REPORT TO: **POLICY AND RESOURCES COMMITTEE - 11 JUNE 2012**

REPORT ON: **DUNDEE STRATEGY FOR THE SAFE USE OF ELECTRONIC COMMUNICATIONS**

REPORT BY: **DIRECTOR, LEISURE AND COMMUNITIES**

REPORT NO: **186-2012**

1.0 PURPOSE OF REPORT

1.1 This report details the work undertaken in developing a Dundee E-Safety Strategy and Action Plan 2012-2015 linked to the Child Protection Inspection in February 2012.

2.0 RECOMMENDATIONS

It is recommended that Committee:

2.1 Approve the Dundee Strategy for the Safe Use of Electronic Communications (E-Safety Strategy) and Action Plan 2012-2015.

2.2 Agree that the Dundee Community Safety Partnership leads the implementation of E-Safety Strategy and Action Plan.

2.3 Confirms the Community Safety Manager as Dundee City Council's E-Safety Lead Officer.

2.4 Agrees to the formation of a Dundee E-Safety Group comprising representatives from Dundee City Council and its partner agencies.

2.5 Refers the report to the Dundee Partnership Management Group for their endorsement..

3.0 FINANCIAL IMPLICATIONS

3.1 Dundee Community Safety Partnership (DCSP) has allocated £1500 from its Commissioning Budget to E-Safety for the financial year 2012-2013. This was approved by Policy and Resources Committee on 23 April 2012. Report No: 143-2012 refers.

3.2 It is expected that Council Departments will continue to support the E-Safety strategy and action plan, by contributing resources in kind e.g. staffing, premises and materials as appropriate and that where budgets allow, finance may also be made available.

3.3 Potential external funding sources may be available for specific projects and all avenues for this will be explored.

3.4 It is expected that the majority of outcomes will be achieved by improving service coordination and maximising the resources currently available.

4.0 MAIN TEXT

4.1 In preparation for the Child Protection Inspection in February 2012, the Community Safety Manager was tasked as Interim E-Safety Lead to prepare an E-Safety Position statement by November 2011 for submission to the Inspection Team.

Whilst it was recognised that considerable work was being undertaken by the City Council and its partners, it was acknowledged that there was no strategic overview or direction for this work. Work on the position statement was progressed through the existing Internet Safety group.

4.2 An E-Safety Strategic Assessment was commissioned by the DCSP and produced by the Community Safety Partnership Analyst. This document highlights the current situation in Dundee across a range of E-Safety issues and is based on intelligence and information submitted by a number of agencies in Dundee who are aware of the issues and their impact on individuals and communities. The E-Safety Strategic Assessment can be found in Appendix 1, pages 3-24.

4.3 Based on the recommendations contained in the Strategic Assessment, an Action Plan for the period 2012-2015 has been produced and can be found in Appendix 2, pages 25-32.

4.4 The Action Plan is linked to the Dundee Single Outcome Agreement, specifically Dundee Outcome 3: Our children will be safe, healthy, achieving, nurtured, active, respected, responsible and included; and Dundee Outcome 7: Our communities will be safe and feel safe.

4.5 The Action Plan will be progressed by the Dundee E-Safety Group, which will report to the Dundee Community Safety Partnership, and the Child Care and Protection Committee, ensuring close liaison with Council Departments, the Dundee Partnership and other relevant agencies.

5.0 POLICY IMPLICATIONS

This report has been screened for any policy implications in respect of Sustainability, Strategic Environmental Assessment, Anti-Poverty, Equality Impact Assessment and Risk Management.

There are no major issues.

An Equality Impact Assessment has been carried out and will be made available on the Council website http://www.dundeecity.gov.uk/equanddiv/equimpact/

6.0 CONSULTATIONS

The Chief Executive, Director of Corporate Services, Head of Democratic and Legal Services, Director of Social Work, Director of Education, Chief Constable and the NHS Tayside Chief Executive have been consulted on the contents of this report.

7.0 BACKGROUND PAPERS

The following background papers have been referred to in the preparation of this report:

Dundee Single Outcome Agreement
E-Safety Strategic Assessment 2012

Stewart Murdoch
Director, Leisure and Communities
30 May 2012

E-Safety Strategic Assessment 2012

Foreword by

Dundee Community Safety Manager Liz Kay

Use of the internet and modern technology has changed our lives beyond imagining over the last twenty years. We have had amazing advances in science, medicine and entertainment. Whilst these advances have, for the most part, been welcomed, they do not come without concern.

E-safety as this area of concern has become known, has increasingly been on the agenda for those who work with children, young people, vulnerable adult groups and the wider community.

Dundee Community Safety Partnership is working to identify and to address these concerns so that we can ensure we are doing everything possible to mitigate the threat to the most vulnerable in our communities.

This strategic assessment has brought together the information currently available to Partners and will help us to identify the most significant threats allowing us to develop specific actions to address these.

By working together and combining our experience, knowledge, skill, resources and commitment, Dundee Community Safety Partnership will develop an action plan to address the issues identified and ensure our most vulnerable are safe and free from danger.

Liz Kay, Community Safety Manager

Acknowledgements:

The following people made contributions to this document, which were gratefully received:

June Jelly, Education Support Officer, ICT Secondary Schools, Dundee City Council

Carole Jenkins, Community Safety Worker, Communities Department, Dundee City Council

Kerstin Jorna, Senior Officer, Strategy & Performance, Social Work Department, Dundee City Council

Jen Keenan, Crime Reduction Officer, Tayside Police

Fiona Macpherson, Section Leader, Children's Library and Information Services, Dundee City Council

Ann Manzi, Children's Services Manager, Barnardo's Polepark Family Services

Contents

Summary of Findings

Current Picture

- Security on the schools network is increasing which is vital given the dynamic nature of the internet.

- Schools already make extensive use of 'Glow', 'ThinkUKnow', and DC2 platforms. All provide online safety advice for children as well as parents/guardians.

- Various members of the Internet Safety Group and wider Community Safety Partnership have received Child Exploitation & Online Protection training and as such Dundee is well placed to provide internet safety advice particularly for children. Other e-safety resources are also fully utilised.

- Four of the main fixed line Internet Service Providers to implement new code of practice by October 2012 which will mean customers will have to make a choice as to set parental controls or not. These changes will mean children and young people are protected further when connecting at home.

Risks and Emerging Trends

- Internet usage likely to increase in line with Scotland's Digital Ambition Strategy and the advancements in internet enabled devices. Although likely to bring benefits this will present the Community Safety Partnership with further challenges.

- Many parents/guardians have limited knowledge of technology safety, therefore unable to provide adequate advice on responsible use to children.

- Rise in popularity in smartphones and other internet enabled devices likely to result in less supervision of the internet by parents/guardians.

- Genuine concerns raised about the amount of online 'friends' children and young people have. Reluctance of some to accept that this sort of behaviour can be dangerous as internet provides the opportunity to purport a different identity.

- Posting too much information online particularly problematic for children as well as adults. Potentially this information could be used for online grooming, cyberbullying, or by fraudsters. General lack of knowledge regarding our 'digital footprint' and how this can impact negatively on people's lives.

- Lack of understanding of the negative impact that posting rude/hurtful comments on social networking sites can have. This is likely due to the lack of face to face contact.

1.0 INTRODUCTION

The following report is the first e-safety strategic assessment for the Dundee Community Safety Partnership (CSP). By establishing a strategic overview the partnership can provide an accurate picture of current priorities as well identifying emerging trends and potential risks. Thus the strategic assessment should drive forward the partnership's commitment to e-safety over the forthcoming years whilst helping set future direction by providing a basis of which to measure progress.

Following the 2008 Byron review of the risks children face from the internet and video games, *Safer Children in a Digital World* was published and the issue of e-safety for children was at the forefront. The foundations of this report were based on content, contact, and conduct. By classifying the online risk in this manner it was proposed that three strategic objectives of Reduce Availability, Restrict Access, and Increase Resilience would be achieved which would mean the risks to children online could be adequately managed[1]. One of the key recommendations made within the report was to establish a UK Council on Child Internet Safety. This resulted in the formation of the UK Council for Child Internet Safety (UKCCIS) which in 2009 set out its commitment towards helping children staying safe on online via the *UK Strategy for Child Internet Safety,* and launch of the digital code – Zip It, Block It, Flag It. Both the strategy and the digital code help lay the groundwork towards helping children and young people stay safe online whilst setting a precedence of achieving a more safe and responsible approach to internet use. In order to take this work forward Scotland wide the Government set out its commitment to child internet safety and its digital ambition via *Scotland's Child Internet Safety Action Plan 2010*, and *Scotland's Digital Future: A Strategy for Scotland 2011*.

Within the Scottish Government's 2010 Action Plan on Child Internet Safety 18 actions were identified which were underpinned by three overarching aims of Creating a Safer Online Environment, Giving Everybody the Skills, Knowledge and Understanding to Help Children and Young People Stay Safe Online, and Inspiring Safe and Responsible Use and Behaviour. These aims closely reflect the objectives of the *UK Strategy for Child Internet Safety, 2009* and as such will help inform the recommendations made within this report in order to provide strategic direction for the CSP in line with the national objectives.

Previously the issue of e-safety within schools was typically tackled on an ad-hoc basis which relied on interested members of staff to pursue this. Although there was an Internet Safety Group established there was not significant buy in from relevant persons/departments thus there was a lack of strategic direction. This was recognised by the CSP and the Children and Young Persons Protection Committee (CYPPC), and as such the CSP Manager has now been appointed interim lead responsible for e-safety within Dundee. It is envisaged that by having an e-safety lead; a strategic assessment; single point of contact (SPOCs) for each agency; as well as an action plan and monitoring framework, Dundee will be better placed to strategically respond to issues of e-safety. A questionnaire using Survey Monkey was also carried out during December 2011. Fifty two responses were received and although not fully comprehensive it gives the CSP a baseline of which to measure progress and details what has already been achieved so far. A copy of the survey results can be obtained from the CSP Manager.

Initially the scope of this strategic assessment was to be confined to the realms of child internet safety, however, after consultation with the Manager of the CSP it was agreed that e-safety is a far broader issue and as such should take the general population into consideration as adults are not immune to the dangers of the online environment.

It is widely recognised that the internet is a vital part of modern day life and is likely to be the greatest source of information for many. It can provide a range of opportunities for learning, development, and socialising for people of all ages. For children in particular this can be a positive experience but there are also associated dangers. Due to the vast array of information present on the internet people can come across inappropriate and irresponsible

[1] Safer Children in a Digital World, The Report of the Byron Review, 2008

material; which can potentially put children/young people and vulnerable adults at risk of harm. However, it's accepted that such risks should be managed adequately in order not to restrict the benefits the internet can provide to everyone.

This report will now provide an account of the current picture of e-safety as well as detailing priority areas, emerging trends and potential risks. This will be followed by a set of recommendations that aims to help the CSP move forward the issue of e-safety as well as taking cognisance of the national strategic objectives.

2.0 CURRENT PICTURE

According to the Office of National Statistics there were 41.62 million (82.9%) persons who had ever used the internet during the third quarter of 2011 in the UK[2]. When examining data Scotland wide, figures provided by Ofcom show that broadband uptake is 61% which falls below the UK average of 71%[3].

Internet usage is linked to a number of different factors such as social, economic, and demographics, and as such internet uptake often differs according to age. According to *The Internet Access Quarterly Update 2011 Q3* the largest population of internet users was in the youngest age group surveyed (16–24 age bracket), 98.6% of this age group had used the internet. This is contrast to the 72.4% of those aged 75 and over, who were non-users. This clearly illustrates the imbalance according to age, however, it is anticipated that future quarterly updates by the ONS will show an increased uptake within this age bracket with figures already showing an upward trend based on Q1 and Q3 of 2011 data alone, when there were 23.8% and 27.6% internet users respectively[4]. This likely increase also falls in line with Scotland's digital ambition of "the rate of broadband uptake by people in Scotland should be at or above the UK average by 2013, and should be highest among the UK nations by 2015"[5]. With this in mind it is crucial that awareness is raised about the potential dangers of the online environment that can impact on society.

2.1 Children/Young People and Adult users of the Internet

The amount of information contained within the internet is colossal some of which is trustworthy and reliable, whilst some pieces of information can purport mistakes, mistruths, misinformation and general propaganda due to the relative freedom the internet provides[6]. Internet users of all ages can potentially fall foul of one of the many pitfalls of the internet such as accepting misinformation, propaganda, scams, and cons. Unfortunately the internet has also provided new opportunities for those who wish to exploit children and the vulnerable. It has been noted that children's bedrooms are "increasingly becoming multi-media centres with televisions, webcams, games consoles"[7]. This of course can lead to less supervision of the internet and thus a greater degree of danger for children. Whilst the internet provides the opportunity to communicate and make new friends there are potential risks of online grooming through popular services such as instant messaging or social networking sites; where people can adopt a different identity and make contact with children or vulnerable persons. Cyberbullying is another of those risks which in part can be attributed to the lack of face to face contact. Cyberbullying occurs when a person is tormented, harassed, threatened, humiliated, embarrassed through the internet, interactive, digital technologies, or mobile phones[8]. Promotion of inappropriate websites such as those that promote suicide, pro-anorexia sites etc are also particularly problematic for vulnerable members of society. According to *Truth, Lies, and the Internet* many children in particular are not careful, discerning users of the internet. This is mainly because they are unable to find what they are looking for and trust the first thing they do. Furthermore, they fail to apply fact checks to their

[2] Internet Access Quarterly Update, 2011 Q3 - based on quarterly experimental statistics derived from the Labour Force Survey
[3] Scotland's Digital Future A Strategy for Scotland
[4] Internet Access Quarterly Update, 2011 Q1
[5] Scotland's Digital Future A Strategy for Scotland, P5
[6] Truth, Lies and the Internet: A Report into Young People's Digital Fluency, 2011
[7] Safer Children in a Digital World, The Report of the Byron Review, 2008 P112
[8] http://www.stopcyberbullying.org/what_is_cyberbullying_exactly.html

information, and are unable to recognise bias and propaganda. Subsequently, one such danger is children and young people becoming fascinated by extreme and violent ideas.

2.2 Terrorism

The internet can be exploited by terrorists and violent extremists as a means for operational purposes and as a means for radicalisation/recruitment. There are countless videos, speeches, audio statements that exist on the internet that are specifically designed to portray distorted views on religions and events. Such messages can often be seen by particularly vulnerable members of society, or they can be actively targeted, to engage with terrorism. There are case studies of young people becoming radicalised through the internet which has resulted in their detention. Due to the breadth of ideological and instructional information on the internet it can be a relatively easy place for persons to become immersed into a particular way of thinking and behaving. It can provide for certain members of society a feeling of belonging which they would not normally obtain through other means. Relationships can be developed online and become very strong which can allow for extremist views to become exacerbated and often go unchallenged within certain groups[9]. Steps have been taken within Scotland however and by way of addressing this is through development of the UK's counter terrorism strategy CONTEST; which aims to reduce the risk from violent extremism. *Prevent* is one strand of the CONTEST strategy which "aims to work with a wide range of partners to stop people from being drawn into violence and to respond to the ideology and threats that we all face from terrorism"[10]. The *Prevent* Community Engagement Officer for Tayside Police delivers a variety of workshops to partners such as WRAP and Operation Hindsight which are Home Office awareness raising exercises for front line professionals. ACT NOW and CONVICTION are interactive community terrorism exercises. It is envisaged that by having an increased number of partners trained to recognise the aims and objectives of Prevent; staff will be better equipped to protect vulnerable people whilst engaging with the wider community safety strategy.

Differences between children and adult users of the internet often mean that children are more likely to use the internet as a form of entertainment. Similarly adults use the internet as a form of entertainment also, but are more likely to use the internet as a means to gather information and to purchase goods and services. Subsequently, this can lead to differences in what children and adults view as appropriate. Furthermore, children may be more proficient users of the internet than their parents and as such have little parental control due to their parents/guardians having a limited knowledge of technology. This was reflected in the 2008 Byron Review when it was noted "age-related changes in internet use are also reflected in increasing parental concerns about the online world, and in the case of those parents with less experience of using technology, a declining sense of efficacy in managing their children's internet experience". However, as the report further concludes this can also lead to children being less likely to approach their parents/guardians regarding problems online due to the fact that they may not truly understand or overreact. Yet previous research has shown that the most common source of information concerning online safety is from parents/guardians, relatives, and schools[11]. This reinforces the need for parents/guardians to receive adequate support and guidance in order that they are competent users of the internet themselves. When examining this issue within a Dundee context it would appear to be a similar trend in that it is an ongoing challenge to engage with parents/guardians to learn about internet safety. Furthermore, there is a general lack of knowledge by some parents/guardians of age appropriate technology, games, and software. A subgroup of the Internet Safety Group has produced a presentation for parents/guardians about internet safety which has been delivered in various schools and community centres since June 2011, but with varying attendance success.

[9] Safeguarding Online, Explaining The Risk Posed By Violent Extremism
[10] http://www.tayside.police.uk/About-Us/Specialist-Units/Prevent
[11] Munch, Poke, Ping: Vulnerable Young People, Social Media and E-Safety, 2011

2.3 Schools

Schools and other services for children and families in particular play a significant role in helping children, and parents/guardians staying safe online, however, it was noted in the 2008 Byron Review that the schools approach to e-safety was neither coherent, comprehensive, nor consistent. Thus key recommendations were made to deliver e-safety through the curriculum as well as providing teachers and the wider children's workforce with the skills and knowledge they need. This was taken on board by the Scottish Government with the education platform now being seen as a core element of the Curriculum for Excellence. The implementation of 'Glow' was instrumental in driving forward the issue of e-safety and is Scotland's schools' intranet, which "provides pupils and teachers with a safe and secure online education community, allowing for joined up networking and learning". This was highlighted by the high user participation of which there 656,000 'Glow' accounts created for pupils, staff, and parents/guardians by January 2010[12]. 'Glow' has an acceptable user policy that all users agree to when they first login and Dundee schools make extensive use of this resource. With regards to general internet use there is a wide area network that serves all pupils and staff and is maintained and monitored centrally within all Dundee schools. Websense is the current net-nanny which protects children from accessing inappropriate material i.e. inappropriate sites are blocked for pupils, sometimes by age and stage. If a site is blocked because it is "uncategorised" or has been categorised incorrectly, teachers can and do request unblocking by re-categorising the site as "education". All users have logins to the Schools' Network so that it is solely for staff and learners. All users sign (or parents sign for younger children) an acceptable use policy before getting access to the network. The responsibilities and safeguards are revisited several times in a pupil's school career, and there are consequences for abuse of the network. Schools also mark internet safety day each year with appropriate assemblies. Security on the Dundee schools' network is increasing which is vital given the dynamic nature of the internet. It has been highlighted however that Websense prevents access to social networking sites so it is difficult to demonstrate to children how to protect themselves when on their home network or online via smartphones. Given the vital role schools play in teaching children internet safety it is essential that schools are given the opportunity to demonstrate to children how to protect themselves on social networking sites given their popularity.

Further progress has seen the establishment of the online 'ThinkUKnow' training tutorials and associated resources for all education professionals in Scotland delivered by the Child Exploitation Protection Centre (CEOP). Locally 'ThinkUKnow' training was run through Continuing Professional Development (CPD) online for staff in May and November 2011. A similar but uncertificated course was run for primary staff in April 2011. In addition to this all Information and Communication Technology (ICT) coordinators in nursery and primary schools across Dundee have received training on accessing and using a wide and varied range of resources to deliver internet safety to pupils on a one to one basis, group or class lessons and whole school assemblies. Internet safety will continue to be on ICT Coordinators' standing agenda. Both 'Glow' and 'ThinkUKnow' platforms provide national advice of online safety for children as well as parents/guardians, and provide direction to local CSP's of good practice, guidance, and discussions of relevant issues. DC2 (Dundee City Digital Classrooms) is Dundee's schools' homepage when users connect online and provides further advice on internet safety as well as authority guidance, acceptable user policy and links to educational materials, as well as other information concerning Dundee. Pupils as well as staff, parents and the public have access to the DC2.

Tayside Police Crime Reduction Officer delivers inputs specifically on technology safety in which all S1 classes within Dundee and offsite education units receive an input. The number of inputs delivered is dependant on the timetables, however, between 1-10 can be delivered per week. The inputs focus on convictions related to misuse of technology, blackmail and threatening behaviour via technology, sending of offensive material online. Through engagement with pupils it has been recognised that there is competition to gain as many online friends on social networking sites and this trend is increasing steadily amongst secondary school pupils. Through discussions with school pupils it was noted that one

[12] Scotland's Child Internet Safety Action Plan, 2010

female S1 pupil had over 1500 online friends which has obvious safety implications as it's unlikely that each one of those friends will be known personally. It has been recognised that there is a reluctance of many upper secondary pupils to acknowledge safe online relationships and alter their unsafe habits by removing personal information such as photographs, dates of births, addresses/telephone numbers, family members, daily routines, and checking into places via SMS which can then posted on social networking sites and allows people to view where you currently are.

Members of the Community Safety Team also provide internet and technology safety training to many different groups ranging from children (P6/P7/S1), young people and adults which include parent groups, community groups/organisations, and staff. Requests can be made directly to the team for their input who can also provide advice and guidance. The number of request has been on an upward trend since 2007/08 with schools being most likely to request further assistance. This is mainly due to the increase in the number of bullying/inappropriate incidents via technological means; which can obviously impact on school relationships. Community Safety Workers are CEOP ambassador trained which allows them to train others. They regularly update their knowledge with new training to ensure emerging technology safety issues are incorporated into training/talks. Dundee Community Safety Partnership, CYPPC and Peer Education Project have also developed 2 interactive DVDs (Upload and Mousetrap) and a number of quizzes which are used in conjunction with CEOP resources. These are used to teach children about the risks associated with the use and misuse of technology which include texting/sexting, social networking, internet use, gaming, and downloading.

Community Safety staff concentrate on giving messages about online and offline friendships, the importance of knowing who you are talking to and what information is being posted online. Whilst the adult presentation allows workers to give parents and carers information about the media landscape where children and young people live, discuss some of the risks and find solutions. Causes of concern have been raised by Community Safety Workers generally mirror those of teaching professionals, and SWD. Overall, there is a real concern about the number of children and young people with Facebook accounts that have no privacy settings, and the amount of personal information being posted. Typically, this is because there is a general lack of understanding of how to create safe profiles. It has also been recognised that it's difficult for children and young people to understand the impact of posting horrible comments online as they don't see the impact. Community Safety Workers have found that many primary schooled aged children will have between 200-300 online friends through various social networking sites as they simply do not recognise how easy it is to change your identity online. Stranger Danger talks are utilised in order to raise awareness of adults making contact with children purporting to be children. Through engagement with children there have been 3 Child Protection concerns raised by Community Safety workers due to this type of behaviour.

2.4 Vulnerable Children and Young People

Internet safety for children and young people cared and accommodated for by Social Work can result in additional concerns given the vulnerability of some of the residents. Locally, there have been concerns raised by Social Work Department (SWD) which include the increased access to pornography style images that are not classed as pornography on the internet, as well as increased access to more disturbing pornographic images. Furthermore, there have been instances whereby a high number of young people have reported receiving offensive photos, web images or messages through the internet. This can result in pressure on school aged children to emulate 'porn' style behaviour in terms of image and actions, including publishing of sexualised images on Facebook and other social networking sites. The formation of children's views can also be distorted of what is "normal" body and "normal" sexual relationships; which in turn can perpetuate further stereotypes, e.g. race, 'heteronormativity'. This can of course lead to disappointment and low self-esteem when the reality is different.

With increased ease of access and convergence of technology SWD have raised concerns that these types of incidents will not only continue but increase in frequency. However, steps

have been taken by SWD in order to address these risks in that all young people in Dundee residential units receive CEOP training. Members of the social work adolescent team have also undergone CEOP training and CEOP films and other resources are downloaded to young people's computers for training and education. A list of useful websites with e-safety quizzes and information for workers, parents, children and young people is also available, or SWD can download and print off these leaflets from the CEOP website. The 'Nae Danger' pack resource produced by FACE project is used regularly and includes a 'Traffic Light' assessment, as well as access to various reports on e-safety. Violence Against Women Partnership provides training for teachers and social workers regarding impact on teenagers of sexually explicit materials in mass media and also discusses the dangers of children taking images of themselves. Parents/guardians have mentioned possible information days to give out advice on internet safety and whilst information was provided to invite parents/guardians to sessions, however, it has been acknowledged they can be a difficult group to reach. Nevertheless, consultation with families and young people about safety forms part of SWD remit, and currently there is a written proposal to run a group for young people solely on the issue of safety. SWD have noted that although awareness can be raised regarding internet safety this will be rendered ineffective unless positive alternatives are offered such as other ways of making friends rather than via social network sites, and the emergence of alternative role models based on non-physical achievements etc.

2.5 Public Access

When considering libraries and other public access PCs log-on is administered by library staff through Discovery online booking system. Each user must have a valid library membership card, and must also agree to the online acceptable user policy before they can connect to any of the services offered such as internet and email etc. There are three age related levels of access; each password protected which is set weekly by library staff. Websense is also the net-nanny and prohibits access to inappropriate content. Locally, it had been highlighted that young people, particularly females, were claiming to be older than their true age or using older friends' membership cards in order to access social networking sites. However, this was addressed by adjusting the available levels of access to allow those aged 13 and upwards access to social networking sites. This falls in line with general policies such as Facebook.

2.6 Internet Service Providers

The issue of child internet safety has also been taken on board by the internet providers; which was highlighted in October 2011, when a new code of practice on parental controls was launched by UKCCIS which involved four of the major fixed line Internet Service Providers (ISPs). BT, Sky, TalkTalk, and Virgin are now committed to implement this code by October 2012. This will now mean new customers are presented with an unavoidable choice of whether to activate parental controls or not. Existing customers will also be given this choice though regular updates[13].

2.7 Changing Ways in which People Connect

It is widely recognised that simply blocking potential inappropriate material is not the solution; instead children and adults should be given the skills that will empower them to become savvy users of the internet. This issue has become more pertinent over previous years for children and young people with regards to the changing ways in which we now access the internet. Research has shown that people now connect to the internet in a multitude of ways rather than the typical home or work connection. The Internet Access – Households and Individuals 2011 opinions survey concluded that 45% (approximately 17.6 million) of internet users now connect via a mobile phone, whilst the use of wireless hotspots has almost doubled in the last 12 months to 4.9 million users[14]. The 16–24 age group saw the fastest

[13] http://www.education.gov.uk/ukccis/news/a00199819/isps-launch-new-code-of-practice-on-parental-controls– accessed 05/01/2012

[14] Please note that data used within this study was conducted January – March 2011 with around 1, 800 adults (those aged 16 and over) randomly selected each month. The sample is designed to ensure that the results represent the population.

growth when using a mobile phone to access the internet. Internet use via laptops, tablets, and other portable devices was also popular with 38% of internet users stating they had used either one of these devices to connect. This popularity is partly down to the WiFi as almost all laptops sold now have a built-in WiFi modem, and typically most ISP's provide a WiFi router within their service packages for new customers. WiFi quite simply it's a mechanism for wirelessly connecting electronic devices to the internet. The opinions survey noted further that 13% of internet users also now connect to WiFi hotspots across Great Britain such as hotels, airports, and cafes etc. When considering WiFi within Dundee libraries there is a guest log-on which is not filtered to any great degree as people are using their on devices to log on. It had been noted that its often difficult for library staff to monitor this type of usage, however, they do take responsibility if they become aware of inappropriate use or something suspicious is reported.

Given the rise in popularity in smartphone technology it's not surprising that this mode of connection to the internet has become popular amongst children. According to Ofcom's Children and parents: media use and attitudes report 41% of children aged 12–15 now own a smartphone; with 29% stating that they use their smartphone to go online at home[15]. Mobile connections can now potentially provide internet connection to multiple devices through a process known as 'tethering'. This is where the mobile internet connection of a mobile phone is shared with other devices to create a mobile hotspot[16]. This is particularly important for children and young people as they can connect to the internet via friends' devices unbeknown to their parents' or guardians.

Further advances with technology now means that 'cloud computing' is becoming increasingly popular amongst internet users. Information is stored in the 'cloud' and allows users to access their own information from various devices. Not only is this particularly useful for businesses as a third party hosts databases or software it also provides storage opportunities for residential internet users. Nowadays data such as documents, emails, photographs, and spreadsheets can be held in the 'cloud' with various companies providing this storage such as Apple, Microsoft, Google, and Dropbox. Typically, users are given basic storage for free but can upgrade to various levels of storage[17]. There are obvious security implications with 'cloud' storage as your data is held elsewhere, however, usually steps are taking by companies to encrypt this data as protection against hacking.

The internet, as the 2008 Byron Report states, provides users with "anonymity, ubiquity, and communication potential". Users of the internet can behave differently due to the lack of gate-keepers as well as the lack of visual cues that usually help towards moderating people's behaviour; whilst communications can spread throughout the world freely with little control. The dynamic nature of the internet will likely bring new benefits as well as challenges which present a challenge to the CSP, however, by having strategic direction and keeping abreast of emerging trends and issues the CSP can meet those challenges.

3.0 SMARTPHONES

Smartphones and mobile internet access has revolutionised they way we access the internet. Built on a mobile computing platform smartphones offers users access to online content, email and a variety of internet based applications. It has been estimated that there are 12 million smartphones users within Great Britain[18]. Smartphones offer applications, mobility and privacy for users that personal computers can't. The popularity of smartphones was highlighted in Ofcom's Communications Market Report, 2011 which reveals *the extent to which the UK has become addicted to smartphones, with people confessing to using them everywhere from the dining table to the bathroom and bedroom.* Thirty seven percent of adults and 60% of teenagers admitted to being "highly addicted" to this type of medium. It has been argued that mobile technology has helped towards creating an overlap of boundaries between work/school and leisure so much so that people have become

[15] Ofcom, Children and Parents: Media use and Attitudes Report, 2011
[16] Ofcom, Communications market Report: UK, 2011
[17] www.guardian.co.uk – accessed on 12/02/2012
[18] Ofcom, Communications market Report: UK, 2011

inseparable from their smartphones. Young people in particular are particularly affected by this whereby they now see continuous online engagement as normal[19].

3.1 Popularity of BlackBerry's amongst Children and Young People

The changing nature in which people connect clearly has significant safety implications for children in particular as it increases the likelihood they can access the internet out with parental control. BlackBerry's have become increasingly popular amongst young people with research indicating 37% of young people own a BlackBerry[20]. BlackBerry Messenger (BBM) is likely to be one such explanation for its popularity. This messenger system is free and allows BlackBerry users to send pictures, files, and audio. Users can interact with a network of others BBMers which effectively acts as a social networking platform[21]. It has been suggested that BlackBerry's played a significant role in the riots during August 2011. This was partly down to it being a free and easy way to broadcast messages, but significantly BlackBerry Messages are private to recipients and encrypted during transmission; a fact that many of the rioters were aware, it has been claimed. Other social networking platforms such as Twitter and Facebook where posts are often public would have allowed the Police to monitor ongoing developments, however, due to BlackBerry's secure network the rioters were able to plan and organise further riots whilst sharing information on Police activity[22]. Locally, SWD have had problems with this type of device through young people arranging to abscond and encouraging young people to abscond from their secure accommodation.

There are of course other dangers associated with smartphones as there is with an internet connection via a home PC or laptop. As noted previously adults as well as children are susceptible to online dangers and with internet connection via smartphone acting as a further mode of connection the partnership must also be aware of these dangers. Social networking is particularly prevalent amongst smartphone users and would appear to be the most popular internet service for adults; with 57% of users (aged 16 and over) spending on average five and a half hours on social networking sites a month[23]. For younger children (aged 8-15), who own a smartphone, tend to use their phone for a broader range of activities compared to children who own a regular mobile phone. Social networking is the most popular activity however with 44% stating they do this at least weekly[24].

3.2 Cyberbullying and 'Sexting'

Community Safety workers have come across instances of primary 4 children owning an I-phone and as such access to social networking sites out of sight from their parents/guardians. As with all communication means there is the potential for bullying, and inappropriate comments. Bullying is no longer confined to the school playgrounds or work place; it now can now take many forms due to the changing way in which we communicate. Cyber bullying via mobile phone, social networking sites does occur and can have the same devastating impact on people's life. According to Ofcom, one in four 12–15 year olds questioned knew of someone who had been bullied through a mobile phone in the past year. Furthermore, one in five of all 12–15 year olds questioned stated that they had personally had a negative experience of online or mobile phone activity in the past year; with the most prevalent issue being gossip being spread[25]. 'Sexting' is a concept developed with regards to sending sexually explicit images this can be through a variety of means such as text or posting images online. Typically, an image will be sent and intended for a specific individual, however, there is the potential for the image being passed to others without the owner's permission. This of course can lead to a great deal of distress for the victim, which can lead to bullying or harassment. It has been claimed children and young people become involved in this type of behaviour in order to show off, entice someone, show an interest someone, or prove commitment. According to UK charity Beatbullying 'sexting' appears to be on the increase

[19] Munch, Poke, Ping: Vulnerable Young People, Social Media and E-Safety, 2011
[20] http://www.bbc.co.uk/news/technology-14397101 – accessed on 13/01/2012
[21] Munch, Poke, Ping: Vulnerable Young People, Social Media and E-Safety, 2011
[22] http://www.guardian.co.uk/uk/2011/dec/07/bbm-rioters-communication-method-choice – accessed on 13/01/2012
[23] Ofcom, Communications market Report: UK, 2011
[24] Ofcom, Children and Parents: Media use and Attitudes Report, 2011
[25] Ofcom, Children and Parents: Media use and Attitudes Report, 2011

revealing that more than a third of under 18s in the UK have received offensive or distressing sexual images via their mobile or computer[26]. When considering these issues locally, SWD have raised concerns regarding bullying in which children or adolescents are photographed or filmed and the images are put online or sent to others via mobile phone. Children being encouraged to carry out sexual acts on a web camera or being asked to send intimate photographs through their mobile phones, or being filmed having sex which is then uploaded onto the internet or sent to others' mobile phones. There are serious harm and criminal implications with this sort of behaviour such as the sexual abuse of children, the emotional impact on vulnerable victims which potentially lead to self harm. As well as children/young people themselves being responsible for committing the crime of distribution of child pornography.

3.3 Global Positioning System and Security Implications

Smartphone technology also offers users Global Positioning System (GPS) which can detail a user's locations. This type of service has safety implications for both adults and children as it can possibly allow people unknown to them to ascertain home, work, and school locations. Similarly many smartphones offer Geotagging; this allows users to 'tag' photos with a geographic location in the form of latitude and longitude. There are numerous websites available that will allow users to upload photographs that display location details, one such popular site is Flickr. This allows users to upload photographs including details of titles, locations, and people. Such a service does have its benefits however given that people can set their own privacy controls can leave users open to abuse/revealing personal information.

3.4 Smartphone Malware

It has been suggested by Get Safe Online research that while online security remains a significant issue, mobile phones are now the new frontier for internet criminals; with mobile malware increasing by 800% in just for months based on Trend Micro's August 2011, Threat to Spotlight. Further research indicates that 66% of all smartphones users use their phone for social networking, 32% use it phone for work, 19% use it for shopping, and 17% use them for financial management. Online fraudsters, it has been claimed, are now utilising smartphones in order to access personal information and money by enticing users into downloading malware. Malware is malicious software and is often used as a generic term referring to any piece of software written with malicious intent or has a harmful purpose. Once downloaded malwares enables fraudsters to take control the victim's phone; allowing them to make calls, send and intercept SMS messages and voicemail messages. The fraudster can also browse and download online content which can give access to all personal and payment data available on the phone. This data can then be sold, and used by, identity fraudsters as well being used to 'spam' other mobile web users. One such example cited by Trend Mirco was fraudsters using this access to send SMS messages continuously to their own premium rate numbers. The victim is oblivious to this until they view their bill or it's flagged by their network provider who identifies suspicious activity[27].

4.0 GAMING AND OTHER MULTI MEDIA DEVICE ACCESS

Many electronic gaming devices now allow access to the internet, for example the following devices have internet capability Nintendo DS (NDS); Play Station 3; Play Station Portable (PSP)/Playstation Vita (PSV); Xbox 360; Ipad; and the Wii. Gaming can have an enormous potential to have a positive impact on people's lives as can help towards the development new skills. Typically, types of gaming will vary with age with both children/young people and adults increasingly using these methods as a means not only to game interactively but to communicate. Whilst it's easy to assume that gaming is confined to the younger generation it has been noted that the average age of the UK gamer is in their late twenties[28].

[26] www.vodafone.com – accessed 17/02/2012
[27] Spectrum, The UK's Fraud Prevention Service Newsletter, 2011
[28] Safer Children in a Digital World, The Report of the Byron Review, 2008

As with all online activity there are associated dangers with online gaming and for children and young people this is particularly significant as it can lead to playing games with persons unknown to them or accessing games which are not age inappropriate. This is highlighted in the Byron Review, 2008 when it's noted that it's not uncommon for children and young people to have played some of the most well known 18 rated titles. It is expected that this type of online connection will become ever more prevalent as the popularity of tablet computers and games consoles increases. According to Ofcom, one in five 16–24 year olds now access the internet via a games console[29]. Whilst two in ten 8–15 year olds go online via a fixed or portable games console/games player[30]. Whilst the main objective of such devices are for online gaming, parents and guardians are reminded that such devices can be open to abuse and hacking as with any internet connection. The issue of hacking was brought to the forefront in 2011, when Sony announced that criminals had successfully targeted the Playstation network, compromising the personal details of 100 million customers. This resulted in the network shutting for several weeks and costs are expected to total $171 million[31]. There are also issues surrounding player identity with reports from Ofcom noting that one quarter of boys (aged under 16) who play games online do so against people that are not known to them[32]. It is quite likely that parents/guardians may not acknowledge the associated dangers with this type of device. It is not unknown for people to give out personal details over this type of medium. Users of online games can purport a different identity and there are games which can aid this; grand theft auto allows users a voice change, therefore distorting perceptions of a player's opponent. Although certified an 18, Community Safety Workers have reported instances of primary school aged children owning such games. Furthermore, they have found this trend to be on the increase amongst younger children (P4 – P7) accessing 15+ or 18 certified games which have been bought by their parents.

4.1 Massively Multiplayer Online Role-Playing Games

Massively Multiplayer Online Roleplaying Games (MMORGs) are a type of online gaming which create online communities and social worlds have become increasingly popular. Participants can select, customise or create characters called 'avatars'. Avatars can allow players to build a virtual world and can be multi-player where players can interact and talk to each other during play. Sites popular amongst children include Moshi Monsters, Club Penguin, Habbo, Stardoll, Gaia, Second Life, World of Warcraft. Typically, new users will be given basic access and can enhance their environment or character through the completion of tasks, however they can also upgrade via a monthly subscription that will allow greater privileges. It has been suggested that 25% of players of these types of online role-playing games are under the age of 18, and spend on average 22 hours per week in this type of online virtual world[33]. Such games, although beneficial for social interaction and community aspects, also presents the same challenges as regular gaming in that participant's can create a false identity and children can access inappropriate content through avatars taking part in inappropriate activities. There have been several concerns raised about this type of entertainment regarding the relationship between fantasy and reality. Disclosure of personal details through instant chat functions when playing games can potentially lead to incidents of grooming and cyberbullying, and links to advertising sites which may not be appropriate. Conduct of the children themselves engaging in racist, sexist or abusive behaviour[34].

The Byron Review highlights that there is little data available about the negative impact of these types of technology on children's development. This is primarily because the pace in which the games industry moves at. There were also concerns made regarding the quality of parental controls, and the need to educate parents about how these are used. One of the recommendations made by the Byron review was that the UKCCIS initiate the formation of a sub-group of the online gaming industry and online gaming regulators to explore good practice in child safety for online games. This group was formed however given the change of Government during this time the group has since been disbanded. Nevertheless, members

[29] Ofcom, Communications market Report: UK, 2011
[30] Ofcom, Children and Parents: Media use and Attitudes Report, 2011
[31] The UK Cyber Security Strategy Protecting and promoting the UK in a digital world, 2011
[32] Ofcom, Children and Parents: Media use and Attitudes Report, 2011
[33] Safer Children in a Digital World, The Report of the Byron Review, 2008
[34] Safer Children in a Digital World, The Report of the Byron Review, 2008

of this group still actively participate in the UKCCIS current project groups, providing their expert knowledge to support the ongoing work of UKCCIS[35].

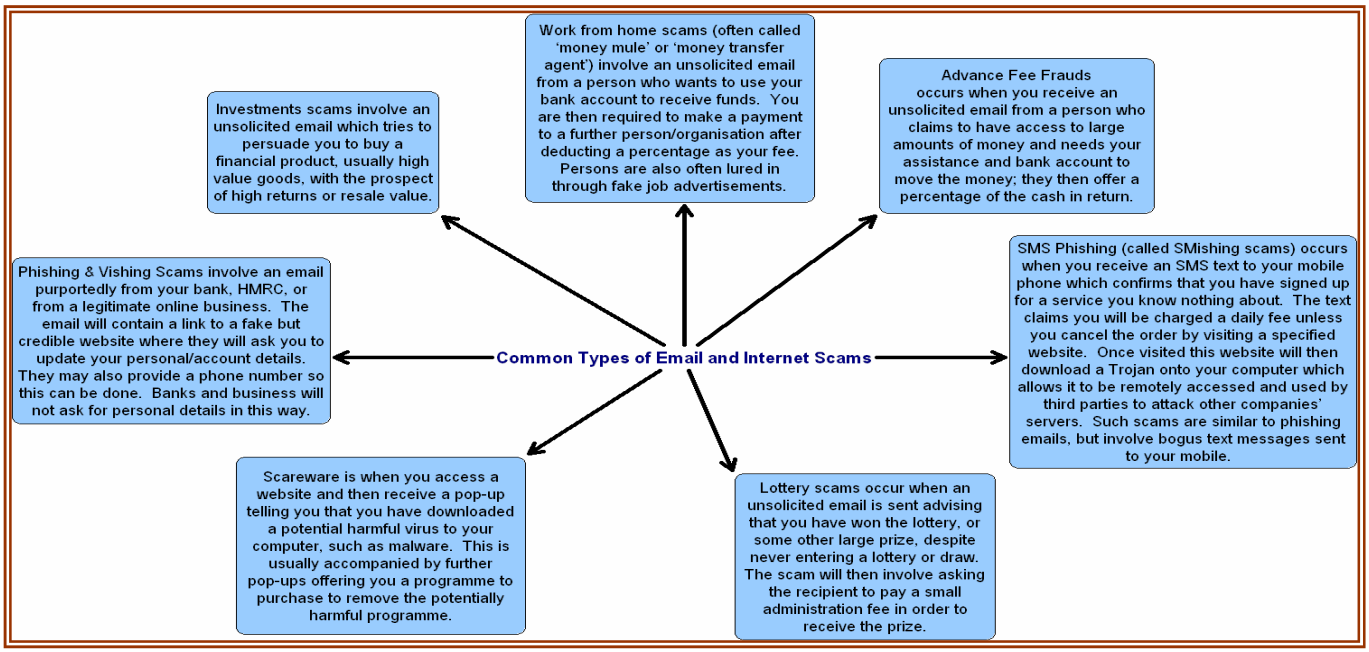
5.0 FRAUD AND INTERNET SCAMS

According to Get Safe Online's annual research, over 40% of computer users have claimed to have fallen victim to a virus attack[36]. This highlights the need for computer users to protect themselves against online fraud as well as being alert to new threats.

"E-crime generally refers to a criminal activity where a computer or computer network is the source, tool, target or place of a crime"[37]. Traditional crimes such as fraud, theft, blackmail, and forgery can also take place online thus highlighting the fact that e-crime is an overarching term used for a multitude of crimes. E-crime however is often difficult to detect simply because the crimes themselves are often very complex. Perpetrators can target victims from different countries which only contributes towards the difficulty of detection. Furthermore, technology is continually evolving with threats and risks a regular occurrence therefore reinforcing the need for Police and CSP to recognise these dangers and by being able to respond to these.

5.1 Fraud Types

Frauds are particularly prevalent online and typically designed to steal a victim's personal, bank account, or credit card details to use fraudulently. There are various types of frauds including advance fee frauds, (also known as 'West African 419' frauds), lottery scams, work from home scams, investment scams, online auctions, phishing, and vishing scams. These various types of scams are noted below in further detail to raise awareness of the different techniques utilised. This list is by no means exhausted due to the evolving nature of the internet there will no doubt be a continuous flow of new scams coming to the forefront. However, it's vital that the CSP keep abreast of these changes as well as the most prevalent types[38].



Such crimes can utilise legitimate companies such as Western Union, Ebay, Moneygram, Gumtree etc; which is likely to add to the authenticity of the potential scam. Often these will

[35] http://www.education.gov.uk/ukccis/groups/a0075857/the-previous-project-groups– accessed 05/01/2012
[36] Spectrum, The UK's Fraud Prevention Service Newsletter, December, 2011
[37] http://www.ecrimewales.com/server.php?show=nav.8856 – accessed on 19/01/2012
[38] Fraud Facts, Cybercrime – email and internet scams, 2009

vary in method however usually involve using stolen bank/credit cards details to purchase goods, or accessing account details such as to extract monies or personal details. There are of course 'traditional' crimes that can occur, such as theft, but can make use of the internet as a means to advertise and sell goods. Typically, items will be stolen and Police or victims themselves will later find said items for sale on various websites. There has also been suggestions made that scams are now infiltrating Britain's online dating scene; with overseas fraudsters exploiting people's loneliness into tricking them to hand over their life savings. Internet dating is a lucrative business and it's estimated there are around 1,400 dating sites within Britain alone, therefore, widening the potential scope of such scams[39]. Another concern raised by Community Safety workers regarding dating websites concerns the posting of pictures of children on people's profiles. Initially, this appears harmless however parents/guardians should be made aware of the potential risks of persons specifically engaging with them so as to make contact with children.

When examining crimes locally the same trends are apparent for instance buying goods off online sites and the goods failing to arrive after monies have been paid, advertising fake flats for rent which then encourage the victim to pay a deposit and first month's rent, sending unsolicited emails purporting to be from a legitimate company requesting recipient give access to their bank facilities for the purposes of transferring money.

5.2 'See Off Scams'

Community Safety Workers, the Home Safety Officer, Tayside Police, and Victim Support have previously delivered a seminar at the Caird Hall in which concerns were addressed about 'scams' This of course covered a variety of topics from bogus callers to email scams. 'See Off Scam' packs were developed and includes advice, window stickers, and a safety magnet. Such engagement with the public is vital in order to portray the message that scams are varied and with the advances in technology there will continue to be risks when connecting to the internet that we are must be aware of. With this is mind it is crucial that there is a continued focus by the CSP to educate adults about potential dangers and provide advice on how to set up suitable safe guards to combat such types of e-crime.

5.3 Current Reporting Methods of Crimes and Incidents

Incidents of e-crime are recorded on Tayside Police crime recording system UNIFI. However, this is dependent on the Reporting Officer detailing the adequate aggravator 'High Tech/E-Crime', therefore, e-crime incidents are not always easily identifiable. CAPTOR is Tayside Police's incident recording system and as such all incidents recorded on CAPTOR will not subsequently result in a crime report. Therefore, monitoring of all incidents on CAPTOR and UNIFI would be beneficial to flag any potential new threats or emerging trends. Furthermore, there are currently various methods for reporting incidents within council departments which may result in incidents being dealt with independently without the knowledge of the Internet Safety Group. With this in mind there may be a need to develop a central reporting system.

[39] Jonathan Leake, Police target lonely hearts fraudster, The Sunday Times News, 27 November 2011

6.0 SOCIAL NETWORKING

There is a diverse range of social networking platforms that allow people to communicate, share messages, pictures, videos, as well as playing games; which bring benefits as well as dangers. Popular sites include Facebook, Twitter, MySpace, and Bebo, Friends Reunited, and LinkedIn[40]. Social networking is prevalent amongst children and adults although typically there tends to be different reasons for the use of this type of medium. Adult users may use social networking as a means to contact family/friends living abroad, or old school friends through sites such as Friends Reunited, vocational social networking through sites such as LinkedIn. Children and young people however tend to use this as a meeting place and to play games etc.

Details contained within the blue boxes are examples of crimes that have occurred within the city. Similar trends are apparent to those raised nationally regarding social networking and the occurrence of grooming, antisocial behaviour and frauds etc via this type of medium. When specifically considering grooming incidents generally, there is an MO of contacting children/ young people speculatively and asking them to perform sexual acts in front of a webcam. The motivation for this is unknown and it is also unknown if the where the victim complies with the request if the images are recorded. If they are recorded are they for personal use or is there an intention to blackmail the victim, or to use as collateral in paedophilic groups.

6.1 Real-Time Updates and Location Based Services

One concept which has gained momentum within social networking is real-time updates and location based services. Through real-time updates users are able to contribute to content to allow people to see where they are, what they are doing, and what is on their minds etc. Twitter and Facebook were both instrumental in driving forward the concept of real-time services. Twitter gives users 140 character limit to broadcast what they are doing and where they are, and allows users to connect to the latest information on what they find interesting and follow conversations[41]. Facebook offers real-time updates by allowing users to 'check-in' to locations and comment; which then allows people to view where you have been, where you are now, and where you are going. It has been estimated that there are over 800 million active users of Facebook world wider, and on average each user has 130 friends[42].

6.2 Popularity of Social Networking

Social networking is prevalent amongst adults whether that be via a mobile connection or a fixed connection. The use of social networking via smartphones has already been discussed, however, when examining the social networking landscape via a PC six in ten broadband users use social networking sites with 54% of internet users stating they had a social network profile in 2010. Facebook by far is the most dominant of the social networking sites where it has been noted that more than 90% of social networking is done via this medium[43]. Recent figures released suggests that Dundee is home to 75, 000 Facebook users, and 20, 000 on LinkedIn[44]

According to Ofcom's Children and Parents Media Use and Attitudes Report 2011, 75% of 12-15 year olds have an active social networking profile, whilst 34% of those ages 8-12 have a profile on sites that requires users to be aged 13 or over. Facebook, Bebo, MySpace all require users to be aged 13 or over. However, younger children simply get around this by

[40] Fraud Facts, Cybercrime – Social Networks and Virtual Worlds, 2009
[41] http://twitter.com/about - accessed on 25/01/2012
[42] http://www.facebook.com/about/location - accessed on 25/01/2012
[43] Ofcom, Communications market Report: UK, 2011
[44] Beware a legal minefield, The Courier, 15 February 2012

providing a false age in order to gain access. The same report further noted that most 8-15 year olds claimed their profile could only been seen by their friends and only a small minority of 8-11 (17%) and 12-15 (28%) year olds had a profile which was open to anyone or open to friends of friends. These statistics on face value appear reassuring that children and young people are taken the necessary steps to protect themselves, however, the main issue highlighted throughout has been that children and young people will often add 'friends' who are people unknown to them, furthermore, these 'friends' can purport a different identity. This has been a consistent concern raised by members of the Internet Safety Group, especially amongst secondary school aged children where there appears to be competition to gain as many online friends as possible. There are sites which promote this type of networking such as Needaddys, which allows people to search for people to add as friends on social networking sites. People can choose what sort of people the want to add which means people can specifically search for certain ages, sex, location. This has obviously implications with regards to grooming as persons can search for certain characteristics and instigate an online friendship with children and young people with the end objective being a face to face meeting after establishing an emotional connection with the child.

Facebook: motorbike stolen and then received messages on Facebook as to who was responsible

6.3 Social Networking Risks

As with the other aspects of e-safety there are similar concerns with social networking such as cyber stalking, and frauds, bullying etc. Bullying amongst children via social networking can be problematic and according to Ofcom, Children and Parents: Media Use and Attitudes Report, is cited as one of the specific dislikes about social networking by children themselves, as well as the possibility of strangers finding out information about them. However, this problem is not confined to children as adults can become embroiled in posting comments regarding fellow employees or bosses which can lead to disciplinary issues. Employers themselves can use social networking sites to pre-screen potential employees with many people unaware that they have a 'digital footprint'[45]. Cyber criminals utilise social networking sites with various methods such as the sharing of links and files which spread spyware and viruses. These then capture the login details for accounts which can then be sold for profit. Fraudsters can impersonate you on a social network website in order to ask your friends for money to help out difficult situations. Fraudsters can also collect your personal data from details that are available online and use this information, usually along with other information obtained elsewhere, to purchase goods and services[46]. All too often people provide too much information via social networking sites through 'check-in' and status updates or details held within the profile themselves such as full names, addresses, dates of birth, telephone numbers, and places of work.

Facebook: sexual harassment of complainer where suspect pestered her friends for her mobile number, asked her out for drinks via Facebook. Ultimately resulted in sexual assault. The relevant part being that she was targeted via multiple methods

When considering these issues locally concerns have been raised by various members of the Internet Safety Group regarding children's use and attitudes towards social media; which generally mirror those concerns raised nationally. Library staff noted that children can be very free with personal details such as sharing mobile telephone numbers with anyone, adding vague acquaintances, friends of friends who may be of much greater age or even complete strangers. Staff members have witnessed instances of children hacking into another's Facebook page (known as 'Fraping') and posting rude or hurtful comments. Furthermore, they have noted cases whereby younger children have alleged that they have access to social networking sites at home therefore should be allowed access in the library also. This could simply be a deliberate ploy to gain access or if true would suggest that parents' themselves are unaware of age restrictions on many social networking sites. However, there have been requests from parents to block their children's access to the internet in libraries because

Facebook: attempting to arrange a riot within the city during disorder within England. Two suspects were later identified and given 3 years' detention for their inflammatory posts

[45] Safer Children in a Digital World, The Report of the Byron Review, 2008
[46] Fraud Facts, Cybercrime – Social Networks and Virtual Worlds, 2009

they have concerns as to their activities. Libraries can implement a straightforward ban for younger children to support parents but not for adolescents.

Social Work Department have raised similar concerns which include rude/hurtful comments being posted about a person's sexuality, sexual behaviour or physical characteristics. Hacking into someone's Facebook page and posting rude comments which would appear to be a common issue for school aged children. Arranging to abscond, general antisocial behaviour, threats of physical violence posted via social networking sites are all particularly problematic especially for vulnerable children. Cyberbullying is another significant concern mainly due to the damage it can cause the victim, and the SWD have noted instances of photographic images being altered and uploaded by others onto social networking sites and used to bully an individual. The issue of posting too much information on such sites is an issue for SWD particularly for a child who is a vulnerable child or accommodated where the address is not to be disclosed to safeguard the safety of the child. There have instances of the children themselves making comments about their social workers on their profiles which have included physical threats.

Facebook: person responsible for an assault identified by complainer on Facebook

Given that it's common for adults to have their children as friends on social networking sites, further concerns raised have been the increasing number of adults who have become involved in children and young people's conversation which can lead to an escalation of issues and further problems for teachers and social workers. Conversely, there has also been general concerns raised regarding young people asking teachers, sports coaches etc to be 'friends' on social networking sites. This issue is likely to remain as people's work and personal lives become intertwined which in part has been driven by the introduction of smartphones and how this has impacted on people's everyday lives and the ability to always be connected to the internet.

Skype: 12 year old male receives a Skype call from a female he didn't know. She asked him to show his genitals, which he did, and then his buttocks, which he refused. She then stated she had been recording the images and would publish them on his friends' Facebook pages at which point he switched off his computer and disconnected his Skype account. Unknown how she identified him and got his Skype contact details, but potentially he has them listed on Facebook or other sites

7.0 RECOMMENDATIONS

Below are a set of recommendations that aim to help the CSP move forward the issue of e-safety. This will also help towards providing a baseline in the action plan and as such the CSP will be better placed to measure progress in the forthcoming years. Short and medium term recommendations have been proposed which will allow pertinent issues to be addressed efficiently, as well as helping support the implementation of the wider community safety strategy in subsequent years.

Short Term

- Identify and confirm an E-Safety Lead Officer for Dundee City Council and ensure the broadest representation on the E- Safety Group.

- Liaise with Personnel colleagues to develop guidance and support for staff when faced with E-Safety issues.

Medium Term

- Develop mechanisms for ensuring links to other policy areas concerned with the care and protection of vulnerable groups, identifying good practice and promoting sharing and learning locally, nationally and internationally.

- Further develop the existing education/awareness raising programmes for children, young people, parents, guardians and the wider community, extending these to include elected members and senior staff in partner organisations.

- Identify appropriate recording mechanisms, building upon current systems where possible and implement these where feasible with minimum impact on resources.

- Create a pool of highly skilled and knowledgeable staff from appropriate disciplines to further develop and deliver quality programmes, encouraging parental involvement where possible and prioritising prevention and early intervention.

.

- Develop close links with creative and innovative projects and teams to create high quality learning materials and explore the use of social media as a vehicle for promoting the e-safety message.

- Address issues of on-line radicalisation; sexual exploitation; fraud and cyber bullying.

8.0 USEFUL WEBSITES AND RESOURCES

Listed below are useful websites which contain links to resources that can provide internet safety for children and adults.

Organisation	Web Address
Bullying UK	http://www.bullying.co.uk
Child Exploitation and Online Protection Centre	http://www.ceop.police.uk
Childnet International	http://childnet-int.org
Cyber Mentors	http://www.cybermentors.org.uk
Directgov: Internet Safety	http://www.direct.gov.uk
E Crime Scotland	http://www.ecrimescotland.org.uk
Education Scotland	http://www.ltscotland.org.uk
Get Safe Online	http://www.getsafeonline.org
Scottish Government Internet Safety	http://www.scotland.gov.uk
ThinkUKnow	http://www.thinkuknow.co.uk
UK Council for Child Internet Safety (UKCCIS)	http://www.education.gov.uk/ukccis
Vodafone Parents' Guide	http://parents.vodafone.com

APPENDIX 2

DUNDEE E-SAFETY ACTION PLAN 2012 - 2015

Links to the Dundee Single Outcome Agreement: S.O.A. 3: Our children will be safe, healthy, achieving, nurtured, active, respected, responsible and included S.O.A. 7: Our communities will be safe and feel safe
Recommendation 1: Identify and confirm an E-Safety Lead Officer for Dundee City Council and ensure the broadest representation on the E- Safety Group

Ref No	What We Will Do	What We Will Achieve	By When	Lead
1.1	Identify and confirm an E-Safety Lead Officer for Dundee City Council	Dundee City Council will have the ability to co-ordinate e-safety activity within the Council and have a Single Point of Contact (SPOC) for agencies dealing with e-safety in Dundee and beyond	June 2012	Chief Officers Group
1.2	Review existing e-safety group membership to ensure broadest representation of relevant agencies at appropriate level including Head Teacher representation at Early Years, Primary and Secondary level and establish sub groups as required	Dundee will have a multi-agency e-safety group with the ability to maximise resources and prioritise activity to protect those most vulnerable to the e-safety threat	September 2012	E-Safety Lead Officer
1.3	Establish an appropriate monitoring and evaluation framework	Meaningful reports highlighting trends, progress and future actions required will be generated and published	March 2013 and annually throughout the life of the plan	E-Safety Lead Officer

DUNDEE E-SAFETY ACTION PLAN 2012 - 2015

Links to the Dundee Single Outcome Agreement: S.O.A. 3: Our children will be safe, healthy, achieving, nurtured, active, respected, responsible and included S.O.A. 7: Our communities will be safe and feel safe
Recommendation 2: Liaise with Personnel colleagues to develop guidance and support for staff when faced with E-Safety issues

Ref No	What We Will Do	What We Will Achieve	By When	Lead
2.1	Liaise with Personnel colleagues to review existing guidance in light of recent incidents and trends	Identification of any additional support needs required for staff	March 2013	E-Safety Lead Officer
2.2	Consult with stakeholders on potential e-safety issues and how these might be addressed	Identification of potential legal and other implications for staff and the Council	March 2013	E-Safety Lead Officer
2.3	Redraft existing e-safety guidance as necessary with Personnel colleagues	Dundee City Council E-Safety guidance will be fit for purpose. Staff will be supported	June 2013	E-Safety Lead Officer

DUNDEE E-SAFETY ACTION PLAN 2012 - 2015

Links to the Dundee Single Outcome Agreement:

S.O.A. 3: Our children will be safe, healthy, achieving, nurtured, active, respected, responsible and included

S.O.A. 7: Our communities will be safe and feel safe

Recommendation 3: Develop mechanisms for ensuring links to other policy areas concerned with the care and protection of vulnerable groups, identifying good practice and promoting sharing and learning locally, nationally and internationally

Ref No	What We Will Do	What We Will Achieve	By When	Lead
3.1	Liaise with Community Planning Manager to determine appropriate policy areas and identify a Single Point of Contact for each	A quality information sharing network between relevant policy areas in relation to e-safety	March 2013 and ongoing throughout life of the plan	E-Safety Lead Officer
3.2	Include SPOCs in E-Safety meetings, sharing of minutes and other information as appropriate	Consistency of message and response to issues. Increased efficiency and lack of duplication	March 2013 and ongoing throughout life of the plan	E-Safety Lead Officer
3.3	Develop criteria to establish what constitutes good practice and research best practice nationally and internationally	Dundee will consistently be demonstrating best practice	June 2013 and ongoing throughout life of the plan	E-Safety Lead Officer
3.4	Establish an on-line sharing space for staff initially, on e-safety related issues	Staff will have increased awareness of e-safety issues and how to respond to these	June 2013 and ongoing throughout life of plan	E-Safety Lead Officer
3.5	Explore feasibility and establish the best way of sharing information with the public	Members of the public will be aware at an early stage of potential SCAMS and other threats	June 2013 and ongoing throughout life of the plan	E-Safety Lead Officer

DUNDEE E-SAFETY ACTION PLAN 2012 - 2015

Links to the Dundee Single Outcome Agreement:

S.O.A. 3: Our children will be safe, healthy, achieving, nurtured, active, respected, responsible and included

S.O.A. 7: Our communities will be safe and feel safe

Recommendation 4: Further develop the existing education/awareness raising programmes for children, young people, parents, guardians and the wider community, extending these to include elected members and senior staff in partner organisations

Ref No	What We Will Do	What We Will Achieve	By When	Lead
4.1	Review existing programmes to update messages and achieve consistency of delivery and age appropriate content	Consistency of messages and delivery	March 2013 and ongoing throughout the life of the plan	E-safety Lead Officer
4.2	Identify specific groups to be targeted including senior managers and elected members	Better informed decision makers	December 2013	E-Safety Lead Officer
4.3	Develop a delivery programme including the most vulnerable and consider those with additional needs	Greater awareness of e-safety issues and how to respond to these	December 2013	E-Safety Lead Officer
4.4	Develop opportunities for parental involvement in the design and delivery of effective awareness raising programmes	Greater parental awareness of the issues and support for children and families outwith the school environment	June 2012 and ongoing throughout the life of the plan	

DUNDEE E-SAFETY ACTION PLAN 2012 - 2015

Links to the Dundee Single Outcome Agreement:

S.O.A. 3: Our children will be safe, healthy, achieving, nurtured, active, respected, responsible and included

S.O.A. 7: Our communities will be safe and feel safe

Recommendation 5: Identify appropriate recording mechanisms, building upon current systems where possible and implement these where feasible with minimum impact on resources

Ref No	What We Will Do	What We Will Achieve	By When	Lead
5.1	Liaise with admin staff, information officers and the I.T Department to map current recording systems in use by Council departments and partners and identify potential opportunities to include e-safety data collection to these	An overview of currently used recording systems and any potential to include e-safety data in these	March 2014	E-Safety Lead Officer
5.2	Identify key e-safety data to be collected and how this can be achieved with minimal additional recording	Clear data specifications for all agencies	September 2014	E-Safety Lead Officer
5.3	Implement e-safety recording systems where feasible	Robust baseline data and trend analysis which will help identify future priorities	March 2015	E-Safety Lead Officer

DUNDEE E-SAFETY ACTION PLAN 2012 - 2015

Links to the Dundee Single Outcome Agreement: S.O.A. 3: Our children will be safe, healthy, achieving, nurtured, active, respected, responsible and included S.O.A. 7: Our communities will be safe and feel safe
Recommendation 6: Support staff from appropriate disciplines to acquire the skills and knowledge required to further develop and deliver quality programmes, encouraging parental involvement where possible and prioritising prevention and early intervention

Ref No	What We Will Do	What We Will Achieve	By When	Lead
6.1	Identify individuals, groups, departments and agencies with the relevant skills to develop and deliver E-Safety programmes.	A pool of highly trained, motivated and effective trainers who can support the development of e-safety awareness raising. Effective and efficient use of resources	December 2012	E-Safety Lead Officer
6.2	Develop bespoke programmes for staff with links to national and international issues as appropriate	A focussed and targeted programme of awareness raising delivering quality and consistent messages	March 2013	E-Safety Lead Officer
6.3	Ensure staff are trained to deal with initial disclosures	Effective support and follow-up for those most affected by e-safety issues	June 13 and ongoing throughout the life of the plan	E-Safety Lead Officer

DUNDEE E-SAFETY ACTION PLAN 2012 - 2015

Links to the Dundee Single Outcome Agreement: S.O.A. 3: Our children will be safe, healthy, achieving, nurtured, active, respected, responsible and included S.O.A. 7: Our communities will be safe and feel safe
Recommendation 7: Develop close links with creative and innovative projects and teams to create high quality learning materials and explore the use of social media as a vehicle for promoting the e-safety message

Ref No	What We Will Do	What We Will Achieve	By When	Lead
7.1	Identify appropriate projects and map available provision both locally and nationally	We will be aware of new projects and build upon the work of existing projects	March 2015	E-Safety Lead Officer
7.2	Encourage young people particularly, but not exclusively to become involved in the design and development of exciting and innovative materials to raise awareness of e-safety issues	Young people will be actively engaged in e-safety projects Dundee will have a range of exciting and innovative resources to support e-safety awareness raising demonstrating best practice	March 2014 and ongoing throughout the life of the plan	E-Safety Lead Officer
7.3	Identify appropriate forms of social media that may be used to promote the e-safety message and ensure a risk assessment of each is undertaken to allow informed decision making on potential use	The e-safety message will be more easily shared and understood Access to the e-safety message will be more widely available	March 2015	E-Safety Lead Officer

DUNDEE E-SAFETY ACTION PLAN 2012 - 2015

Links to the Dundee Single Outcome Agreement: S.O.A. 3: Our children will be safe, healthy, achieving, nurtured, active, respected, responsible and included S.O.A. 7: Our communities will be safe and feel safe
Recommendation 8: Address issues of on-line radicalisation; sexual exploitation; fraud and cyber bullying

Ref No	What We Will Do	What We Will Achieve	By When	Lead
8.1	Scope the extent of these issues in Dundee in relation to national/international context	An understanding of the scale of the issues as they relate to Dundee	September 2013	E-Safety Lead Officer
8.2	Identify good practice elsewhere and how that may or may not be transferable to Dundee	Awareness of options for tackling the issues in Dundee	June 2013 and ongoing throughout the life of the plan	E-Safety Lead Officer
8.3	Liaise with Dundee Violence Against Women Project and Care and Protection Services over Sexual Exploitation	Co-ordinated and strategic response to issues with no duplication of effort	June 2012 and ongoing throughout the life of the plan	E-Safety Lead Officer
8.4	Implement education and awareness raising programmes.	Greater awareness and consistency of message	June 2013 and ongoing throughout the life of the plan	E-Safety Lead Officer
8.5	Work with Peer Educators to explore the development of a Cyber Peer Mentoring Project for young people	Young people will be actively engaged in seeking and developing appropriate responses to issues	June 2014	E-Safety Lead Officer