s and the beginning of the 1990s (Fadheela Al-Mahroosa, Fouad Abdullaa, Susan Kamalb, and Al-Ansarib 2005). However, the number of these reports remains quite limited and difficult to access.
- The fact that research data from the West on children's use of the Internet are widely available (Byron 2008; Davidson, Lorenz, and Martellozzo 2010; Livingstone and Bober 2005) does not imply that children in the East do not use the Internet and therefore are not exposed to risks. The Internet does not have any geographical boundaries and when children and adults navigate this useful tool, they are exposed to the same types of risks, whether they are located in the West or the East. As these findings have demonstrated, this lack of research and may reflect the fact that there is more awareness about child safety in the digital world in the West than in the East, but this assumption remains unproven.
- All stakeholders were extremely supportive of this research and are in favour of children and young people receiving the necessary education to remain safe online. They recognised that children use the Internet a great deal because it is fun and it is a fascinating learning tool. Children are inquisitive and will always be more adept users than their parents, will try to push boundaries and be prepared to take online risks (Davidson, Lorenz, and Martellozzo 2010). Thus, most of the stakeholders claimed that it is important to empower young people to stay safe and teach them to take responsibility for their own actions.

- All stakeholders recognised that there is a clear generational digital divide which suggests that parents do not feel equipped with the necessary tools to assist their children to stay safe.
- It was also suggested that there is a social class digital divide in the Kingdom- as poorer, less educated parents have lower computer literacy and understanding of Internet safety issues and may be more likely to exert extreme physical punishment in response to online peer communications on SNS.
- In relation to online abuse, stakeholders working in the child abuse area (MOH, MOE) and particularly those working with child victims of abuse and neglect support the view that the Internet “does not cause abuse”.
- All stakeholders felt that safeguarding children and adults is a complex agenda dependent on multidisciplinary collaboration involving Government Departments, NGOs, Social Services, Charities, Law Enforcement Agencies, the private sector and academic specialists.

## 11. Key Findings & Recommendations:

### 11.1 The Bahrain Context

- 1) This research has sought to put Internet safety at the centre of this Review and has gathered substantial empirical evidence from a variety of key sources. The research methodology is discussed in detail in Chapter 6.
- 2) In order to be able to make any recommendations, it is imperative to understand how people use the internet and other technologies within the context in which they live. Hence, the researchers have spent time in the '*field*' and have listened to the voices of children, parents, teachers and key stakeholders.
- 3) The internet is an excellent tool that is effective for education, entertainment and communication. Clearly the advantages of the Internet greatly outweigh the disadvantages, but adults and young people can be exposed to cyber fraud, cyber bullying, harmful content and harassment. This report supports findings that have emerged from other research undertaken in Europe and the United States, but has particular relevance also to the Middle East.
- 4) The way people use the internet is very much part of the culture in which the medium is used. Comparing the Bahrain position and the growth of Internet communications both in the country itself, the region and, indeed, the world is particularly interesting in the context of the region's cultural norms and what is considered to be acceptable (or not) in public and private life.
- 5) Sections 3 and 4 (adult survey and child/focus groups survey) show that internet use is very high in Bahrain's adult and child/young people population; mobile devices such as iPhones and Blackberrys are increasingly more popular.
- 6) Clearly it is becoming increasingly difficult to control Internet access as it becomes ever more omnipresent. Fixed, mobile, gaming machines, TV's, Wifi etc. all play a central role in life as they do elsewhere.
- 7) The connected world has access to a host of previously forbidden and/or inaccessible information and images. The opportunity to behave 'inappropriately' has increased, particularly as the medium is 'perceived' as being safe and anonymous.
- 8) This is particularly pertinent to children, as many feel safe and largely free from adult supervision. This seems particularly so in the Bahrain context as evidenced by the high proportion of young people who are trusting enough to meet with online strangers or 'virtual friends'.
- 9) In western cultures, children and adolescents are able to act out their pseudo grown up lives and new found 'cool' attitudes out of sight (without their parents'

knowledge). They are not concerned with, or do not feel empowered to, manage risk in the digital world in the same way as they do in the 'real' world. It can be argued that behaviours are the same in the Kingdom of Bahrain. The Internet represents a global community that unites different cultures and religions.

- 10) Home and school access has become widespread in many Middle Eastern countries, particularly Bahrain. As a result, adults and children are spending more and more time online. In order to navigate the information highway safely, people need good protective software on their PCs and other mobile devices, but they also need to be educated in good practice to protect themselves from fraud, cyber bullying, and exposure to harmful content and online abusers. This is especially important for children.
- 11) The advent of wireless technology means that young people can access the Internet remotely almost anywhere and away from parental supervision. So, how do we provide adequate road signs, speed limits and diversions to save ourselves and the more vulnerable from the dangers of dark country roads and bridge outages? As Byron pointed out: "Going online and playing video games may be more complex and diverse than crossing the road" (Byron, 2009).
- 12) The solution to providing a safe Internet environment is not simple; thus, a combination of advice, tools and rules to help everybody navigate the Internet safely and with understanding is needed. At the conference organised by FOSI and TRA (Bahrain, April 2010) the common recommendation focused upon the importance of educating teachers, empowering parents and guiding children.
- 13) The Provision of tools and packages that can be used to guard against malware and unknown sources is key as is the provision of a balanced legal framework to provide guidance and protection.

### **11.2 Summary of Key Findings: Adult Survey Data**

- The great majority (79%) of the adult population that participated in the online survey claimed to have more than 6 years' online experience. Only 30 people (4%) claimed to have less than one year's experience. This shows that the population of Bahrain has a high level of online experience.
- However, internet security awareness appears to be generally low. This assertion is supported by the high number of risks adults take online. The most common risks taken are the opening of email attachments that do not come from reliable sources (38.9%), receiving a virus from an email or download (35.8%), posting personal information on a website (31.9%) and sharing personal information with someone they have only met online (17.9%). There appears to be a high level of trust which was also evident from the child data.

- Adults are exposed to negative online experiences. More than half of the survey population (54%) said that they have received unwanted messages or material (spam, pornography, indecent messages) from people they don't know. However, they do not have the necessary knowledge and tools to avoid technical problems or to resolve them.
- Adults do not have a reliable source of information to consult regarding Internet advice. Most people used sources which were not necessarily reliable (e.g. friends, the internet, websites). People who are less confident about safety are those who are less knowledgeable about internet security (this finding is supported by recent research in the UK, National Audit Office, 2010). It can, therefore, be argued that people who can consult a reliable website will become more confident about their ability to be safe online and will be enabled to expand their online activities.

### 11.3 Summary of Key Findings: Child Survey and Focus Groups

- 16) Young people use the Internet an average of 2.5 – 3.5 hours every day. They use the Internet for a number of different reasons; mainly for homework purposes, to play games or to interact with other people. They connect through a multitude of ways: through instant messaging, chat rooms, games, blogging and Social Networking Sites (SNS). Although there are over 200 SNS, the most popular appear to be Facebook, Twitter and MySpace.
- 17) Young people enjoy posting pictures of themselves, videos, information about what they do and where they go. Unfortunately, it emerged that they do not have a great understanding of what is meant by personal information. There is clearly a lack of awareness regarding what is considered personal information and what is not. Most children for example, would freely post on their SNS profile what they do or where they are everyday.
- 18) It appears that children do not realise how public and accessible their information really is. A significant number of young people had their public profile on SNS set to public and did not know how to set it to private. This is indeed concerning. Mobile devices such as iPhones and Blackberries allow people to update their status every minute of the day making them constantly traceable and possibly vulnerable.
- 19) Older children in the 14-16 and 17-18 age groups took the most risks in terms of online safety; they were more likely to have shared personal information with a stranger and to have opened an email attachment from an unknown source than children in the 11-13 age group. This finding is consistent with data from a recent

UK study (Davidson, Lorenz, and Martellozzo 2010) and from research conducted in Europe (Livingstone, 2009).

- 20) A high number (43%, 1090) of young people had met with an online contact who they had not met in person before. This data indicates much higher proportions of children meeting with online contacts when compared to recent studies in Europe with 10% (Livingstone and Haddon 2009) and the UK with 7% (Davidson, Lorenz, and Martellozzo 2010). Muslims were more likely to meet a stranger than any other religious group (46% had) and children attending public schools were more likely to meet contacts (54% had) than children attending private schools (34% had). Public school girls were more likely to meet than private school girls.
- 21) The majority of the respondents took positive action in responding to unpleasant contact either by blocking or by closing the window. Only a minority of children would confide in either a friend (20% would), a relative (15% would) or a teacher (5% would). Communication seems to be an issue as young people appear unwilling to seek adult advice when they encounter problems online.
- 22) Children seem to enjoy their online privacy and protect their anonymity. As a result, they do not share their online experience with adults. The majority of young people claimed that their parents 'sometimes' or 'never' knew what they were doing online (52%).
- 23) Parents do not participate with their children online and learn the Internet 'habits' of their children and their friends. Findings indicate that a significant number of parents do not ask their children what they do online. A large proportion of respondents were allowed unsupervised access to the internet (87%) and there was little significant variation by nationality, religion, age or gender.
- 24) Cyberbullying was also identified as a problem, particularly in private schools. The consequences of such acts can be extremely damaging to the child. The internet has, however, facilitated bullying behaviour taking place via instant messaging and social networking sites. Teachers also suggested that cyberbullying or 'teacher humiliation' on SNS is becoming problematic.
- 25) Therefore, internet awareness should encompass training on cyber bullying and practice in the ethical use of technology. Of the 925 (36%) young people who claimed to have felt uncomfortable, the majority (79%) described cyber bullying behaviour including posting something unpleasant or the sending of an unpleasant email (23% had been asked to do something they did not want to do).
- 26) The majority of children (62%) had not received internet safety training at school. In the cases of those children who had received internet safety training advice, family or friends tended to be the source of that advice. Given that the

majority of children suggested that their parents knowledge was limited, this is of concern.

#### **11.4 Summary of Key Findings: Stakeholder Interviews**

- 1) In Bahrain there is no legislative framework that either seeks to protect children from Internet related or other forms of abuse, or that seeks to protect adults from cybercrime (other than basic e-transaction legislation passed in 2002).
- 2) A legislative framework in the child protection area which includes online 'luring' (grooming) and indecent child image production and collection is proposed.
- 3) Cybercrime legislation is also proposed.
- 4) There is a strong opposition to blanket blocking of the Internet and attempts to further control Internet usage. Educational awareness training for parents and children was instead strongly advocated.
- 5) Very little has been done to educate adults and children about internet safety.
- 6) The main difference between the real world and cyberspace is anonymity. Although it can be exciting and fun for children to go online and form new friendships, what should not be underestimated is that by affording anonymity the Internet allows anyone to be whoever they want to be, at any time and in any place (Davidson and Martellozzo 2008). Therefore, children may find that their virtual friends are not who they say they are on their online profile. While some children may feel confident with Internet use and may feel secure online, they still need adult help to make wise decisions.
- 7) A number of young female teenagers (during 2009 and increasing in 2010) are interacting with teenage boy's online, via Instant Massager (IM) or social networking sites such as Facebook and Twitter. This social interaction has been hidden from parents as it is considered culturally unacceptable by some parents. When the interaction is discovered, some feel threatened by their parents' reaction and some have been subjected to severe physical punishment on the part of their parents. Unfortunately a number of these interactions have resulted in the attempted suicide of the girls (there were seven such cases in April 2010).
- 8) Although most of the interactions have occurred between young people, a minority have been perpetrated by adult males, although no meeting has taken place.
- 9) The sexual and physical abuse of children occurs within Bahraini families, and is also perpetrated by strangers, as it does in all other societies. There is however evidence from stakeholders that the cultural context produces specific sometimes violent responses on the part of some parents to situations that are perceived to

be unacceptable. The Bahrain Child Welfare Centre works with children and their families involved in abuse, but it was suggested that further work be undertaken.

- 10) There is currently no willingness to prosecute cases of sexual abuse and physical abuse. There is no mandatory referral law in Bahrain, but there is a professional requirement for health professionals to refer abused children to the Child Protection Committee. However, there are currently no such requirements for other professionals, such as teachers or social workers, to report abuse. The proposed child protection legislation does however address this issue.
- 11) There is a strong social class digital divide in the Kingdom. Poorer, less educated parents have lower computer literacy and understanding of internet safety issues and stakeholders suggested that there may be a greater tendency to exert extreme physical punishment.
- 12) All stakeholders felt that safeguarding children and adults is a complex agenda dependent on multidisciplinary collaboration involving Government Departments, NGOs, Social Services, Charities, Law Enforcement Agencies, the private sector and academic specialists.
- 13) However, to be able to achieve the above, it was recognised that it is important to have a good legislative framework in place. All stakeholders felt that there is a need for legislation to protect children from abuse in both the real world (the family, school and society in general) and cyber space (internet grooming, abuse, cyber-bullying). The two issues cannot be easily separated.
- 14) Stakeholders emphasised the importance of ensuring that the proposed child protection legislation be introduced and that steps be taken to ensure that the legislation is implemented, this includes training for the police and prosecutors for example.
- 15) Stakeholders suggested that a national media campaign to raise awareness should accompany training programmes for children and parents.
- 16) Stakeholders recommended that an e-safety Committee be set to plan and implement the Kingdoms Internet safety strategy. The Committee should include a broad range of representatives from the government, NGOs, higher education, TRA, ISPs and community group.



## 12. Recommendations

The data presented in this report represent the views of a wide cross section of Bahraini society. The findings raise a number of issues which should inform the development of a comprehensive e-safety strategy. The recommendations are based on the key findings and have, for ease of reference, been divided under three main headings:

### 12.1 Education and information about internet safety

- 1) There is a need to teach adults and parents to be aware of the risks they, and ultimately their children, can be exposed to online. This can be achieved by the provision of basic cyber safety training and by encouraging adults to participate in cyber safety classes or parent evenings in schools.
- 2) There is a need to teach children to be aware of the risks they may be exposed to when online and the consequences such exposure may have. Furthermore, simple awareness is insufficient, there is a need to actually consider the risks and how they might affect them. It is important to remind children about safety, particularly when sharing personal information on Social Networking Sites.
- 3) Children need to be made aware that posting objectionable material or comments on their Facebook site, for example, may have long term consequences, such as jeopardising their future employment prospects. Furthermore, children should be made aware that everything they post represents a digital footprint that cannot be easily removed and sometimes cannot be removed at all.
- 4) Teachers need be trained to consistently deliver Internet safety messages. Some schools currently do teach their pupils Internet safety in a way that they regard as appropriate. However, it is important that messages reach each child in the same manner. This should be achieved by delivering a) regular lessons on internet awareness by social specialists and b) practical training session in labs.
- 5) Internet safety should be regularly addressed in schools because the internet is part of every child's life. Therefore, an awareness programme should be designed and delivered in each school as part of the curriculum.
- 6) People need to be able to rely on trustworthy, efficient and simplified information sources.
- 7) It is strongly recommended that the Muslim population should be educated about internet safety and be made aware that not all groups that are established in social networks under an Islamic title are genuine groups. Although the culture in

Bahrain and in many Arabic countries encourages unquestioning and respect for Islamic initiatives, it is imperative that this issue is addressed.

- 8) There is much work to be done in raising awareness and educating parents regarding not only Internet safety issues but also appropriate responses to children's online peer to peer activity. Creative ways of communicating with all sectors of the population should be developed to achieve this end.

## 12.2 Parental Involvement

Parents play a key role in educating children about online safety. They should be involved in their children's development and encouraged to have an open dialogue about internet safety with their children. This can be done in a number of different ways:

- 9) Parents should encourage their children to talk to them about any problems they encounter. If their children have made mistakes, parents should be supportive rather than judgmental. It is important, for example, to remember that it cannot always be assumed that young people make the choice to visit sites that are unsuitable.
- 10) Parents should ask their children to teach them to use the internet, particularly Social Networking Sites.
- 11) Parents should spend time visiting educational sites such as those on cyber bullying and plagiarism. This will help them to teach their children how to use the internet ethically. Respecting intellectual property is just one example of this.
- 12) Parents should be proactive in informing themselves and becoming knowledgeable on emerging digital technologies
- 13) Parents have to learn about technologies such as filtering software and should be aware that an unmonitored computer may give children access to inappropriate material as well as the possibility of their computer becoming damaged.
- 14) Parents should know that blocking their children from using the internet damages them more than helps them. We live in a digitally connected world and children need to be taught and encouraged to navigate through that world safely.
- 15) All adults, particularly those working with vulnerable children need to be familiar with online risks and need to be able to deliver key messages on internet safety.

## 12.3 Technical solutions

- 16) When considering technology, solutions (such as Client (PC based) solutions) that have been applied so far are not the only answer.

- 17) Internet users should be made aware of what to do to protect themselves and their families. ISPs could play a role in this by ensuring that consumers are informed.
- 18) Ultimately, the Internet Service Provider and Communication Service Provider (ISP/CSP) market needs to be more proactive in attempting to advise and protect consumers from obvious harm, and should provide simple tools in the network environment which will allow users to easily set up rules and policies that suit them and their children.
- 19) Internet experts suggest that this can be done in many ways. For example an approach often mentioned is a 'Walled Garden' where users (most likely, children) have access to a known and trusted basket of sites and content (FOSI/TRA Conference, 2010).
- 20) It is recommended that TRA and ISPs build upon the Memorandum of Understanding (MOU) that was signed at the FOSI/TRA conference in April 2010 and work together to build technical solutions to protect all users in the Kingdom.
- 21) ISPs should also play a role in collaborating with other agencies and organisations to ensure Internet safety and in the provision of safety advice to children.

#### **12.4 Government Involvement**

- 1) There is a need for a legislative framework that protects children from abuse in both the real world (the family, school and society in general) and cyber space (internet grooming, abuse, cyber-bullying).
- 2) The proposed child protection legislation should be enacted and implemented.
- 3) Stakeholders suggested stronger government engagement with ISPs but also with the community, including a consultation process regarding Internet safety.
- 4) It was strongly recommended by all key stakeholders that blocking or filtering material does not provide a sustainable solution, and that in the spirit of openness, the community should be directly involved in discussions about blocking.
- 5) The government should ensure that e-safety training is incorporated in the schools' curriculum across the Kingdom. Different training delivery approaches may be needed in the private and public schools sectors.
- 6) The government should ensure that all schools and local child services use a reputable filtering system.

### 12.5 Further research

- 7) The fact that research data from the West on children's use of the Internet are widely available (Byron 2008; Davidson, Lorenz, and Martellozzo 2010; Livingstone and Bober 2005) does not imply that children in the East do not use the Internet and therefore are not exposed to risks.
- 8) The Internet does not have any geographical boundaries and when children and adults navigate this useful tool, they are exposed to the same types of risks, whether they are located in the West or the East.
- 9) This project is the first large scale exploration of Internet safety in the Middle East region, further research should address the experience in other countries in the region and should evaluate progress made against the recommendations set out in this report in the Kingdom of Bahrain.

## 13. Key Recommendations

It is recommended that:

1. A high level committee should be established to set out and ensure implementation of the Kingdom's child e-safety strategy. The Bahrain Committee for Child Internet Safety (BCCIS) should include representatives from: Government ministries; the legal profession; relevant NGOs; child welfare organisations; academia; ISPs; TRA and key community groups. The strategy should be informed by the findings from this research and by good practice from other countries.
2. The proposed legislative child protection framework should be introduced and implementation in respect of the online luring (clause 17) and indecent image production and distribution (clause 129) clauses should be monitored by BCCIS;
3. A Bahrain Police High Technology Crime Unit should be established to provide a dedicated cybercrime policing function. Training for police officers and prosecutors should be introduced to ensure effective implementation of the new child protection legislation and the new cybercrime legislation (if introduced);
4. The use of restrictive measures using technology has to be fit for purpose and future proof. There is very little value in static measures in a dynamic web 2.0 internet;
5. There is an urgent need for an internet watch foundation model to tackle the issues of illegal use and act as a conduit for law enforcement management of cybercrime. The Bahrain Internet Watch Foundation should also monitor the implementation of the new cybercrime legislation to ensure effectiveness and consistency in approach;
6. There is a need to engage with international stake holders on policy, legislative and technology issues (i.e. best practices, Facebook, MySpace etc.);
7. ISPs and TRA should play an active role in providing safety advice and technical advice on computer protection to adult Internet users via their websites and public workshops.
8. A comprehensive age specific, Internet safety training programme should be developed for both the private and public school sectors as part of the curriculum. The programme should draw upon good practice from programmes developed in other countries, but should take account of the cultural context in Bahrain. The training should include safety information along with guidance on *ethical* online behaviour. An evaluation component should be built into the programme from the outset to enable monitoring and good quality control ;

9. Young people should be consulted on the most appropriate and effective means of delivering the programme and on programme design, in order to ensure maximum impact;
10. Schools should introduce a designated e-safety staff function to ensure that programmes are delivered on a rolling basis in each school and that outreach safety advice work is undertaken with parents;
11. Schools, NGOs and ISPs should play an active role in working with parents to raise awareness about Internet safety and about the nature of young people's online behaviour. Families in socially deprived areas might benefit from more informal advice offered via individuals trained in Internet safety awareness from community groups, NGOs and Mosques. The digital divide between generations currently allows young people the freedom to navigate the information highway largely free from parental guidance and supervision, this is more marked amongst the lower social classes.
12. A far reaching media campaign should be organised by BCCIS using a wide range of media including: Newspapers; television and radio. Safety messages should be clear and simple and designed to appeal to different audiences.
13. The e-safety strategy should be developed and implemented in stages within a specified time frame. Progress against agreed objectives should be monitored and evaluated by BCCIS 1 full year following initial implementation to enable review and further development of the strategy.
14. The first stage in the development the BCCIS should take the form of a high level, roundtable presentation of key Findings and recommendations from the research, to key stakeholder groups on publication of the report in September 2010.

## Bibliography

- ArabNetwork, Global.  
" <http://www.bahraingateway.org/index.cfm?fuseaction=document.home&id=995>.  
"
- Bahrain Internet Society BIS. <http://www.bis.org.bh/>.
- Beatbullying <http://www.beatbullying.org/abw/cyberbullying.html>.
- BeFree <http://www.befreecenter.org/News/-what-do-children-need-to-be-protected-over-the-internet.aspx>.
- Bourke, M.L and A.E Hernandez. 2009. "The 'Butner Study' redux: A report of the incidence of hands-on child victimization by child pornography offenders. ." *Journal of Family Violence* 24:183-191.
- Byron, T. 2008. "Safer Children in a Digital World. The report of the Byron Review ".
- Calder, M. 2004. *Child Sexual Abuse and the Internet: Tackling New Frontier*: Russell House Publishing
- Carr, J and Z Hilton. 2010. "Protecting children online." in *Internet Child Abuse: Current Research & Practice*, edited by J. Davidson and P. Gottschalk. London: Routledge.
- Castells, M. 1996. *The Network Society*. Oxford: Blackwell Publishers.
- Castells, M. 2004. *The Power of Identity*. Oxford: Blackwell Publishers.
- CRIOC Belgian centre for consumer group information and research. 2008.
- Cross, D. 2009. "Bullies Open New Front in Cyberspace."  
[http://www.waamh.org.au/upload/downloadFiles/Bullies\\_open\\_New\\_Front\\_in\\_Cyberspace.pdf](http://www.waamh.org.au/upload/downloadFiles/Bullies_open_New_Front_in_Cyberspace.pdf).
- Davidson, J and P Gottschalk. 2010. *Internet Child Abuse: Current Research and Practice*. London: Russell House.
- Davidson, J and P Gottschalk. 2010. *Online Groomers: Profiling, Policing and Prevention*. London: Russell House Publishing.
- Davidson, J. and E. Martellozzo. 2005. "'Policing the Internet and Protecting Children from Sex Offenders on Line: When Strangers Become Virtual Friends' "  
<http://www.oii.ox.ac.uk/research/cybersafety/extensions/pdfs/papers>
- Davidson, J., M. Lorenz, and E. Martellozzo. 2010. "Evaluation of CEOP ThinkUKnow. Internet Safety Programme and Exploration of Young People's Internet Safety Knowledge." *Centre for Abuse and Trauma Studies*.
- Davidson, J. and E Martellozzo. 2008a. "Internet Sex Offenders: Risk, Control and State Surveillance." in *Individual Freedom, Autonomy and the State*, edited by M. Johnson and S. Scalter. Cambridge: Hart Press.
- Davidson, J. and E. Martellozzo. 2008b. "Policing the Internet: Protecting Vulnerable Children From Sex Offenders In Cyberspace." *Police Investigations Police Practice & Research: An International Journal*.
- Davies et al. 2008. *The Learner and their Context - Benefits of ICT outside formal education*. Coventry: Becta.
- Elliott, I.A., A.R Beech, T. Mandeville-Norden, and E. Hayes. 2008. "Psychological Profiles of Internet Sexual Offenders." *Sexual Abuse: A Journal of Research and Treatment* 21:76-92
- Eynon, R. 2009. *Harnessing Technology: the Learner and their Context: How Young People use Technologies outside Formal Education*. Coventry: Becta.
- Fadheela Al-Mahroosa, Fouad Abdulla, Susan Kamalb, and Ahmed Al-Ansarib. 2005. "Child abuse: Bahrain's experience." *Child Abuse and Neglect* 29:187-193.
- Family Online Safety Institute. 2010. "[www.fosi.org](http://www.fosi.org)."
- Ferraro, M.M. and E. Casey. 2005. *Investigating Child Exploitation and Pornography: The Internet, the Law and Forensic Science*. New York: Elsevier Academic Press.
- Finkelhor, D. 1984. *Child Sexual Abuse; New Theory and Research*. New York: Free Press.

- Finkelhor, D., J. Kimberly, and J. Wolak. 2000. "On Line Victimization: a report on the Nation's Youth " National Centre for Missing and Exploited Children, Alexandria, Virginia
- Foundation for International Development Research. 2009. "[www.saferinternet.ru](http://www.saferinternet.ru)."
- Fortin, J. 2003. *Children's Rights and the Developing Law*. London: Lexis Nexis, Butterworths.
- Gallagher, B. 2008. "Dangerous worlds? The problems of international and internet child sexual abuse." *Journal of Safer Communities* 7.
- Gillespie, A. 2009. "Defining Child Pornography: Challenges for the Law." in *Global Symposium on Internet Abuse*. North Carolina.
- Gulf News. 30/03/2010. "<http://www.hurriyetdailynews.com/n.php?n=135-children-abused-in-bahrain-2010-03-30>."
- Hasebrink, U, S Livingstone, L Haddon, and K Olafsson. 2009. "Comparing children's online opportunities and risks across Europe: Cross-national comparisons for EU Kids Online." LSE, London, London.
- Hernandez, A, E. April 5-7, 2009. "Psychological and Behavioural Characteristics of child Pornography Offenders in Treatment " in *Global Symposium: Examining the relationship between online and offline offenses and preventing the sexual exploitation of children*. North Carolina.
- IWF. 2007. "2007 Annual and Charity Report." Internet Watch Foundation, London.
- IWF, <http://www.iwf.org.uk/media/news.archive-2009.258.htm>. 2009.
- Jones, T. 2003. "Child Abuse or Computer Crime? The Proactive Approach." in *Policing Paedophile on The Internet*, edited by A. MacVean and P. Spindler. Estbourne, East Sussex: The New Police Bookshop on behalf of The John Grieve Centre.
- kidscape.org.uk/cyberbullying. "<http://www.kidscape.org.uk/cyberbullying/>."
- Kierkegaard, S. 2008. "Cybering, online grooming and ageplay." *Computer Law and Security Report* 24:41-55.
- Klaine, E., H. Davis, and M Hicks. 2001. "Child pornography: The criminal justice system response." National Centre for Missing And Exploited Children Washington D.C. [www.missingkids.com/en\\_us/publications/NC81.pdf](http://www.missingkids.com/en_us/publications/NC81.pdf).
- Livingstone, S and L Haddon. 2009. "EU Kids Online: final Report." LSE, London.
- Livingstone, S and M. Bober. 2005. *Internet Literacy Among Children and Young People*, LSE
- Martellozzo, E. 2010. "Sex Offenders Use of the Internet " in *Internet Child Abuse: Current Research & Practice*, edited by J. Davidson and P. Gottschalk: Routledge.
- Ministry of Education. 2005. "Bahrain gears up to Create the Schools of the Future." [www.education.gov.bh](http://www.education.gov.bh).
- Mitchell, K.J., D. Finkelhor, and J. Wolak. 2005. *Internet and Family and Acquaintance Sexual Abuse*. Sage.
- Morgan, D. 2007. "Focus Group." in *The SAGE Dictionary of Social Research Methods*, edited by V. Jupp. London: Sage.
- National Audit Office. 2010. "Memorandum Staying Safe Online."
- NSPCC. 2007. "Sexual Abuse."
- Ofcom. 2009 "Digital Lifestyles: Young adults aged 16-24." [http://www.ofcom.org.uk/advice/media\\_literacy/medlitpub/medlipubrss/digital\\_young/](http://www.ofcom.org.uk/advice/media_literacy/medlitpub/medlipubrss/digital_young/).
- Quayle , E and M Taylor. 2002. "Paedophiles, Pornography and the Internet: Assessment Issues." *British Journal of Social Work*:863-75.
- Quayle, E. and M. Taylor. 2003. "Model of Problematic Internet Use in People with a Sexual Interest in Children." *Cyber Psychology & Behaviour* 6.
- Robbins, P and Darlington R. 2003. *The Role of the Industry and the Internet Watch Foundation*, Edited by MacVean and Spindler. New police Bookshop.
- Robson, C. 2002. *Real World Research*. Oxford: Blackwell Publishing.
- Webster, S., J. Davidson, A. Bifulco, T. Pham, and V Caretti. 2009. "European Online Grooming Project : Progress Report Covering Period: 1 June 2009 - 31 December 2009."



Wolak, J., Finkelhor D., and K.J. Mitchell. 2005. "Child Pornography Possessors arrested in Internet-related Crimes." National Centre for Missing & Exploited Children.

Unicef. 1989. "United Nations International Convention on the Rights of the Child, 1989." [www.unicef.org](http://www.unicef.org).

## 14. Appendix One: Adult Survey (in English)

Q no.	Question	Instructions/hosting notes
	<b>SCREENING QUESTIONS</b>	
<b>Q1</b>	<b>What is your gender?</b> <ul style="list-style-type: none"> <li>• Male</li> <li>• Female</li> </ul>	Single response Link to gender quotas
<b>Q2</b>	<b>What is your age?</b>	Numerical response
<b>Q3</b>	<b>What is your nationality?</b>	Single, open response Link to nationality quotas
<b>Q4</b>	<b>Do you have children?</b> <ul style="list-style-type: none"> <li>• Yes</li> <li>• No</li> </ul>	Single response
<b>Q5</b>	<b>If yes, how many?</b>	Only if 'yes' to Q4 Numeric, single response
	<b>INTERNET USE</b>	
<b>Q6</b>	<b>How do you connect to the Internet?</b> <ul style="list-style-type: none"> <li>• Desktop PC</li> <li>• Laptop</li> <li>• iPhone</li> <li>• Blackberry</li> <li>• Other mobile device – please state</li> </ul>	Multiple response
<b>Q7</b>	<b>In which ways have you used the internet in the last three months?</b> <ul style="list-style-type: none"> <li>• Spent time with my friends</li> <li>• Sent and received emails</li> <li>• Instant messaging</li> <li>• Social networking sites such as Facebook</li> <li>• Looked at chat rooms, discussion or blogs</li> <li>• Played games online</li> <li>• Downloaded music or movies</li> <li>• Looked for information about hobbies and personal interests</li> <li>• Looked for information for work or homework</li> <li>• Other (please specify)</li> </ul>	Multiple response

<b>Q no.</b>	<b>Question</b>	<b>Instructions/hosting notes</b>
<b>Q8</b>	<b>How much time do you spend online in an average day? Please include time spent sending and receiving emails.</b> <ul style="list-style-type: none"> <li>• None</li> <li>• Less than an hour</li> <li>• One to two hours</li> <li>• Three to four hours</li> <li>• More than four hours</li> </ul>	Multiple response
<b>Q9</b>	<b>Where do you use the Internet?</b> <ul style="list-style-type: none"> <li>• Work</li> <li>• Home</li> <li>• Cyber-cafe</li> <li>• School</li> <li>• Other – please state</li> </ul>	Multiple response
<b>Q10</b>	<b>Do you use social networking sites?</b> <ul style="list-style-type: none"> <li>• Yes</li> <li>• No</li> </ul>	Filter, single response
<b>Q11</b>	<b>If yes, which ones do you use?</b> <ul style="list-style-type: none"> <li>• Facebook</li> <li>• MySpace</li> <li>• Twitter</li> <li>• Hi5</li> <li>• Yahoo 360</li> <li>• Bebo</li> <li>• Other – please state</li> </ul>	Only if Q6 if 'yes' to Q5 Multiple response
<b>Q12</b>	<b>How long have you been using the internet?</b> <ul style="list-style-type: none"> <li>• Less than 1 year</li> <li>• 1-2 years</li> <li>• 2-3 years</li> <li>• Between 3 and 6 years</li> <li>• More than 6 years</li> </ul>	Single response
<b>Q13</b>	<b>Have you ever shopped online?</b> <ul style="list-style-type: none"> <li>• Yes</li> <li>• No</li> </ul>	

Q no.	Question	Instructions/hosting notes
Q14	<b>If yes, which online which items have you bought?</b> <ul style="list-style-type: none"> <li>• Books</li> <li>• Music, films and other electronic entertainment products</li> <li>• Electronic devices, computer and office supplies</li> <li>• Items for home and garden (furniture, tools, appliances, etc.)</li> <li>• Groceries</li> <li>• Toys and child care items</li> <li>• Clothes and shoes</li> <li>• Cosmetics and Medicines</li> <li>• Other – please specify</li> </ul>	Only if 'yes' to Q13
Q15	<b>Which internet service provider do you use?</b>	Open response
<b>INTERNET SAFETY</b>		
Q16	<b>Have you ever done any of the following online? Please select all that apply to you.</b> <ul style="list-style-type: none"> <li>• Opened an email attachment that wasn't from a trusted source</li> <li>• <b>Posted personal information on a website</b></li> <li>• <b>Shared personal information with someone you only met online</b></li> <li>• <b>Received a virus from an email or download</b></li> <li>• <b>None of these</b></li> </ul>	Multiple response 'None' = exclusive
Q17	<b>Have you ever received unwanted messages or material (spam, pornography, indecent messages) from people you know?</b> <ul style="list-style-type: none"> <li>• Yes</li> <li>• No</li> </ul>	Single response
Q18	<b>If yes, did you know how to remove this material?</b> <ul style="list-style-type: none"> <li>• Yes</li> <li>• No</li> </ul>	Only if 'Yes' to Q17

<b>Q no.</b>	<b>Question</b>	<b>Instructions/hosting notes</b>
<b>Q19</b>	<b>How safe do you feel online?</b> <ul style="list-style-type: none"> <li>• Very safe</li> <li>• Safe</li> <li>• Somewhat safe</li> <li>• Not very safe</li> <li>• Not safe at all</li> </ul>	Single response
<b>Q20</b>	<b>Do you feel you know enough about staying safe online?</b> <ul style="list-style-type: none"> <li>• Yes</li> <li>• No</li> </ul>	Single response
<b>Q21</b>	<b>Have you received or looked for advice about internet safety?</b> <ul style="list-style-type: none"> <li>• Yes</li> <li>• No</li> </ul>	Single response
<b>Q22</b>	<b>Where did you get advice about internet safety?</b> <ul style="list-style-type: none"> <li>• Friends or relatives</li> <li>• An anti-virus company</li> <li>• A website</li> <li>• Other (please specify)</li> <li>• Can't remember</li> </ul>	<b>ONLY IF "Yes" at Q21</b> Multiple response 'None' and 'Don't know' = exclusive
<b>Q23</b>	<b>Do you use internet safety software (anti-virus, firewalls, etc.)?</b> <ul style="list-style-type: none"> <li>• Yes</li> <li>• No</li> </ul>	Single response
<b>Q24</b>	<b>If yes, which software do you use?</b>	<b>Only if 'yes' at Q23</b>

**Thank you for completing the survey.**

## 15. Appendix 1: Adult Survey (in Arabic)

### مراجعة الوضع في مملكة البحرين بالنسبة للسلامة على الإنترنت 2010

#### استطلاع آراء مستخدمي الإنترنت

الأستاذة جوليا ديفيدسون والدكتورة إيلينا مارتيلوزو بالنيابة عن  
هيئة تنظيم الاتصالات بمملكة البحرين

يهدف هذا الاستبيان إلى التعرف على آرائك وخبراتك حول الطريقة التي تستخدم بها الإنترنت. وستساعد النتائج المستخلصة من هذا البحث على التعرف على ممارسات وسياسة السلامة على الإنترنت في جميع أنحاء مملكة البحرين.

ويجري حالياً القيام بهذه الدراسة من قبل باحثين مستقلتين بتكليف من الهيئة وهما الأستاذة جوليا ديفيدسون، جامعة كنغستون، لندن والدكتورة إيلينا مارتيلوزو، جامعة ميدلسكس، لندن بصفتها مديرتي هذا البحث. وسوف يدير هذا البحث محلياً الدكتور خالد المطوع، جامعة البحرين.

وسوف يتم التعامل مع أية معلومات تزودنا بها بسرية تامة ولن يتم إرفاق الأسماء مع الاستبيانات. يرجى الرد على هذا الاستطلاع في موعد أقصاه يوم الاثنين، الموافق 8 مارس 2010.

Instructions/hosting notes	السؤال	رقم السؤال
	أسئلة عامة	
Single response Link to gender quotas	ما هو جنسك؟ • ذكر • أنثى	س1
Numerical response	كم عمرك؟	س2
Single, open response Link to nationality quotas	ما هي جنسيتك؟	س3
Single response	هل لديك أبناء؟ • نعم • لا	س4
Only if 'yes' to Q4 Numeric, single response	إذا كانت الإجابة بنعم، كم عددهم؟	س5
	استخدام الإنترنت	
Multiple response	ما الذي تستخدمه للاتصال بالإنترنت؟ • حاسوب شخصي • حاسوب محمول • أي فون iPhone • بلاكبيرى Blackberry • جهاز متنقل آخر – يرجى ذكر ذلك	س6

Instructions/hosting notes	السؤال	رقم السؤال
Multiple response	<p>لأي غرض قمت باستخدام الإنترنت في الأشهر الثلاثة الماضية؟</p> <ul style="list-style-type: none"> <li>• قضاء الوقت مع الأصدقاء</li> <li>• إرسال واستلام رسائل البريد الإلكتروني</li> <li>• الرسائل الفورية</li> <li>• مواقع الشبكات الاجتماعية، مثل الفيس بوك</li> </ul> <p><b>Facebook</b></p> <ul style="list-style-type: none"> <li>• المحادثات، مناقشات أو بلوغز <b>Blogs</b></li> <li>• لعب الألعاب على الإنترنت</li> <li>• تنزيل الموسيقى أو الأفلام</li> <li>• البحث عن معلومات حول الهوايات والاهتمامات الشخصية</li> <li>• البحث عن معلومات تتعلق بالعمل أو الواجبات المنزلية</li> <li>• أخرى (يرجى ذكر ذلك)</li> </ul>	س7
Multiple response	<p>كم تستغرق من الوقت على الإنترنت في اليوم في المتوسط، بما في ذلك الوقت الذي تقضيه في إرسال واستلام رسائل البريد الإلكتروني؟</p> <ul style="list-style-type: none"> <li>• لا يوجد</li> <li>• أقل من ساعة واحدة</li> <li>• ساعة إلى ساعتين</li> <li>• ثلاث إلى أربع ساعات</li> <li>• أكثر من أربع ساعات</li> </ul>	س8
Multiple response	<p>أين تستخدم الإنترنت؟</p> <ul style="list-style-type: none"> <li>• في العمل</li> <li>• في المنزل</li> <li>• في مقاهي الإنترنت</li> <li>• في المدرسة</li> <li>• أخرى – يرجى ذكر ذلك</li> </ul>	س9
Filter, single response	<p>هل تستخدم مواقع الشبكات الاجتماعية؟</p> <ul style="list-style-type: none"> <li>• نعم</li> <li>• لا</li> </ul>	س10



Instructions/hosting notes	السؤال	رقم السؤال
<p>Only if 'yes' to Q10</p> <p>Multiple response</p>	<p>إذا كانت الإجابة بنعم، ما هي المواقع التي تستخدمها؟</p> <ul style="list-style-type: none"> <li>• الفيس بوك Facebook</li> <li>• ماي سبيس MySpace</li> <li>• تويتر Twitter</li> <li>• هاي فايف Hi5</li> <li>• ياهو 360 Yahoo 360</li> <li>• بيبو Bebo</li> <li>• أخرى – يرجى ذكر ذلك</li> </ul>	س11
<p>Single response</p>	<p>منذ متى وأنت تستخدم الإنترنت؟</p> <ul style="list-style-type: none"> <li>• أقل من سنة واحدة</li> <li>• سنة إلى سنتين</li> <li>• سنتان إلى ثلاث سنوات</li> <li>• بين ثلاث وست سنوات</li> <li>• أكثر من ست سنوات</li> </ul>	س12
	<p>هل سبق لك وأن قمت بالتسوق على الإنترنت؟</p> <ul style="list-style-type: none"> <li>• نعم</li> <li>• لا</li> </ul>	س13
<p>Only if 'yes' to Q13</p>	<p>إذا كانت الإجابة بنعم، ما الذي قمت بشرائه؟</p> <ul style="list-style-type: none"> <li>• كتب</li> <li>• أدوات موسيقية، أفلام ومنتجات ترفيهية إلكترونية</li> <li>• أجهزة إلكترونية، حاسوب ومعدات المكاتب</li> <li>• أدوات للمنزل والحديقة (أثاث، أدوات، أجهزة، إلخ)</li> <li>• سلع</li> <li>• لعب الأطفال وأدوات رعاية الطفل</li> <li>• ملابس وأحذية</li> <li>• مستحضرات تجميل وأدوية</li> <li>• أخرى – يرجى ذكر ذلك</li> </ul>	س14

رقم السؤال	السؤال	Instructions/hosting notes
س15	ما هو مزود خدمة الإنترنت الذي تتعامل معه؟	Open response
	السلامة على الإنترنت	
س16	هل سبق لك وأن قمت بأي من التالي على الإنترنت؟ يرجى اختيار ما ينطبق عليك. <ul style="list-style-type: none"> <li>• فتح مرفق برسالة إلكترونية دون التأكد من مصدر هذه الرسالة</li> <li>• نشر معلومات شخصية على موقع إلكتروني</li> <li>• المشاركة في معلومات شخصية مع شخص التقيته على الإنترنت</li> <li>• استلام فيروس من رسالة بريد إلكتروني أو من تنزيل برامج</li> <li>• لا شيء من هذه</li> </ul>	Multiple response 'None' = exclusive
س17	هل سبق لك وأن استلمت رسائل أو مواد غير مطلوبة (رسائل غير مرغوب فيها، مواد إباحية، رسائل غير لائقة) من أناس تعرفهم؟ <ul style="list-style-type: none"> <li>• نعم</li> <li>• لا</li> </ul>	Single response
س18	إذا كانت الإجابة بنعم، هل عرفت كيفية إزالة هذه المواد؟ <ul style="list-style-type: none"> <li>• نعم</li> <li>• لا</li> </ul>	Only if 'Yes' to Q17
س19	ما مقدار شعورك بالأمن على الإنترنت؟ <ul style="list-style-type: none"> <li>• الشعور بأمن كبير</li> <li>• الشعور بأمن</li> <li>• الشعور بأمن نوعاً ما</li> <li>• عدم الشعور بأمن كبير</li> <li>• عدم الشعور بأمن على الإطلاق</li> </ul>	Single response
س20	هل تشعر بأنك تعرف كيفية الاستخدام الآمن على الإنترنت بشكل كافٍ؟ <ul style="list-style-type: none"> <li>• نعم</li> <li>• لا</li> </ul>	Single response

Instructions/hosting notes	السؤال	رقم السؤال
Single response	هل سبق لك وأن تلقيت أو بحثت عن مشورة حول السلامة على الإنترنت؟ <ul style="list-style-type: none"> <li>• نعم</li> <li>• لا</li> </ul>	س21
ONLY IF "Yes" at Q21 Multiple response 'None' and 'Don't know' = exclusive	من أين حصلت على هذه المشورة؟ <ul style="list-style-type: none"> <li>• الأصدقاء أو الأقرباء</li> <li>• شركة مكافحة للفيروسات</li> <li>• موقع إلكتروني</li> <li>• أخرى (يرجى تحديد ذلك)</li> <li>• لا يمكن تذكر ذلك</li> </ul>	س22
Single response	هل تستخدم برنامج للسلامة على الإنترنت (برنامج مكافح للفيروسات، برنامج الفاير وولز firewalls، إلخ)؟ <ul style="list-style-type: none"> <li>• نعم</li> <li>• لا</li> </ul>	س23
Only if 'yes' at Q23	إذا كانت الإجابة بنعم، ما البرنامج الذي تستخدمه؟	س24

نشكركم على ملئ هذا الاستطلاع.

## 16. Appendix 3: Children Survey (in English)

Q no.	Question	Coding & filter Instructions
	<b>SCREENING QUESTIONS</b>	
<b>Q1</b>	<b>What is your gender?</b> <ul style="list-style-type: none"> <li>• Boy</li> <li>• Girl</li> </ul>	Single response Link to gender quotas
<b>Q2</b>	<b>What is your age?</b>	Numerical response, valid only between 11 and 17
<b>Q3</b>	<b>What is your nationality?</b>	Single response Link to nationality quotas
<b>Q4</b>	<b>Have you had any internet safety training at your school?</b> <ul style="list-style-type: none"> <li>• Yes</li> <li>• No</li> </ul>	Single response
	<b>INTERNET USE</b>	
<b>Q5</b>	<b>How much time do you spend online in an average day? Please include time spent sending and receiving emails.</b> <ul style="list-style-type: none"> <li>• None</li> <li>• Less than an hour</li> <li>• One to two hours</li> <li>• Three to four hours</li> <li>• More than four hours</li> <li>• Don't know</li> </ul>	Single response
<b>Q6</b>	<b>How do you use the Internet?</b> <ul style="list-style-type: none"> <li>• Desktop PC</li> <li>• Laptop</li> <li>• iPhone</li> <li>• Blackberry</li> <li>• Other (please state)</li> </ul>	Multiple response

Q no.	Question	Coding & filter Instructions
Q7	<p><b>How have you used the internet in the last three months?</b>  <b>Please tick all that apply.</b></p> <ul style="list-style-type: none"> <li>• Spent time with my friends</li> <li>• Sent and received emails</li> <li>• Instant messaging</li> <li>• Updated my profile on social networking sites such as Facebook</li> <li>• Looked at chat rooms, discussion or blogs</li> <li>• Posted things in chat rooms, discussion or blogs</li> <li>• Played games online</li> <li>• Downloaded music or movies</li> <li>• Looked for information about hobbies and personal interests</li> <li>• Looked for information for school work or homework, e.g. for an essay</li> <li>• Other (please specify)</li> </ul>	Multiple response
Q8	<p><b>Are you allowed to use the internet at home without an adult in the room?</b></p> <ul style="list-style-type: none"> <li>• Yes</li> <li>• No</li> </ul>	Single response
Q9	<p><b>Do you think your parents are aware of what you use the internet for?</b></p> <ul style="list-style-type: none"> <li>• Always</li> <li>• Sometimes</li> <li>• Never</li> </ul>	Single response
<b>INTERNET SAFETY BEHAVIOUR</b>		
Q10	<p><b>Have you ever done any of these things?</b>  <b>Please select all that apply to you.</b></p> <ul style="list-style-type: none"> <li>• Opened an email from someone you don't know</li> <li>• Opened an email attachment from someone you don't know</li> <li>• <b>Posted personal information on a website</b></li> <li>• <b>Shared personal information with someone you met online</b></li> <li>• <b>Received a virus from an email or download</b></li> <li>• <b>None of these</b></li> </ul>	Multiple response 'None' = exclusive
Q11	<p><b>Has anyone made you feel upset or uncomfortable online?</b></p> <ul style="list-style-type: none"> <li>• Yes</li> <li>• No</li> </ul>	Single response

Q no.	Question	Coding & filter Instructions
Q12	<b>If yes, how?</b> <ul style="list-style-type: none"> <li>• Saying something nasty</li> <li>• Asking me to do something I didn't want to</li> <li>• Sending a nasty email</li> <li>• Posting something about me on a social networking site</li> <li>• Other</li> </ul>	Only if 'yes' to Q11
Q13	<b>What information have you ever shared with people you have met online?</b> <ul style="list-style-type: none"> <li>• My real name</li> <li>• My age</li> <li>• My email address</li> <li>• My home address</li> <li>• My home phone number</li> <li>• My mobile number</li> <li>• My school</li> <li>• Photos of myself</li> <li>• Bank or credit card details</li> <li>• Login or password details for an online game</li> <li>• None of these</li> </ul>	Multiple response 'None' = exclusive
Q14	<b>Have you ever met in person, someone you first met on the internet?</b> <ul style="list-style-type: none"> <li>• Yes</li> <li>• No</li> </ul>	Single response
Q15	<b>If someone you don't know contacts you and you don't like them, or if they send something that makes you uncomfortable, what do you do?</b> <ul style="list-style-type: none"> <li>• Tell them you feel upset</li> <li>• Close the message or website immediately</li> <li>• "Block them" from accessing your account or profile</li> <li>• Tell a friend</li> <li>• Tell a relative</li> <li>• Tell a teacher at school</li> <li>• Other (please specify)</li> </ul>	Multiple response
	<b>INTERNET SAFETY AWARENESS</b>	
Q16	<b>Do you feel you know enough about staying safe online?</b> <ul style="list-style-type: none"> <li>• Yes</li> <li>• No</li> </ul>	Single response
Q17	<b>Have you received or looked for advice about internet safety?</b> <ul style="list-style-type: none"> <li>• Yes</li> <li>• No</li> </ul>	Single response

Q no.	Question	Coding & filter Instructions
Q18	<b>Where did you get advice about internet safety?</b> <ul style="list-style-type: none"> <li>• <b>Friends or relatives</b></li> <li>• <b>School</b></li> <li>• <b>An anti-virus company</b></li> <li>• <b>A website</b></li> <li>• <b>Other (please specify)</b></li> <li>• <b>Can't remember</b></li> </ul>	<b>ONLY IF "Yes" at Q15</b> Multiple response 'None' and 'Don't know' = exclusive

**Thank you for completing the survey.**

## 17. Appendix 4: Children Survey (in Arabic)

### SCREENING QUESTIONS

#### أسئلة عامة

Q1 Name of the student (Optional)

اسم الطالب اختياري

---



---



---


(126-129)

Q2 Serial Number of the student (Optional)

الرقم التسلسلي للطالب اختياري

---



---



---


(130-133)

Q3 **Check Gender Quota**  
What is your gender? (Single Answer)

Boy

..... ولد

Girl

..... بنت

ما هو جنسك؟

Code (134)	Route
1	
2	

Q4 What is your religion? (Single Answer)

Code (135)	Route
---------------	-------



هل بإمكانك اخباري ما هي ديانتك؟

Muslim

.....مسلم

Christian

.....مسيحي

Hindu

.....هندوسي

Others (please specify)

.....(أخرى) رجاء التحديد

1

2

3

4

Q5

What is your age? (Single Answer)

Code  
(136)

Route

كم عمرك؟

11 years

11 سنة

12 Years

12 سنة

13 Years

13 سنة

14 Years

14 سنة

15 Years

15 سنة

16 Years

16 سنة

17 Years

17 سنة

18 Years

18 سنة

1

2

3

4

5

6

7

8

Q6

What is your nationality? (Single Answer)

Code  
(137)

Route

ما هي جنسيتك؟

Bahraini

.....بحريني

Emirati

.....اماراتي

Kuwaiti

01

02

03

.....كويتي		
Omani		
.....عماني	04	
Qatari		
.....قطري	05	
Saudi Arabian		
.....سعودي	06	
Jordanian		
.....أردني	07	
Lebanese		
.....لبناني	08	
Syrian		
.....سوري	09	
Indian		
.....هندي	10	
Indonesian		
.....اندونيسي	11	
Pakistani		
.....باكستاني	12	
Philipino		
.....فلبيني	13	
Srilankan		
.....سريلانكي	14	
Algerian		
.....جزائري	15	
Egyptian		
.....مصري	16	
Iranian		
.....إيراني	17	
Moroccan		
.....مغربي	18	
Sudanese		
.....سوداني	19	
Tunisian		
.....تونسي	20	
American		
.....أمريكي	21	
British		
.....بريطاني	22	
Australian		
.....أسترالي	23	
Canadian		
.....كندي	24	
Others – Please specify.		
.....(أخرى) رجاء التحديد	25	

Q7

What is your School Name? (Single Answer)

ما هو اسم مدرستك ؟

Code (140)	Route

The British School of Bahrain	المدرسة البريطانية في البحرين	1	
Al Noor International School	مدرسة النور العالمية	2	
Isa Town Middle Boys Intermediate School	مدرسة مدينة عيسى الإعدادية للبنين	3	
Al Hidayah Boys Secondary School	مدرسة الهداية الثانوية للبنين	4	
Umm Salamah Middle Girls Intermediate School	مدرسة أم سلمة الإعدادية للبنات	5	
Hamad Town Secondary Girls School	مدرسة مدينة حمد الثانوية للبنات	6	
St Christopher's School	مدرسة سانت كريستوفرز	7	
The Indian School	المدرسة الهندية	8	

Q8	Have you had any internet safety training at your school?	Code (141)	Route
	هل قامت مدرستك بتدريبك في مجال السلامة على الإنترنت؟		
	Yes		
	..... نعم	1	
	No		
	..... لا	2	

#### INTERNET USE

#### استخدام الإنترنت

Q9	How much time do you spend online in an average day? Please include time spent sending and receiving emails?	Code (142)	Route
	كم تستغرق من الوقت على الإنترنت في اليوم في المتوسط، بما في ذلك الوقت الذي تقضيه في إرسال واستلام رسائل البريد الإلكتروني؟		
	None		
	..... لا يوجد	1	
	Less than an hour		
	..... أقل من ساعة واحدة	2	
	One to Two hours		
	..... ساعة إلى ساعتين	3	
	Three to Four hours		
	..... ثلاث إلى أربع ساعات	4	
	More than four hours		
	..... أكثر من أربع ساعات	5	
	Don't know		
	..... لا أعلم	6	

Q10	How do you use the Internet? <i>PROBE Please tick all that apply.</i>	Code (143)	Route
	ما الذي تستخدمه للاتصال بالإنترنت؟		

الرجاء إختيار كل ما هو مناسب PROBE

Desktop PC

.....حاسوب شخصي

Laptop

.....حاسوب محمول

iPhone

..... iPhone أي فون

Blackberry

..... Blackberry بلاكبيرى

Others (please specify)

..... (أخرى) يرجى ذكر ذلك

1

2

3

4

5

Q11

How have you used the internet in the last three months?

PROBE Please tick all that apply.

Code  
(144)

Route

لأي غرض قمت باستخدام الإنترنت في الأشهر الثلاثة الماضية؟

الرجاء إختيار كل ما هو مناسب PROBE

Spent time with my friends

.....قضاء الوقت مع الأصدقاء

Sent and received emails

.....إرسال واستلام رسائل البريد الإلكتروني

Instant messaging

.....الرسائل الفورية

Updated my profile on social networking sites such as Facebook

..... تحديث ملفي الشخصي على مواقع الشبكات الإجتماعية، مثل الفيس بوك Facebook

Looked at chat rooms, discussion or blogs

.....المحادثات أو المناقشات أو بلوغز Blogs

Posted things in chat rooms, discussion or blogs

..... نشر الأشياء في غرف المحادثات أو المناقشات أو بلوغز Blogs

Played games online

.....لعب الألعاب على الإنترنت

Downloaded music or movies

.....تنزيل الموسيقى أو الأفلام

Looked for information about hobbies and personal interests

..... البحث عن معلومات حول الهوايات والاهتمامات الشخصية

Looked for information for school work or homework, e.g. for an essay

..... البحث عن معلومات تتعلق بالمدرسة أو العمل أو الواجبات المنزلية، مثلاً كتابة مقال

Other (please specify)

..... (أخرى) يرجى ذكر ذلك

01

02

03

04

05

06

07

08

09

10

11

Q12

Are you allowed to use the internet at home without an adult in the room?

Code  
(146)

Route

هل يُسمح لك باستخدام الإنترنت في المنزل دون مراقبة من شخص أكبر منك؟

Yes

..... نعم

No

..... لا

1

2

Q13	Do you think your parents are aware of what you use the internet for? هل تعتقد بأن والديك على علم بالغرض الذي تستخدم الإنترنت من أجله؟	Code (147)	Route
	Always ..... دائماً	1	
	Sometimes ..... أحياناً	2	
	Never ..... أبداً	3	

### INTERNET SAFETY BEHAVIOUR

Q14	Have you ever done any of these things? Please select all that apply to you? <i>PROBE "None" = Exclusive</i> <i>PROBE Please tick all that apply.</i> هل سبق لك وأن قمت بأي من التالي على الإنترنت؟ يرجى اختيار ما ينطبق عليك <i>PROBE الرجاء إختيار كل ما هو مناسب</i>	Code (148)	Route
	Opened an email from someone you don't know ..... فتح رسالة بريد إلكتروني تلقيتها من شخص لا تعرفه	1	
	Opened an email attachment from someone you don't know ..... فتح مرفق برسالة بريد إلكتروني تلقيتها من شخص لا تعرفه	2	
	Posted personal information on a website ..... نشر معلومات شخصية على موقع إلكتروني	3	
	Shared personal information with someone you met online ..... المشاركة في معلومات شخصية مع شخص التقيته على الإنترنت	4	
	Received a virus from an email or download ..... استلام فيروس من رسالة بريد إلكتروني أو من تنزيل برامج	5	
	None of these ..... لا شيء من هذه	6	

Q15	Has anyone made you feel upset or uncomfortable online? هل شعرت بمضايقات من أحد على الإنترنت؟	Code (149)	Route
	Yes ..... نعم	1	Q16
	No ..... لا	2	Q17

Q16	If yes, how? <i>PROBE Please tick all that apply.</i> إذا كانت الإجابة بنعم، كيف؟ <i>PROBE الرجاء إختيار كل ما هو مناسب</i>	Code (150)	Route
	Saying something nasty ..... قول أشياء مقرفة لي	1	

Asking me to do something I didn't want to	2	
الطلب مني فعل شيء لا أريد في فعله		
Sending a nasty email	3	
إرسال رسالة بريد إلكتروني مقرفة لي		
Posting something about me on a social networking site	4	
نشر أشياء عني على موقع شبكة اجتماعية		
Other	5	
أخرى		

Q17	What information have you ever shared with people you have met online? PROBE "None" = Exclusive PROBE Please tick all that apply.	Code (151)	Route
	ما هي المعلومات التي قمت بمشاركتها مع أشخاص التقيتهم على الإنترنت؟ الرجاء إختيار كل ما هو مناسب PROBE		
	My real name	01	
	اسمي الحقيقي		
	My age	02	
	عمر		
	My email address	03	
	عنوان بريدي الإلكتروني		
	My home address	04	
	عنوان منزلي		
	My home phone number	05	
	رقم هاتف منزلي		
	My mobile number	06	
	رقم هاتفي المتنقل		
	My school	07	
	مدرستي		
	Photos of myself	08	
	صورتي الشخصية		
	Bank or credit card details	09	
	بيانات البنك الذي أتعامل معه أو بطاقة الائتمان		
	Login or password details for an online game	10	
	بيانات الدخول أو كلمة السر للعبة على الإنترنت		
	None of these	11	
	لا شيء من هذه		

Q18	Have you ever met in person, someone you first met on the internet? هل التقيت شخصياً بأحد التقيته أولاً على الإنترنت؟	Code (153)	Route
	Yes	1	
	نعم		
	No	2	
	لا		

Q19	If someone you don't know contacts you and you don't like them, or if they send something that makes you uncomfortable, what do you do? PROBE Please tick all that apply.	Code (154)	Route
-----	--	---------------	-------

إذا قام أحد لا تعرفه بالاتصال بك وأنت لا تحب ذلك أو إذا قام أحد بإرسال شيء إليك يضايقك، مالذي تفعله؟		
<i>PROBE</i> الرجاء إختيار كل ما هو مناسب		
Tell them you feel upset		
..... إخباره بأن هذا الشيء يضايقك	1	
Close the message or website immediately		
..... غلق الرسالة أو الموقع الإلكتروني على الفور	2	
"Block them" from accessing your account or profile		
..... حجب هذه الأشياء من الدخول إلى حسابك أو ملفك الشخصي	3	
Tell a friend		
..... إخبار صديقك بذلك	4	
Tell a relative		
..... إخبار قريبك بذلك	5	
Tell a teacher at school		
..... إخبار مدرسك بالمدرسة بذلك	6	
Other (please specify)		
..... أخرى) يرجى تحديد ذلك)	7	

## INTERNET SAFETY AWARENESS

التوعية بالسلامة على الإنترنت

Q20	Do you feel you know enough about staying safe online?	Code (155)	Route
	هل تشعر بأنك تعرف كيفية الاستخدام الآمن على الإنترنت بشكل كافٍ؟		
	Yes		
	..... نعم	1	
	No		
	..... لا	2	
Q21	Have you received or looked for advice about internet safety?	Code (156)	Route
	هل سبق لك وأن تلقيت أو بحثت عن مشورة حول السلامة على الإنترنت؟		
	Yes		
	..... نعم	1	Q22
	No		
	..... لا	2	
Q22	Where did you get advice about internet safety?	Code (157)	Route
	<i>PROBE 'None' and 'Don't know' = exclusive</i>		
	<i>PROBE Please tick all that apply.</i>		
	من أين حصلت على هذه المشورة؟		
	<i>PROBE</i> الرجاء إختيار كل ما هو مناسب		

Friends or relatives	الأصدقاء أو الأقرباء	1	
School	المدرسة	2	
An anti-virus company	شركة مكافحة للفيروسات	3	
A website	موقع إلكتروني	4	
Other (please specify)	أخرى (يرجى تحديد ذلك)	5	
Can't remember	لا يمكن تذكر ذلك	6	

**Thank you for completing the survey**

نشكركم على ملئ هذا الاستطلاع



## 18. Appendix 5: Focus Group Interview

### Interview Guide

#### 1. Introducing the Research and Confirming Consent

Interviews will begin with introductions and an explanation of the research aims in simplified terms. Confidentiality issues will be reiterated in keeping with Barnardos advice on researching children (see below). The researchers have applied this approach in work with children in the past and found it to be effective. The informed consent of the children participating in the research will have been obtained. Children will be informed that they may withdraw from the research at any time. Accessible language will be used to encourage participation and the research aims and expectations will be explained clearly. Children will be encouraged to question the researcher about the research and the methods. The procedure for confirming children's consent recommended by Barnardos will be adapted for use, this is cited below:

*Hi my name is (researchers first name), and I am researching (describe project briefly in appropriate language)*

*I would like you to (describe what you like the child to do. Don't use words like „help“ or „cooperate“, which can inform a subtle form of coercion)*

*Do you want to do this? (If the child does not give clear affirmative agreement to participate, you may not continue with this child) or Do you all want to do this? (For focus groups)*

*Do you have any questions before we start? (answer any questions clearly)*

*If you want to stop me at any time just tell me (if the child says to stop you must stop)*  
(Barnardos, p4, 2005)

#### 2. Assurance of confidentiality and anonymity

A statement regarding confidentiality and anonymity will be given, with the usual provisos. It is recognised that a minority of the children may have specific concerns over the confidentiality of their participation given their experiences. It is possible that children may have had negative online experiences and Barnardos (2005) recommend that limitations upon confidentiality should be addressed with children in the following way:

*„Whatever you have to say in this interview stays in this room unless you disclose („tell us“ seems preferable) that you or someone else is in danger of serious harm (this should probably be „harm“). In such a case I would need to report that to someone who might be able to help“- in the school (Barnardos, p5).*

Focus group leader to note gender, age, ethnic composition of group. Don't forget to assign a number to each child to avoid using real names.

### Interview Guide

#### A. Use of the Internet

1. Do you use the Internet? (ice breaker)
2. How much time do you usually spend online every day?
3. What do you do online? (explore)
4. Where is the computer you use the most? (probe – bedroom or family room, elsewhere, internet cafe', neighbourhoods' house)?
5. Do you have an iphone or Blackberry?
6. If so, what do you use it for?
7. Do you tell your parents what you do online?
8. Do your parents ask what you do online?

**B. General awareness of Internet safety and recollections of safety messages and sources (approximate in no of months or weeks)**

9. What do you know about staying safe online? (no prompt)
10. Do you belong to a social networking group (e.g. Facebook, Hi5)?
  - a. If yes, which one?
  - b. If yes, how many profiles do you use?
  - c. If yes, what information do you include in your profile? (Probe- messages, school name, pictures)
  - d. Approximately how many friends do you have on your social networking site/sites
  - e. How many of these friends have you met before?
  - f. Have you set your profile to private or public?
11. Do you use skype, Messenger, Paltalk rooms and other communication media to communicate with your friends?
12. Have you ever spoken to people you did not know who added to their list? (If so, probe the nationality of the person in the profile)
13. Did you add the person to your profile? (probe the reason why)
14. Is it ok to meet someone you've only spoken to online?
15. Have you done this? (If yes, explore)
16. Is it ok to post personal information?
17. Have you done this? (explore if yes)
18. What sort of personal information have you posted?
19. What do you consider 'personal' information?
20. Where do you save your data when you use computers at school, in cafes, in the library etc?
21. Have you ever felt uncomfortable online?

**C. Children's awareness of Internet safety**

22. Tell me how you stay safe online
23. Do you learn about Internet safety at school?
24. If yes, can you tell me about that?
25. Who told you about Internet safety? (probe- parents, friends, personal experience).
26. Have you discussed Internet safety with your parents?
27. How much would you say your parents know about the Internet and Internet safety?
28. Have you met up with someone you only talked to online?
29. Have you ever communicated with someone you haven't met via webcam?
30. Do you think you should be taught about safety in school?
31. How would you like a safety lesson to look like?

## 19. Appendix 6: Stakeholder Interviews

---

**Research Aim:**

The research aims to explore young people's (aged 7-18) experience and awareness of Internet use and Internet /other digital media safety in the Kingdom of Bahrain.

**Interview Objectives:**

- understand the current legislative and policy context of Internet safety in the Kingdom
- understand the current approach to Internet safety (children and adults)
- seek stakeholder recommendations regarding Internet safety practice and policy
- identify the stakeholders aspirations for the research

The Telecommunications Regulatory Authority (TRA) has asked us as independent academics to conduct this research. The project is lead by Professor Julia Davidson, from Kingston University, London and Dr Elena Martellozzo from Middlesex University. The research will be managed locally by Dr Khalid Al-Mutawah from Bahrain University. The research will include an online survey hosted by Nielsen (Research Agency) for a sample of children aged 11-18 and focus groups with children aged 7-18. Throughout the research careful consideration will be given to all relevant ethical aspects of this research to ensure strict adherence to codes of conduct:

*As this is an exploratory study, we wish to encourage participants to discuss their views and experiences in an open way without excluding issues which may be of importance to individual respondents and the study as a whole. Therefore, unlike a survey questionnaire or semi-structured interview, the questioning will be responsive to respondents' own experiences, attitudes and circumstances.*

## **INTRODUCTION**

*Aim: to remind the participant about the aims of the study, explain how the interview will be conducted, and how the data collected will be used.*

8. Introduce self and organisation
9. Reiterate the aims of the study
  - independence of researchers
  - review topics to be covered
  - recording of interview, data storage and DPA issues
  - confidentiality
  - how findings will be reported
  - length of interview – 1hour approximately

## **1. BACKGROUND AND LEGISLATIVE/POLICY OVERVIEW**

---

*Aim: to explore the stakeholder's current role /background and involvement in the Internet industry/Internet safety/NGO/Govt Dpt*

2. Nature of organisation/background and context
3. Current position / job title
4. Nature of role
5. Views on current legislative context regarding Internet safety

## **3. CURRENT APPROACH TO INTERNET SAFETY**

---

*Aim: To explore what the stakeholder considers to be the current context*

7. Views on context of Internet safety
8. *In interviewees experience what kind of problems do adults and children face online?(any examples)*
9. *In interviewees experience any problems specific to nationals? Non-nationals? Are there any differences?*
10. What has been done to address these?
11. Any other issues to consider?

## **4. RECOMMENDATIONS**

---

*Aim: To explore what should in the stakeholders view be done to address safety*

12. What should be done to address Internet safety with adults?(explore national/non-national issue)
13. What should be done to address Internet safety with children?(explore national/non-national issue)

14. What should ISPs do?
15. What should schools do?
16. What can be done to educate parents?
17. What role should TRA play?

## **5. ASPIRATIONS FOR THE STUDY**

---

*Aim: To explore the stakeholder's aspirations for the research and how it can have most applied value to them, their colleagues and organisation*

18. How could the research influence your practice/policy?
19. What are the most useful ways of hearing about research findings?
20. Other closing comments

### IMPORTANT

**AT THE END OF INTERVIEW THANK PARTICPANT FOR THEIR TIME.  
REITERATE THAT THE INTERVIEW WILL REMAIN CONFIDENTIAL. TELL  
THEM THAT THEY ARE WELCOLME TO CONTACT MEMBERS OF THE  
STUDY TEAM TO ASK QUESTIONS AT A LATER DATE IF THEY WISH.  
EXPALIN NEXT STEPS FOR THE STUDY**