SERVICE CHILDREN'S EDUCATION

POLICY

E-Safety

Issued November 2011

New technologies have become integral to the lives of children and young people in today's society, both within schools and in their lives outside school.

The e-Safety Policy explains how the Agency intends to do this, whilst also addressing wider educational issues in order to help young people (and their parents / carers) to be responsible users and stay safe while using the Internet and other communications technologies for educational, personal and recreational use.

An Agency of the Ministry of Defence

Title	SCE E-Safety Policy (Acceptable Use Policy)
Reference number	SCE/1/2/10/2
Supersedes	None
Date of issue	November 2011
Review date	December 2013
Review by & lead member of staff	ICT Adviser, ICT & Facilities Manager, AEO(PD)
Prepared by	ICT Adviser Pupil and Family Services Primary ICT Consultants Secondary ICT Consultant
Consultation	AEO (PD), ICT & Facilities Manager, ICT Systems Manager Representatives from ISDT Team and Pupil and Family Services
Supply / distribution	Available as a read-only document on the intranet plus one hard copy to each school & setting
Other relevant approved documents	JSP 740 Acceptable Use policy JSP 440 The Defence Manual of Security SCE Information Security Incident Management Policy JSP 747 IM Protocols & Policy, email, IM, Personal Electronic Writing, Digital Identities JSP 708 MOD Policy on Chat Rooms SCE Information Management Strategy
Approved by	Agency Executive Board (November 2011)
Authorized by	DCE

E – Safety Policy

1 Background & Purpose

1.1 New technologies have become integral to the lives of children and young people in today's society, both within schools and in their lives outside school.

1.2 The Internet and other digital and information technologies are powerful tools, which open up new opportunities for everyone. Electronic communication helps teachers and students / pupils learn from each other. These technologies can stimulate discussion, promote creativity and increase awareness of context to promote effective learning. Children and young people should have an entitlement to safe Internet access at all times.

1.3 The requirement to ensure that children and young people are able to use the Internet and related communications technologies appropriately and safely is addressed as part of the wider duty of care to which all who work in schools are bound. A school e-Safety policy should help to ensure safe and appropriate use. The development and implementation of such a strategy should involve all the stakeholders in a child's education from the head teacher and SGC to the senior leaders and classroom teachers, support staff, parents, members of the community and the students / pupils themselves.

1.4 The use of these exciting and innovative tools in school and at home has been shown to raise educational standards and promote pupil / student achievement.

However, the use of these new technologies can put young people at risk within and outside the school. Some of the dangers they may face include:

- Access to illegal, harmful or inappropriate images or other content
- Unauthorised access to / loss of / sharing of personal information
- The risk of being subject to grooming by those with whom they make contact on the Internet.
- The sharing / distribution of personal images without an individual's consent or knowledge
- Inappropriate communication / contact with others, including strangers
- Cyber-bullying
- Access to unsuitable video / Internet games
- An inability to evaluate the quality, accuracy and relevance of information on the Internet
- Plagiarism and copyright infringement
- Illegal downloading of music or video files
- The potential for excessive use which may impact on the social and emotional development and learning of the young person.

1.5 Many of these risks reflect situations in the off-line world and it is essential that this e-Safety policy is used in conjunction with other school policies (e.g. behaviour, anti-bullying and child protection policies).

1.6 As with all other risks, it is impossible to eliminate those risks completely. It is therefore essential, through good educational provision to build students' / pupils' resilience to

the risks to which they may be exposed, so that they have the confidence and skills to face and deal with these risks.

1.7 The school must demonstrate that it has provided the necessary safeguards to help ensure that they have done everything that could reasonably be expected of them to manage and reduce these risks. The e-Safety policy that follows explains how we intend to do this, while also addressing wider educational issues in order to help young people (and their parents / carers) to be responsible users and stay safe while using the Internet and other communications technologies for educational, personal and recreational use.

2. Scope

2.1 This policy applies to all members of the school community (including staff, students / pupils, volunteers, parents / carers, visitors, community users) who have access to and are users of school ICT systems, both in and out of school.

2.2 The Education and Inspections Act 2006 empowers headteachers, to such extent as is reasonable, to regulate the behaviour of students / pupils when they are off the school site and empowers members of staff to impose disciplinary penalties for inappropriate behaviour. This is pertinent to incidents of cyber-bullying or other e-Safety incidents covered by this policy, which may take place out of school, but is linked to membership of the school.

2.3 The school will deal with such incidents within this policy and associated behaviour and anti-bullying policies and will, where known, inform parents / carers of incidents of inappropriate e-Safety behaviour that take place out of school.

3. Roles and Responsibilities

3.1 The following section outlines the roles and responsibilities for e-Safety:

3.2 Head teacher and Senior Leaders:

- The Head teacher is responsible for ensuring the safety (including e-Safety) of members of the school community, though the day to day responsibility for e-Safety will be delegated to the E-Safety Co-ordinator / Officer
- The Head teacher / Senior Leaders are responsible for ensuring that the E-Safety Coordinator / Officer and other relevant staff receive suitable CPD to enable them to carry out their e-Safety roles and to train other colleagues, as relevant
- The Head teacher / Senior Leaders will ensure that there is a system in place to allow for monitoring and support of those in school who carry out the internal e-Safety monitoring role. This is to provide a safety net and also support to those colleagues who take on important monitoring roles
- The Senior Leadership Team / Senior Management Team will receive regular monitoring reports from the E-Safety Co-ordinator / Officer
- The Head teacher and another member of the Senior Leadership Team / Senior Management Team should be aware of the procedures to be followed in the event of a serious e-Safety allegation being made against a member of staff.

3.3 E-Safety Coordinator / Officer

- leads on e-Safety
- takes day to day responsibility for e-Safety issues and has a leading role in establishing and reviewing the school e-Safety policies / documents
- ensures that all staff are aware of the procedures that need to be followed in the event of an e-Safety incident taking place
- provides training and advice for staff
- liaises with SCE
- liaises with school ICT technical staff
- receives reports of e-Safety incidents and creates a log of incidents to inform future e-Safety developments
- meets regularly with E-Safety SGC member to discuss current issues, review incident logs and filtering / change control logs
- reports regularly to Senior Leadership Team

3.4 SCE Technical support staff / School Network Manager

These staff are responsible for ensuring:

- that the school's ICT infrastructure is secure and is not open to misuse or malicious attack
- that users may only access the school's networks through a properly enforced password protection policy
- the school's filtering policy is applied and updated on a regular basis
- that he / she keeps up to date with e-Safety technical information in order to effectively carry out their e-Safety role and to inform and update others as relevant
- that monitoring software / systems are implemented and updated as agreed in school policies

3.5 Teaching and Support Staff

- are responsible for ensuring that:
- they have an up to date awareness of e-Safety matters and of the current school e-Safety policy and practices
- they have read and understood JSP 740 and signed the school Staff Acceptable Use Policy (AUP)
- they report any suspected misuse or problem to the appropriate person for investigation
- digital communications with students / pupils (e-mail / Virtual Learning Environment (VLE) / voice / VTC / MOVI) should be on a professional level and only carried out using official school communication systems
- e-Safety issues are embedded in all aspects of the curriculum and other school activities
- students / pupils understand and follow the school e-Safety and acceptable use policy

- students / pupils have an understanding of research skills and the need to avoid plagiarism and uphold copyright regulations
- they monitor ICT activity in lessons, extra curricular and extended school activities
- they are aware of e-Safety issues related to the use of mobile phones, cameras and hand held devices and that they monitor their use and implement current school policies with regard to these devices
- in lessons where Internet use is pre-planned students / pupils should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in Internet searches

3.6 Designated senior person for child protection

Staff should be trained in e-Safety issues and be aware of the potential for serious child protection issues to arise from:

- sharing of personal data
- access to illegal / inappropriate materials
- inappropriate on-line contact with adults / strangers
- potential or actual incidents of grooming
- cyber-bullying

3.7 Students / pupils

- are responsible for using the school ICT systems in accordance with the Student / Pupil Acceptable Use Policy, which they will be expected to sign before being given access to school systems
- have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations
- need to understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so
- will be expected to know and understand school policies on the use of mobile phones, digital cameras and hand held devices. They should also know and understand school policies on the taking / use of images and on cyber-bullying
- should understand the importance of adopting good e-Safety practice when using digital technologies out of school

3.8 Parents / Carers

Parents / carers play a crucial role in ensuring that their children understand the need to use the Internet / mobile devices in an appropriate way. The school will therefore take every opportunity to help parents understand these issues through parents' evenings, newsletters, website / VLE and information about national / local e-Safety campaigns / literature. Parents and carers will be responsible for:

- endorsing (by signature) the Student / Pupil Acceptable Use Policy
- accessing the school website / VLE / on-line student / pupil records in accordance with the relevant school Acceptable Use Policy.

4 Policy Statements

4.1 Education – students/pupils

- A planned e-Safety programme should be provided as part of ICT / PHSE / other lessons and should be regularly revisited – this will cover both the use of ICT and new technologies in and beyond school
- Key e-Safety messages should be reinforced as part of a planned programme of assemblies and tutorial / pastoral activities
- Students / pupils should be taught in all lessons to be critically aware of the materials / content they access on-line and be guided to validate the accuracy of information
- Students / pupils should be helped to understand the need for the student / pupil AUP and encouraged to adopt safe and responsible use of ICT, the Internet and mobile devices both within and outside school
- Students / pupils should be taught to acknowledge the source of information used and to respect copyright when using material accessed on the Internet
- Rules for use of ICT systems / Internet will be posted in all rooms
- Staff should act as good role models in their use of ICT, the Internet and mobile devices

4.2 Education & Training – Staff

It is essential that all staff receive e-Safety training and understand their responsibilities, as outlined in this policy. Training will be offered as follows:

- A planned programme of formal e-Safety training will be made available to staff. An audit of the e-Safety training needs of all staff will be carried out regularly. It is expected that some staff will identify e-Safety as a training need within the performance management process
- All new staff should receive e-Safety training as part of their induction programme, ensuring that they fully understand the school e-Safety policy and Acceptable Use Policies
- JSP 740, together with this e-Safety policy will be presented to and discussed by staff in staff / team meetings / INSET days

4.3 Training – SGC

- SGC should have an awareness of e-Safety and how this is applied and implemented in school
- SGC should be invited to take part in e-Safety training / awareness sessions

4.4 Technical – infrastructure / equipment, filtering and monitoring

SCE Technical Support Officer/school network manager will be responsible for ensuring that the school infrastructure / network is as safe and secure as is reasonably possible and that policies and procedures approved are implemented. It will also need to ensure that the relevant people named in the above sections will be effective in carrying out their e-Safety responsibilities.

- There will be regular reviews and audits of the safety and security of school ICT systems

- Servers, wireless systems and cabling must be securely located and physical access restricted
- All users will have clearly defined access rights to school ICT systems
- All users (at KS2 and above) will be provided with a username and password
- The “master / administrator” passwords for the school ICT system, used by the Network Manager (or other person) must also be available to the Headteacher or other nominated senior leader
- Users will be made responsible for the security of their username and password, must not allow other users to access the systems using their log on details and must immediately report any suspicion or evidence that there has been a breach of security
- The school has provided appropriate user-level filtering through the use of the (insert name) filtering programme
- In the event of the Network Manager (or other person) needing to switch off the filtering for any reason, or for any user, this must be logged and carried out by a process that is agreed by the Headteacher (or other nominated senior leader)
- Requests from staff for sites to be added or removed from the filtered list will be actioned by the Network Manager
- School ICT technical staff regularly monitor and record the activity of users on the school ICT systems and users are made aware of this in the Acceptable Use Policy. (schools may wish to add details of the monitoring programmes that are used)
- (possible statement) Remote management tools are used by staff to control workstations and view users activity
- Appropriate security measures are in place (schools may wish to provide more detail) to protect the servers, firewalls, routers, wireless systems, work stations, hand held devices etc from accidental or malicious attempts which might threaten the security of the school systems and data
- An agreed policy is in place (to be described) for the provision of temporary access of “guests” (eg trainee teachers, visitors) onto the school system
- An agreed policy is in place (to be described) that allows staff to / forbids staff from installing programmes on school workstations / portable devices
- An agreed policy is in place (to be described) regarding the use of removable media (eg memory sticks / CDs / DVDs) by users on school workstations / portable device
- The school infrastructure and individual workstations are protected by up to date virus software
- Personal data can not be sent over the Internet or taken off the school site unless safely encrypted or otherwise secured.

4.5 Use of images

- When using digital images, staff should inform and educate students / pupils about the risks associated with the taking, use, sharing, publication and distribution of images. In particular they should recognise the risks attached to publishing their own images on the Internet e.g. on social networking sites

- Staff are allowed to take and use images to support educational aims, but must follow school policies concerning the sharing, distribution and publication of those images. Those images should only be taken on school equipment, the personal equipment of staff should not be used for such purposes
- Care should be taken when taking images that students / pupils are not participating in activities that put them at risk or bring the individuals or the school into disrepute
- Students / pupils must not take, use, share, publish or distribute images of others without their permission
- Photographs published on the website, or elsewhere that include students / pupils will be selected carefully and will comply with good practice guidance on the use of such images
- Students' / Pupils' full names will not be used anywhere on a website or blog, particularly in association with photographs
- Written permission from parents or carers will be obtained before photographs of students / pupils are published on the school website (may be covered as part of the AUP signed by parents or carers at the start of the year
- Student's / Pupil's work can only be published with the permission of the student / pupil and parents or carers.

5 The Use of E-mail

5.1 Electronic mail (e-mail) is now an important means of communication for most members of SCE. Messages can be delivered almost anywhere in the world rapidly and it is simple to generate, reply to, or forward e-mail.

5.2 There are responsibilities involved in using e-mail. In signing the Agency Acceptable Use Policy all employees agree to fulfil these responsibilities and acknowledge the wider MoD Policy and UK Data Protection law.

5.3 All SCE staff are allocated a "sceschools.com" e-mail address when they join the Agency. This e-mail address should be used for all official SCE e-mails. The use of a private e-mail address to send and receive "Personal" and / or "Personal Sensitive" information as defined by the Data Protection Act is forbidden.

5.4 Staff allocated a Defence Information Infrastructure account (DII) must adhere to the appropriate SyOPS when using it.

5.5 General Considerations when using E-mail

- E-mail is not a confidential means of communication. Staff should bear in mind that e-mail messages can be very easily read by those for whom they were not intended and in particular recognise that e-mails can be:
    - intercepted by third parties (legally or otherwise)
    - wrongly addressed
    - forwarded accidentally
    - forwarded by initial recipients to third parties against your wishes
    - viewed accidentally on recipients' computer screens

- Sensitive personal data should not be communicated by e-mail unless the express permission of the subject has been obtained or unless adequate encryption facilities have been employed. Sensitive personal data can be sent across DII systems.
- Staff must not include any defamatory comments in any e-mail messages. E-mail is a form of publication and the laws relating to defamation apply. A comment made in jest can be misinterpreted by its recipient. In – for example - a case of harassment it is the effect of a communication which is considered and not the intention of the sender.
- Staff must never use a false identity in e-mails, and must be aware that there is no guarantee that e-mail received was in fact sent by the purported sender. If, for any reason, an e-mail is sent on behalf of someone else the sender must make that clear at the beginning of the message.
- The SCE e-mail system must not be used to create or distribute unsolicited, offensive, or unwanted e-mail, including the dissemination of chain letters. The sending of unsolicited marketing messages is now a criminal offence.
- E-mail messages that show SCE in an unprofessional light or that could expose SCE to legal liability must not be sent by any member of staff. E-mails sent by a member of SCE have the same standing as a letter on headed notepaper even if the contents are described as “private”. As such all communications are subject to the FOIA and DPA.
- Be very careful when downloading material from the internet and opening external e-mails if there is any suspicion of it including a virus. If you have any suspicions, do not open an attachment and contact your school ICT staff or peripatetic ICT Technical Support Officer immediately.
- Staff must not invade anyone’s privacy by any means using e-mail.
- E-mail is not a substitute for record-keeping purposes. Where long term accessibility is an issue staff must transfer e-mail records to a more lasting medium or other electronic environment.
- The laws applying to copyright apply to e-mail messages and attachments. Staff must familiarise themselves with SCE’s policies in relation to copyright and be careful when copying material for inclusion in e-mail.
- Documents attached to e-mails may contain information from which the history of a document’s creation may be deduced. This data may identify those involved in generating or altering that item.
- As a member of SCE you are covered by the Data Protection Act (1998). This prescribes a number of further rights and responsibilities in using e-mail
    - Personal data is subject to the Act. Under its terms, personal data includes any information about a living identifiable individual, including his/her name, address, phone number, and e-mail address. I f you include such information in an e-mail or an attachment to an e-mail, you are deemed to be "processing" personal data and must abide by the Act. Personal information includes any expression of opinion.
    - Putting personal information (and especially personal sensitive information) in an unencrypted e-mail bears significant risk and is not an acceptable practice. The use of a “safe-haven” fax machine or suitably “caveated” and double-enveloped letter must be considered for the sending of all such information

- Staff must not collect such information without the individual knowing what it is to be used for and how it might be transmitted to third parties. Information so collected must not be disclosed or amended except in accordance with the purpose for which the information was collected; information must be accurate and up to date.
- SCE has by law to provide any personal information held about any data subject who requests it under the Act. This includes information on individual PCs in departments and all staff have a responsibility to comply with any instruction to release such data made by SCE Data Protection Lead. E-mails which contain personal information and are held in live, archive or back-up systems or have been "deleted" from the live systems, but are still capable of recovery, may be accessible by data subjects.
- The law also imposes rules on the retention of personal data. Such data should be kept only for as long as it is needed for the purpose for which it was collected.
- Care must be taken when sending e-mails containing personal information to countries outside the European Economic Area, especially if those countries do not have equivalent levels of protection for personal data.

6. Social Networking

6.1 Acceptable use of social networking sites

6.2 The widespread availability and use of social networking applications bring opportunities to understand, engage and communicate with our audiences in new ways. It is important that we are able to use these technologies and services effectively and flexibly. However, it is also important to ensure that we balance this with our duties to our services users and partners, our legal responsibilities and our reputation.

6.3 For example, our use of social networking applications has implications for our duty to safeguard children, young people and vulnerable adults.

6.4 The requirements set out below aim to provide this balance to support innovation whilst providing a framework of good practice.

Social networking applications include, but are not limited to:

- Blogs
- Online discussion forums
- Collaborative spaces
- Media sharing services e.g. Youtube
- ‘Micro logging’ applications e.g. Twitter

6.5 Many of the principles of this policy also apply to other types of online presence such as virtual worlds and RSS aggregation services and the use of all such services must be discussed with the Communications Officer before use.

6.6 Use in Schools

6.7 The use of social networking sites within schools is only allowed in appropriately controlled situations and in support of legitimate curriculum activities – for example to teach the safe use of the internet.

- Staff and students must not access social networking sites for personal use via school information systems, school networks or using school equipment.
- If staff access social networking sites using their personal computer systems1 and equipment, they should never give out personal information of any kind which could identify themselves, colleagues and / or pupils as members of Service Children's Education or one of its schools.
- Staff must not place inappropriate photographs on any social network space and must – where they do post photographs - ensure that background detail (eg house number, street name, school) can not identify them. Photographs of colleagues and / or pupils - taken for example on school trips - must not be posted without the express permission of those in the photographs or their parents / carers.
- Staff are strongly advised not to communicate with students over social network sites using their personal systems and equipment. .
- Staff must not run social network spaces for student use on a personal basis. If social networking is used for supporting students with coursework (for example the Connected Learning Community), professional spaces must be created by staff for use by students.[2]

6.8 Schools are vulnerable to material posted about them online and all staff should be made aware of the need to report this should they become aware of anything bringing the school into disrepute. Schools are advised to check regularly, using a search engine, to see if any such material has been posted.

6.9 If staff use social networking sites they should not publish specific and detailed "personal views" relating to the Agency, its schools, staff or students.

6.10 The school network and IT facilities must not be used for the following activities:

- Conducting illegal activities
- Accessing or downloading pornographic material
- Gambling
- Soliciting for personal gain or profit
- Managing or providing a business or service
- Revealing or publicising proprietary or confidential information
- Representing personal opinions as those of the Agency or its schools
- Making or posting indecent or offensive remarks or proposals

[1] Staff may only use MoD issued equipment for Agency / school business. The use of personal equipment is forbidden.

[2] Online communications tools, such as weblogs ("blogs") and Wikis, have a potentially useful role in schools – such as on school websites, learning journals, celebrating good work, sharing information and facilitating collaboration. Where pupils and their families share such tools with staff in school it is important that this should always be through school-based provision, such as the SCE Connected Learning Community.

6.11. Terms of Use

6.12 All proposals for using social networking applications as part of SCE (whether they are hosted by the Agency or by a third party) must be approved by the Communications Officer first (info@sceschools.com)

6.13 All Staff must adhere to these Terms of Use. The Terms of Use below apply to all uses of social networking applications by all staff. This includes, but is not limited to, public-facing applications such as open discussion forums and internally-facing uses such as project blogs regardless of whether they are hosted on corporate networks or not.

6.14 SCE expects that users of social networking applications will always exercise the right of freedom of expression with due consideration for the rights of others and strictly in accordance with these Terms of Use.

6.11 Legislation

6.12 The following legislation - enforceable against public sector employees including school staff - must be considered when using the internet or email:

- Human Rights Act 1998
- Regulation of Investigatory Powers Act 2000 (RIPA)3
- Data Protection Act 1998
- Freedom of Information Act 2000
- Copyright, Designs and Patents Act 1988, amended by the Copyright and Related Rights Regulations 2003
- Computer Misuse Act 1990, amended by the Police and Justice Act 2006
- Obscene Publications Act 1959, Protection of Children Act 1988, Criminal Justice Act 1988

6.13 These Acts are concerned with material that might be

- criminal,
- cause harm to young people or
- be otherwise unlawful.

6.14 Enforcement

6.15 Any breach of the terms set out below could result in the application or offending content being removed in accordance with the published complaints procedure and the publishing rights of the responsible SCE employee being suspended.

6.16 The Agency reserves the right to require the closure of any applications or removal of content published by Agency representatives which may adversely affect the reputation of SCE or put it at risk of legal action.

---

[3] Covert monitoring is unlawful unless undertaken in accordance with RIPA and the Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000. There are two areas where monitoring is lawful. The Headteacher should make all reasonable efforts to ensure users know when communications may be intercepted and monitored.

6.17 Any communications or content you publish that causes damage to the Agency, any of its employees or any third party's reputation may amount to misconduct or gross misconduct to which the Agency's Dismissal and Disciplinary Policies apply.

7. Data Protection

7.1 The Data Protection Act (DPA) applies to all MOD establishments wherever located. Staff must thus ensure that they:

- Keep personal data in a secure environment, minimising the risk of its loss or misuse
- Use personal data only on MOD issued, secure, password-protected computers and other devices, ensuring that they are properly "logged-off" at the end of any working session
- Transfer data using encryption and secure password protected devices

7.2 When using communication technologies schools must consider the following as good practice:

- Users need to be aware that email communications are not secure and can be monitored
- Users must immediately report, to the nominated person, the receipt of any email that makes them feel uncomfortable, is offensive, threatening or bullying in nature and must not respond to any such email
- Any digital communication between staff and students / pupils or parents / carers (email, chat, VLE etc) may be the subject of both DPA and FOIA requests and must be professional in tone and content.

8. Misuse

8.1 Misuse of MOD / Agency and school electronic and telecommunications equipment is a serious disciplinary offence.

8.2 Each Headteacher can exercise a right to monitor the use of a school's information systems and internet access. This includes the right to intercept email and delete inappropriate materials where unauthorised use of the school's information system may be taking place, or the system may be being used for criminal purposes, or for storing unauthorised text, imagery or sound.

8.3 Staff must be aware that improper or unacceptable use of the internet, email and equipment could result in legal proceedings and the use of the school's Disciplinary Procedure.

8.4 Sanctions will depend upon the gravity of misuse and could result in dismissal.

8.5 All employees should bear in mind that information they share through social networking applications, even if they are on private spaces, are still subject to copyright, data protection and Freedom of Information legislation, the Safeguarding Vulnerable Groups Act 2006 and other legislation. They must also operate in line with the SCE Equality and Diversity Policy.

8.6. Misuse by staff

8.7 If a member of staff is believed to misuse the Internet or cLc in an abusive or illegal manner, a report must be made to the Headteacher immediately and then the

Allegations Against Staff Procedure and the Child Protection Policy must be followed to deal with any misconduct and all appropriate authorities contacted

8.8 Allegations are defined as information relating to either potential criminal conduct or conduct raising concerns about a person's suitability.

8.9 Misuse by pupils

8.10 Should a pupil be found to misuse the on-line facilities whilst at school, through the cLc or in a setting the following consequences will occur:

- Any child found to be willfully misusing the Internet by not following the Acceptable Use Rules will have a letter sent home to parents/carers explaining the reason for suspending the child or young person's use for a particular lesson or activity
- Further misuse of the rules will result in not being allowed to access the Internet for a period of time and another letter will be sent home to parents/carers
- A letter will be sent to parents/carers outlining the breach in Child Protection Policy where a child or young person is deemed to have misused technology against another child or adult.

8.11 In the event that a child or young person accidentally accesses inappropriate materials the child will report this to an adult immediately and take appropriate action to hide the screen or close the window, e.g. use 'Hector Protector', for example, (dependent on age) so that an adult can take the appropriate action. Where a child or young person feels unable to disclose abuse, sexual requests or other misuses against them to an adult, they can use the Report Abuse button (www.thinkuknow.co.uk) to make a report and seek further advice. This button is easily identifiable on the SCE cLc. The issue of a child or young person deliberately misusing on-line technologies should also be addressed by the establishment.

8.12 Children should be taught and encouraged to consider the implications for misusing the Internet and posting inappropriate materials to websites, for example, as this can lead to legal implications.