E-Safety Policy

2016-2018

Introduction

1.1. Cromwell J and I school sees the area of e-safety as a child protection issue and not one that is solely evident in ICT. All staff and pupils have a duty to be aware of their own and others' e-safety at all times.

2. Scope

2.1. This policy applies to Cromwell J and I school governing body, all teaching and other staff, whether employed by the City Council or employed directly by the school, external contractors providing services on behalf of the school, teacher trainees and other trainees, volunteers and other individuals who work for or provide services on behalf of the school. These individuals are collectively referred to as 'staff members' in this policy.

2.2. e-safety is not limited to school premises, school equipment or the school day, neither is it limited to equipment owned by the school. Any incident that happens during the school day will be reported in line with the flowchart for recording and reporting e-safety incidents.

2.3. Incidents from outside school that are disclosed or observed by staff will be dealt with in line with child protection procedures and the procedures outlined in this policy.

2.4 e-safety concerns the day to day running of the physical network and information passing through it whether connected via the internet, virtual private networks, intranets or local area networks.

2.5 Pupils are to be taught safe practices and that the e-safety policy will be monitored and enforced.

2.6 The school will respond to e-safety incidents involving members of the school (staff or pupils) as if they occurred during the school day, on the school site even if perpetrated using equipment not owned or operated by the school.

3. Legal Framework

3.1 Many young people, and indeed some staff, use the Internet regularly without being aware that some of the activities they take part in are potentially illegal.

3.2 The law is developing rapidly and changes occur frequently. Please note this section is designed to inform users of legal issues relevant to the use of communications, it is not professional advice.

3.3 Full details of the legal framework may be found in Appendix E

- Racial and Religious Hatred Act 2006
- Criminal Justice Act 2003
- Sexual Offences Act 2003
- Communications Act 2003 (section 127)
- Data Protection Act 1998
- The Computer Misuse Act 1990 (sections 1 — 3)
- Malicious Communications Act 1988 (section 1)

• Copyright, Design and Patents Act 1988
• Public Order Act 1986 (sections 17 — 29)
• Obscene Publications Act 1959 and 1964
• Protection from Harassment Act 1997
• Regulation of Investigatory Powers Act 2000
• Criminal Justice and Immigration Act 2008
• Education and Inspections Act 2006

4. Related Policies

4.1 This policy should be read in conjunction with the acceptable usage policy, child protection policy, anti-bullying policy, behaviour management policy, staff handbook and in line with the flowchart for recording and reporting e-safety incidents.

5. Statement of duty of care

5.1 The designated person for child protection will have overall responsibility for all e-safety matters and will be informed of all incidents in line with the flowchart for recording and reporting e-safety incidents. This is reported at safeguarding meetings and also shared at governing body meetings.

5.2 This said all staff have a responsibility to support e-safe practices in schools.

5.3 Pupils and staff at all levels need to understand their responsibilities and liabilities in the event of deliberate attempts to breach e-safety protocols or those laid out in the acceptable usage policy.

6. Teaching safe practices

6.1 All staff will be trained in good e-safety practices through the school's professional development activities including those given by internal and external trainers.

6.2 Pupils are taught e-safe practices throughout the school year, in line with the computing curriculum, and teachers ensure that they respond to the needs of their class as and when e-safety discussions arise.

6.3 Pupils new to the school or those who may not have completed the previous year's e-safety training will receive updates from their class teacher to bring them in line with other pupils.

7. Statement of provision of safe environment in schools (including monitoring of the policy)

7.1 The school currently provides access to the internet through BGFL as a filtered internet service provider. The school ensures that all hardware owned by the school network is provided with sufficient anti-virus and firewall protection.

7.2 The school uses sophisticated e-safety monitoring software (Policy Central) to notify the Network Manager of any incident of potentially unwanted use. These are followed up where necessary in line with this policy.

7.3 It is expected that all staff and pupils adhere to this policy at all times; it should be read in conjunction with the acceptable usage policy. The policy is monitored by both the ICT coordinator and the headteacher through the use of regular review with members of the school and in line with the flow chart for e-safety incidents.

8. Procedures to be followed in the event of a breach of e-Safety

8.1 All instances of e-safety, whether by direct observation or disclosure, will be taken seriously.

8.2 The process to follow should an observation or disclosure be made is laid out clearly in the flow chart for e-safety incidents. The flow chart should be followed and incident report completed at the earliest opportunity and in any case within 24 hours.

8.3 The incident flow chart for e-safety incidents includes the protection of evidence should there be a serious breach of e-safety.

8.4 Serious is defined as any breach that is intentional, whether by a member of the school or aimed towards a member of the school. Any device that has been involved in a serious breach should be taken, if safe to do so, and placed within the locked server room for investigation.

8.5 All breaches whether serious or not will be recorded in line with the flow chart for e-safety incidents. The folder of e-safety incident report forms is kept in the server room.

8.6 E-safety incidents that are deemed as serious could be incidents of sexual or violent imagery, bullying, racist or offensive text, physical attack, e-attack or sexual grooming. In these cases the e-safety policy should be read with other appropriate policies such as Child Protection, Acceptable Use and Disciplinary. This may involve other agencies including police and social services

9. The physical environment Wireless networks

9.1 The school uses wireless networking; all wireless networks will be encrypted.

9.2 During the installation of such networks all subcontractors installing Wireless Access Points would need to demonstrate that the required encryption is in place prior to them leaving the school site and the work being signed off as complete.

10. Passwords

10.1 The school operates with passwords on all networked devices.

10.2 The passwords for staff users is an alphanumeric password provided by the school, staff may change these.

10.3 All network users agree that they will not attempt to access the school network using any other username/password than their own.

11. Data transfer

11.1 Only sensitive data that is essential for staff to work on at home should be taken off site.

11.2 Class lists with tracking data may be taken off site, however pupil information taken from SIMS including home addresses, medical, educational and personal information should not be taken off site unless pre-arranged and agreed with the headteacher and only then should be removed in exceptional circumstances.

11.3 Any data that is removed from the school site should be removed on a school laptop with the normal level of e-safety security as outlined in this policy or on a hardware encrypted memory stick provided by the school. These are the only methods that sensitive data should be transferred.

11.4 Information regarding staff and pupils that needs to be shared between job-share staff and between teaching, support and administrative staff should be placed on the school network where usual data protection and e-safety measures are in effect.

11.5 Hardware encrypted USB memory sticks will be provided to staff should there be a requirement for them to do this and the encryption keys for such will be provided to staff to remember. These keys should not be written down.

11.6 All staff have a duty to ensure that non-school staff do not have access to school data being used at home as outlined in the Acceptable Use policy.

12. Staff bringing in files from home for Teaching and Learning.

12.1 Any member of staff that brings files from home for Teaching and Learning is responsible for ensuring that the file they propose to use in school is free from virus/spyware/malware and it is their responsibility to ensure that the material contained in the file is fit for purpose and does not contain any offensive or copyright material.

13. Incoming files on disk/USB memory

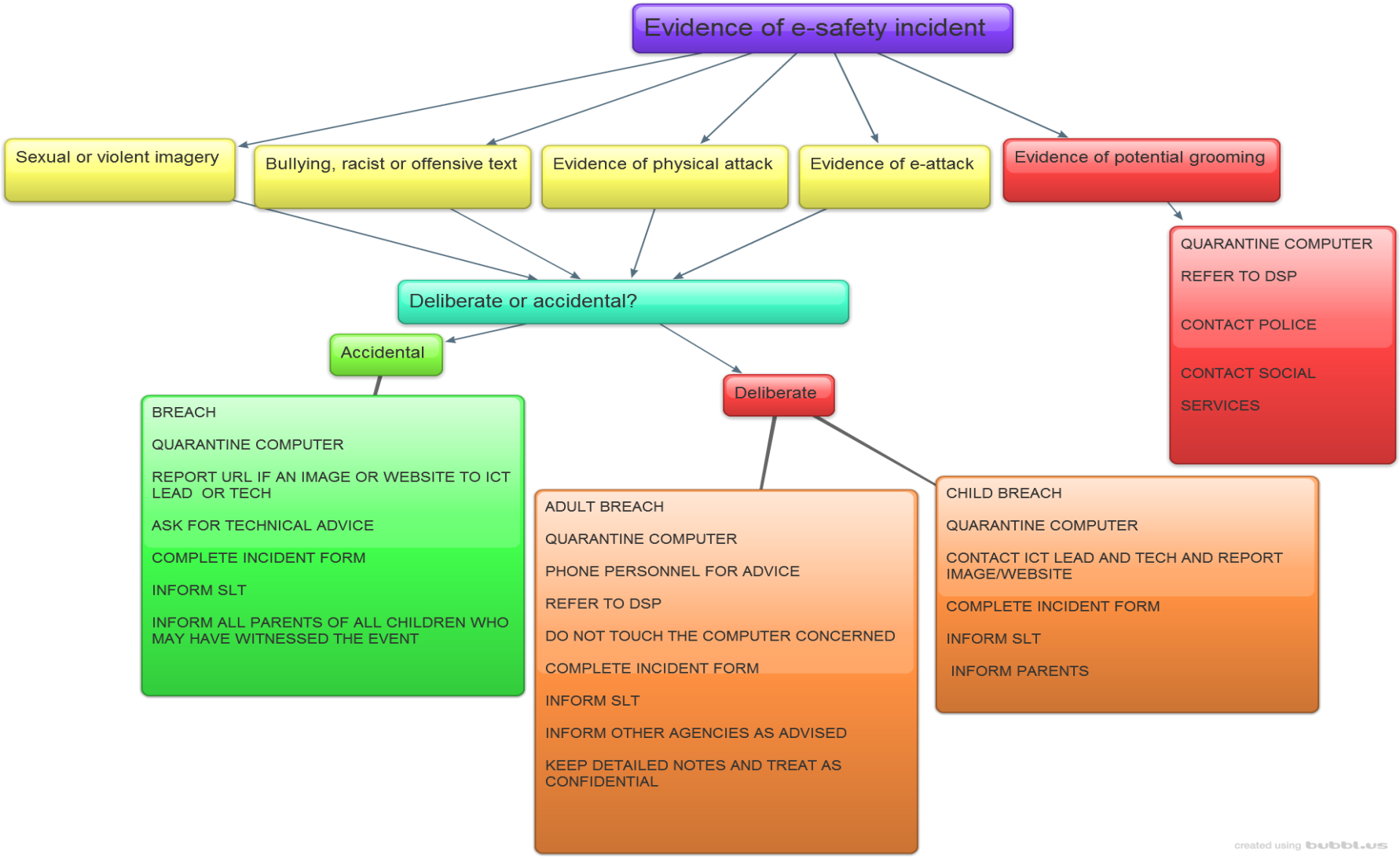
13.1 Pupils should not bring files into school on disks or USB memory sticks as these present significant risks to the school network.

14. Monitoring and reporting procedures

14.1 Records of all incidents involving e-safety will be compiled on the standard incident report forms which are kept in the e-safety incident report folder within the Headteachers office.

14.2 These records may be shared with legitimate agencies as necessary to ensure e-safety.

Appendix A E-Safety Incident Flowchart



APPENDIX B

E-Safety Incident form	Date:	Time:	
Staff member discovering incident:			
People involved in incident : (Child/Adult)			
Nature of incident: (Tick)	Accidental access to inappropriate material		
	Intentional access to inappropriate material		
	Cyber bullying		
	Grooming		
	Other (Specify)		
When did the event occur?	During a lesson		
	In Unsupervised Time		
	Outside School hours		
Does the event warrant direct police involvement? (Tick)	YES if Grooming, violent images, pornographic images, other criminal activity		
Briefly describe the incident			

SLT Section					
Staff incident	Personnel contacted on	Recommended action		Action applied	CO Govs
Child incident	Contacted Parents on	Actions Taken/ Interview with parents		Sanctions	
Filed copies	E-Safety incident file	Child protection officer	Child/Personnel file		

Appendix C

Further advice and guidance

Monitoring and reporting advice from Becta
http://schools.becta.org.uk/index.php?section=is&catcode=ss_to_es_pp_aup_03&rid=12002

E-safety charter
https://selfreview.becta.org.uk/

Becta Next generation Learning page
http://www.nextgenerationlearning.org.uk/

Becta e-safety quiz for parents
http://www.nextgenerationlearning.org.uk/en/Benefits/E-Safety-Quiz/
http://www.nextgenerationlearning.org.uk/en/Benefits/learn-safelyonline/

Next Generation Learning Charter
https://selfreview.becta.org.uk/about_next_generation_learning_charter

The Byron Report
http://www.dcsf.gov.uk/byronreview/pdfs/Final%20Report%20Bookmarked.pdf

The Byron Report Children's Summary
http://www.dcsf.gov.uk/byronreview/pdfs/A%20Summary%20for%20Children%20and%20Young%20People%20FINAL.pdf

The Byron Report Executive Summary
http://www.dcsf.gov.uk/byronreview/pdfs/Executive%20summary.pdf

Appendix D

e-safety for parents

While it is good practice to offer parents advice on e-safety, it is not practicable for school to offer technical advice on individual operating systems, hardware or software.
The advice offered to parents should cover the main concerns regarding e-safety and should direct them where to gain specific advice for their systems.
Should any parent ask a member of staff for advice they should be given the following information.
We should not offer advice on type of equipment or operating system other than in the most general of terms. Parents need to make their own informed choices, but will sometimes want advice from schools. There is a need to remain objective and not to favour any particular manufacturer over another.

Using the internet is great for young people's education and development. It opens up exciting new opportunities for learning. Whatever they're up to - researching a school project, chatting with friends or playing a game - your children are likely to spend even more time surfing the web as they get older. Fortunately there are some simple things you can do to help them surf safely and feel confident about learning online.

 Becta Next generation Learning page
http://www.nextgenerationlearning.org.uk/

 Becta e-safety quiz for parents
http://www.nextgenerationlearning.org.uk/en/Benefits/E-Safety-Quiz/
 http://www.nextgenerationlearning.org.uk/en/Benefits/learn-safelyonline/
 http://www.thinkuknow.co.uk/

 The Byron Report
http://www.dcsf.gov.uk/byronreview/pdfs/Final%20Report%20Bookmarked.pdf

 The Byron Report. Children's Summary
http://www.dcsf.gov.uk/byronreview/pdfs/A%20Summary%20for%20Children%20and%20Young%20People%20FINAL.pdf

 The Byron Report Executive Summary
http://www.dcsf.gov.uk/byronreview/pdfs/Executive%20summary.pdf

Home wireless networks

Wireless networks should be properly encrypted.
(Instructions on how to do this usually come with the wireless router) failure to do so renders the account holder liable for any misuse of the internet connection associated with the unencrypted network and may allow others to see and access computers and peripheral devices connected to it.

Location of computer(s)

Computers should be in a public area. It is good practice where there is a case for the computer being in a bedroom or other out of line of sight location for an agreement to be reached stating that the computer will be monitored from time to time.

Internet Service Provider child controls

Internet or operating system child controls should be investigated and used. This may require you to set up logons at home, or separate logon accounts with your internet service provider.
Most will permit a number of sub accounts.
The benefits of doing so give peace of mind and will in some cases allow for usage reports to be generated.
It is reasonable for users of home systems to accept that they can be monitored from time to time.

Anti-Virus, spyware/malware

Robust all round anti-virus/spyware/malware solutions should be in place at all times and updated frequently in line with the manufacturer's guidance.
Individuals may be liable for damage caused to other systems by malware imported from home systems.

Appendix E
Legal Framework

Notes on the legal framework
Many young people, and indeed some staff, use the Internet regularly without being aware that some of the activities they take part in are potentially illegal. The law is developing rapidly and changes occur frequently. Please note this section is designed to inform users of legal issues relevant to the use of communications, it is not professional advice.

Racial and Religious Hatred Act 2006
This Act makes it a criminal offence to threaten people because of their faith, or to stir up religious hatred by displaying, publishing or distributing written material which is threatening. Other laws already protect people from threats based on their race, nationality or ethnic background.

Criminal Justice Act 2003
Section 146 of the Criminal Justice Act 2003 came into effect in April 2005, empowering courts to impose tougher sentences for offences motivated or aggravated by the victim's sexual orientation in England and Wales.

Sexual Offences Act 2003
It is an offence to take, permit to be taken, make, possess, show, distribute or advertise indecent images of children in the United Kingdom. 'A child' for these purposes is anyone under the age of 18. Viewing an indecent image of a child on your computer means that you have made a digital image. An image of a child also covers pseudo-photographs (digitally collated or otherwise). This can include images taken by and distributed by the child themselves (often referred to as "Sexting"). A person convicted of such an offence may face up to 10 years in prison.
The offence of grooming is committed if you are over 18 and have communicated with a child under 16 at least twice (including by phone or using the Internet). It is an offence to meet them or travel to meet them anywhere in the world with the intention of committing a sexual offence.
Causing a child under 16 to watch a sexual act is illegal, including looking at images such as videos, photos or webcams, for your own gratification.
It is also an offence for a person in a position of trust to engage in sexual activity with any person under 18, with whom they are in a position of trust. (Typically, teachers, social workers, health professionals, connexions staff etc fall into this category of trust).
Any sexual intercourse with a child under the age of 13 commits the offence of rape.
N.B. Schools should already have a copy of "Children & Families: Safer from Sexual Crime" document as part of their child protection packs.
More information about the 2003 Act can be found at www.teachernet.gov.uk

Communications Act 2003 (section 127)
Sending by means of the Internet a message or other matter that is grossly offensive or of an indecent, obscene or menacing character; or sending a false message by means of or persistently making use of the Internet for the purpose of causing annoyance, inconvenience or needless anxiety is guilty of an offence liable, on conviction, to imprisonment.
This wording is important because an offence is complete as soon as the message has been sent: there is no need to prove any intent or purpose.

Data Protection Act 1998

The Act requires anyone who handles personal information to notify the Information Commissioner's Office of the type of processing it administers, and must comply with important data protection principles when treating personal data relating to any living individual. The Act also grants individuals rights of access to their personal data, compensation and prevention of processing.

The Computer Misuse Act 1990 (sections 1 — 3)

Regardless of an individual's motivation, the Act makes it a criminal offence to:

- Gain access to computer files or software without permission (for example using someone else's password to access files)
- Gain unauthorised access, as above, in order to commit a further criminal act (such as fraud)
- Impair the operation of a computer or program (for example caused by viruses or denial of service attacks) UK citizens or residents may be extradited to another country if they are suspected of committing any of the above offences.

Malicious Communications Act 1988 (section 1)

This legislation makes it a criminal offence to send an electronic message (email) that conveys indecent, grossly offensive, threatening material or information that is false; or is of an indecent or grossly offensive nature if the purpose was to cause a recipient to suffer distress or anxiety. This can include racist, xenophobic and homophobic comments, messages etc.

Copyright, Design and Patents Act 1988

Copyright is the right to prevent others from copying or using his or her "work" without permission. The material to which copyright may pertain (known in the business as "work") must be the author's own creation and the result of some skill and judgement.

It comes about when an individual expresses an idea in a tangible form. Works such as text, music, sound, film and programs all qualify for copyright protection. The author of the work is usually the copyright owner, but if it was created during the course of employment it belongs to the employer.

It is an infringement of copyright to copy all or a substantial part of anyone's work without obtaining the author's permission. Usually a licence associated with the work will allow a user to copy or use it for limited purposes. It is always advisable to read the terms of a licence before you copy or use someone else's material.

It is also illegal to adapt or use software without a licence or in ways prohibited by the terms of the software licence.

Public Order Act 1986 (sections 17 — 29)

This Act makes it a criminal offence to stir up racial hatred by displaying, publishing or distributing written material which is threatening. Like the Racial and Religious

Hatred Act 2006 it also makes the possession of inflammatory material with a view of releasing it a criminal offence.

Obscene Publications Act 1959 and 1964

Publishing an "obscene" article is a criminal offence. Publishing includes electronic transmission.

Protection from Harassment Act 1997

A person must not pursue a course of conduct, which amounts to the harassment of another, and which he knows or ought to know amounts to harassment of the other. A person whose course of conduct causes another to fear, on at least two occasions, that violence will be used against him is guilty of an offence if he knows or ought to know that his course of conduct will cause the other so to fear on each of those occasions.
This also includes incidents of racism, xenophobia and homophobia.

Regulation of Investigatory Powers Act 2000

The Regulation of Investigatory Powers Act 2000 (RIP) regulates the interception of communications and makes it an offence to intercept or monitor communications without the consent of the parties involved in the communication. The RIP was enacted to comply with the Human Rights Act 1998.
The Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000, however, permit a degree of monitoring and record keeping, for example, to ensure communications are relevant to school activity or to investigate or detect unauthorised use of the network. Nevertheless, any monitoring is subject to informed consent, which means steps must have been taken to ensure that everyone who may use the system is informed that communications may be monitored.
Covert monitoring without informing users that surveillance is taking place risks breaching data protection and privacy legislation.

Criminal Justice and Immigration Act 2008

Section 63 offence to possess “extreme pornographic image”
63 (6) must be “grossly offensive, disgusting or otherwise obscene”
63 (7) this includes images of “threats to a person life or injury to anus, breasts or genitals, sexual acts with a corpse or animal whether alive or dead” must also be “explicit and realistic” Penalties can be up to 3 years imprisonment.

Education and Inspections Act 2006

Education and Inspections Act 2006 outlines legal powers for schools which relate to cyberbullying/bullying:
Headteachers have the power “to such an extent as is reasonable” to regulate the conduct of pupils off site.
School staff are able to confiscate items such as mobile ‘phones etc when they are being used to cause a disturbance in class or otherwise contravene the school behaviour/anti-bullying policy.

E.Karwowski
ICT Lead
August 2016
Review date: August 2018