Bracknell Forest Partnership
Community Safety Partnership

Bracknell Forest Council

e-safety Exemplar Policy and Guidance 2012

Contents

1. Introduction
2. Background
3. Duty of Care by Organisations
4. The Risks
5. Acceptable Use Policies (AUPs)
6. e-safety Lead
7. Managing Incidents

Appendices

A. e-safety Rules (Younger child)
B. Online Safety Rights Charter (Older child/young person)
C. Internet Safety Tips and Tricks (Vulnerable Adult with mental capacity and their parents/carers)
D. Be safe when using the internet (Vulnerable Adult without mental capacity)
E. Example Policy: Organisation Staff and Volunteers
F. Inappropriate and Illegal Online Acts
G. Legal Framework
H. Facebook Guidance for Schools (Cyberbullying/Inappropriate Behaviour)
I. Example Policy: Parents and Carers
J. School Policy Template: Electronic Devices – Searching and Deletion
K. Further Guidance

1 Introduction

This policy provides guidance on effective approaches to e-safety for organisations in Bracknell Forest.

It covers:

- **Policies and guidance** to enable organisations to support the e-safety of children, young people and vulnerable adults
- The **responses** necessary when a risk to a child, young person or vulnerable adult is discovered
- **Awareness-raising** for children, young people, vulnerable adults, their parents/carers and organisation staff and volunteers so that they are able to keep themselves, as well as those in their care, as safe as possible when using the internet and other electronic communication technologies

It is essential that existing policies, held by organisations, are applied to the digital environment and regularly reviewed against this e-safety guidance and updated as necessary.

This guidance can be used as a stand-alone document or it can be used to inform existing policies. It should also be read in conjunction with the Bracknell Forest Community Safety Partnership's (CSP's) e-safety Strategy and Action Plan (http://www.bracknell-forest.gov.uk/esafety), the Berkshire Local Safeguarding Children Board Child Protection Procedures (http://proceduresonline.com/berks/) and the Berkshire Safeguarding Adults Policy and Procedures (2011) (http://berksadultsg.proceduresonline.com/index.htm).

2 Background

Definition: e-safety is defined as being safe from risks to personal safety and well-being when using all fixed and mobile devices that allow access to the internet as well as those that are used to communicate electronically. This includes personal computers, laptops, mobile phones and gaming consoles such as Xbox, Playstation and Wii.

Safeguarding against these risks is not just an ICT responsibility, it is everyone's responsibility and needs to be considered as part of the overall arrangements in place that safeguard and promote the welfare of all members of the community, particularly those that are vulnerable.

3 Duty of Care by Organisations

As part of the Every Child Matters agenda set out by the Government (Education Act 2002 and the Children Act 2004) and the 'No Secrets' agenda, produced by the Government in 2000, it is the duty of organisations to ensure that children, young people and vulnerable adults are protected from potential harm.

In order to do this, vulnerable individuals in our community and their parents/carers need to be involved in the safe use of on-line technologies. It is also important that adults who work with these vulnerable people are clear about safe practices so that they are safeguarded from misunderstanding or being involved in possible allegations of inappropriate behaviour.

Unfortunately, it is not possible to create a 100% safe environment and it is the organisation's responsibility to demonstrate that they have managed the risks and done everything they reasonably could to protect the children, young people or vulnerable adults that they work with. Organisations require policies and procedures that are clear and easy to follow so that risks are minimised and any incidents that do occur can be dealt with quickly and effectively.

Children, young people and vulnerable adults need to be as 'savvy' as possible about what they read, hear and see. In the same way that the quality of information received via radio, newspaper and television is variable, everyone needs to be helped to develop skills in selection and evaluation of internet-based information. It is therefore important that any education programme links to activities that help evaluate what is fact, what is fiction, what is opinion and whether something is plausible or biased.

In addition to accessing the internet in organisation settings, children, young people and vulnerable adults may access the internet and/or use other digital technologies in their own time at other locations. This is when they will be at greater risk if they have not been taught about how to use them safely and what the dangers are.

4 The Risks

The internet is an essential element in 21st century life and ICT knowledge, now seen as an important life-skill, is vital to access life-long learning and employment. It is also important to recognise that the internet provides many benefits, not just to children, young people and vulnerable adults, but also to the professional work of staff.

While acknowledging the benefits, it is also important to recognise that risk to safety and well-being of users is ever-changing as technologies develop. These can be summarised as follows:

- Content
  - Commercial (adverts, spam, sponsorship, personal information)
  - Aggressive (violent/hateful content)
  - Sexual (pornographic or unwelcome sexual content)
  - Values (bias, racism, misleading info or advice)
- Contact
  - Commercial (tracking, harvesting personal information
  - Aggressive (being bullied, harassed or stalked)
  - Sexual (meeting strangers, being groomed)
  - Values (self-harm, unwelcome persuasions)
- Conduct
  - Commercial (illegal downloading, hacking, gambling, financial scams, terrorism)
  - Aggressive (bullying or harassing another)
  - Sexual (creating and uploading inappropriate material)
  - Values (providing misleading info or advice)

Much of the material on the internet is published for an adult audience and some is unsuitable for children and young people. In addition, there is information on weapons, crime and racism that would be considered ***inappropriate and restricted*** elsewhere.

It is also known that adults who wish to abuse others may pose as a child/young person/peer to engage with them and then attempt to meet up with them. This process is known as ***'grooming'*** and may take place over a period of months using chat rooms, social networking sites and mobile phones.

Cyberbullying is bullying through the use of communication technology and can take many forms e.g. sending threatening or abusive text messages or e-mails either personally or anonymously, making insulting comments about someone on a social networking site or blog or making/sharing derogatory or embarrassing videos of someone via mobile phone or e-mail.

5 Acceptable Use Policies (AUPs)

All organisations providing internet access for children, young people and vulnerable adults should have AUPs in place which set out guidance for the acceptable, safe and responsible use of on-line technologies. The correct and appropriate use of AUPs will safeguard not only those that are vulnerable but also adults who work or volunteer within these settings. It may be appropriate to develop a number of documents as part of the AUP for different audiences (a number of examples are included in this document as appendices).

6 e-safety Lead

It is important to have a lead e-safety person (usually the manager or child protection lead) within each organisation whose main roles and responsibilities should include:

- Maintaining the AUPs
- Ensuring that the organisation’s policies and procedures include aspects of e-safety.
- Working with the filter system provider to ensure that the filtering is set at the correct level for staff, children, young people and vulnerable adults
- Report issues to the head of the organisation
- Ensure that staff participate in e-safety training
- Ensure that e-safety is included in staff induction
- Monitor and evaluate incidents that occur to inform future safeguarding developments

7 Managing Incidents

The organisation manager/e-safety lead/child protection lead will ensure that an adult follows these procedures in the event of any misuse of the internet:

Has there been inappropriate contact?

1. Report to the organisation manager/e-safety lead/child protection officer
2. Advise the child, young person or vulnerable adult on how to terminate the communication and save all evidence
3. Contact the parent(s)/carer(s)
4. Contact the police on 101
5. Log the incident
6. Identify support for the child, young person or vulnerable adult

Has someone been bullied?

1. Report to the organisation manager/e-safety lead/child protection officer
2. Advise the child, young person or vulnerable adult not to respond to the message
3. Refer to relevant policies including anti-bullying, e-safety and AUP and apply appropriate sanctions
4. Secure and preserve any evidence
5. Contact the parent(s)/carer(s)
6. Consider informing the police on 101, depending on the severity or repetitious nature of the offence
7. Log the incident
8. Identify support for the child, young person or vulnerable adult

Has someone made malicious/threatening comments? (child/young person/vulnerable adult or organisation staff/volunteer)

1. Report to the organisation manager/e-safety lead/child protection officer
2. Secure and preserve any evidence
3. In the case of offending web-based e-mails being received, capture/copy the ‘header’ info, if possible.
4. Inform and request that the comments are removed from the site/block the sender
5. Inform the police on 101 as appropriate
6. Log the incident
7. Identify support for the child, young person or vulnerable adult

Has an inappropriate/illegal website been viewed?

1. Report to the organisation manager/e-safety lead/child protection officer
2. If illegal (See Appendix F), do not log off the computer but disconnect from the electricity supply and contact the police on 101
3. Record the website address as well as the date and time of access
4. If inappropriate (See Appendix F), refer the child/young person/vulnerable adult to the AUP that was agreed and reinforce the message
5. Decide on the appropriate sanction
6. Inform the parent(s)/carer(s)
7. Contact the filtering software provider to notify them of the website
8. Log the incident

9. Identify support for the child, young person or vulnerable adult

Has an allegation been made against a member organisation staff/volunteer?

Child/Young People Organisation

In the case of the above, the Berkshire LSCB Child Protection Procedures should be referred to (http://proceduresonline.com/berks/).

All allegations should be reported to the organisation manager, police (101) and the Local Authority Designated Officer (LADO) (01344 352020), as appropriate.

Vulnerable Adult Organisation

In the case of the above, the Berkshire Safeguarding Adults Policy and Procedures 2011 should be referred to (http://berksadultsg.proceduresonline.com/index.htm).

All allegations should be reported to the organisation manager, police (101) and the Community Response and Re-enablement Team (01344 351500), as appropriate.

Note: Please refer to Appendix F for a summary of what constitutes inappropriate and illegal acts involving the internet and electronic communication technologies. Further advice and guidance is shown below.

Children and Young People

To discuss an e-safety concern involving a child or young person, please contact 01344 352020

Vulnerable Adults

To discuss an e-safety concern involving a vulnerable adult, please contact Adult Social Care and Health Community Response and Re-enablement Team on 01344 351500

For professional advice, contact the UK Safer Internet Centre's Helpline on helpline@saferinternet.org.uk or 0844 381 4772.

To request an e-safety presentation for parents/carers or for children, young people and vulnerable adults, please contact Childnet on kidsmart@childnet.com or Microsoft on stuartha@microsoft.com.

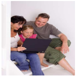
To request to attend e-safety workforce training, please contact Liz Challis at Bracknell Forest Council on 01344-352000.

APPENDICES

Appendix A

e-safety Rules

Ask permission before using the internet



Tell a trusted adult if you see anything that makes you feel uncomfortable

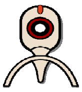
Immediately close any webpage that you are uncomfortable with

Do not give out any personal information such as name, address, telephone number(s), age, school name or bank card details

Make sure that when using social networking sites, privacy settings are checked so that not just anyone can see your page/photos

Only contact people that you have actually met in the real world

Never arrange to meet someone that you have only met on the internet



Only use a webcam with people you know

Think very carefully about any pictures that you post online

Never be mean or nasty to anyone on the internet or when using a mobile phone. If you know of someone being mean to another person, tell a trusted adult

Only open e-mails from people that you know

Avoid using websites that you wouldn't tell anyone about and use a student friendly search engine such as http://www.askforkids.com

Appendix B

Bracknell Forest Partnership
Community Safety Partnership

Bracknell Forest Council

Online Safety Rights Charter

I - You have the right to **enjoy the internet** and all the fun and safe things it has to offer.

II - You have the right to **keep information about you private**. You only have to tell people what you really want them to know.

III - You have the right to explore the internet but remember that you **cannot trust everything that you see or read** on the internet.

IV - You have the right to **know who you are talking to** on the internet. You don't have to talk to someone if you don't want to.

V - Remember **not everyone is who they say they are** on the internet. You have the right to tell someone if you think anyone is suspicious. If you arrange to meet someone, tell a trusted adult or take a friend with you.

VI - You have the right **NOT to fill out forms or to answer questions** you find on the internet.

VII - You have the right **NOT to be videoed or photographed** by anyone using cameras, web cams or mobile phones.

VIII - You have the right **NOT to have any videos or images** of yourself put on the internet and you have the right to report it to an adult if anyone does this. (Remember that once images are posted online, they may not be able to be withdrawn).

IX - You have the right **NOT to be bullied by others** on the internet and you have the right to report it to an adult if this happens.

X - If you **accidently see something you shouldn't**, you have the right to tell someone and not to feel guilty about it.

XI - We are **ALL responsible for treating everyone online with respect**. You should not use behaviour or language that would be offensive or upsetting to somebody else.

This Rights Charter Was Developed By Oldham Youth Council

Appendix C

Internet Safety Tips and Tricks

It is important for carers to remind any vulnerable person who uses the internet or other communication technology of the following:

- Always explore the privacy settings of your social networking site to protect your privacy and to protect yourself from strangers (for a range of online tutorials, go to http://www.kidsmart.org.uk/skills-school/)
- Facebook users can download a CEOP application to their Facebook page at http://apps.facebook.com/clickceop which enables quick access to help at a touch of a button
- Get friends and family to have a look at your social networking site to check that you aren’t giving out too much personal information or posting inappropriate photos/films. They might see something you’ve missed
- Keep your passwords to yourself
- Respect yourself and others online
- If you are unlucky enough to have a bad experience, online report it to the service provider and tell a trusted person. You can also report to: CEOP REPORT ceop.police.uk
  or phone 101 (police non-emergency number)
- Cyberbullying is never acceptable. If you or someone you know is targeted by bullies online, tell them to:
  - report the bully to the website/service operator
  - keep evidence of the bullying behaviour
  - resist the temptation to reply to nasty messages
  - tell a trusted person

For more advice and tips, go to: http://www.bracknell-forest.gov.uk/esafety

Appendix D

Be safe when using the Internet

Ask someone you trust to make sure you are safe on the internet and Facebook (find out more at http://www.kidsmart.org.uk/skills-school/).

Never tell anyone anything about you on the internet.

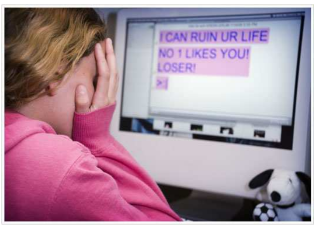
Never show them pictures. Tell someone you trust what you talked about on the internet.

Never tell anyone your passwords.

Be nice to others online.

On Facebook, click on http://apps.facebook.com/clickceop. You will get a button. Click on it if someone does something bad to you on Facebook.

CEOP REPORT
ceop.police.uk



If someone is nasty to you on the internet, tell someone who looks after you. Phone 101 to tell the police, or www.ceop.police.uk

Never let people say nasty things to you on the internet. If they are:

- Tell the website
- Do not delete the nasty things they said
- Do not speak to them anymore
- Do not say nasty things to them
- Tell someone you trust

For more tips, go to: http://www.bracknell-forest.gov.uk/esafety

Appendix E

Example Policy: Organisation Staff and Volunteers

This covers use of digital technologies in the organisation i.e. e-mail, internet, intranet and network resources, learning platforms, software, mobile technologies, equipment and systems.

- I will only use the organisation's digital technology resources and systems for professional purposes or for uses deemed reasonable by the manager.
- I will only use secure e-mail system(s) for any organisation's business (web mail accounts are not secure e-mail system(s)).
- I will not browse, download or send material that could be considered offensive to colleagues and any other individuals.
- I will report any accidental access, receipt of inappropriate materials or filtering breaches to the manager.
- I will not allow unauthorised individuals to access e-mail / internet / intranet / networks or systems.
- I will ensure that all my login credentials (including passwords) are not shared with any other individuals, displayed or used by any individual than myself.
- I will not download any software or resources from the internet that can compromise the network or are not adequately licensed.
- I will follow the DSCF 2009 'Guidance for Safer Working Practice for Adults who work with Children and Young People' (http://www.timeplan.com/uploads/documents/Downloads/Safer-Working-Practices.pdf
- I will ensure that my personal e-mail accounts, mobile/home telephone numbers are not shared with children, young people or families.
- I will not allow children and young people to add me as a friend to their social networking site nor will I add them as friends to my social networking site.
- I will ensure that any private social networking sites / blogs etc. that I create or actively contribute to are not confused with my professional role.
- I understand that all internet and network usage can be logged and this information could be made available to my manager on request.
- I will not connect a computer, laptop or other device to the network/internet that has not been approved by the organisation and meets its minimum security specification.
- I will not use personal digital cameras or camera phones for transferring images of children and young people or staff without permission.
- I will not engage in any online activity that may compromise my professional responsibilities.
- I understand that the Data Protection Act requires that any information seen by me with regard to staff or children and young people, held within any organisation system, will be kept private and confidential, EXCEPT when it is deemed necessary that I am required by law to disclose such information to an appropriate authority.

- I will at all times behave responsibly and professionally in the digital world and will not publish any work-related content on the internet.
- I will ensure that I am aware of digital safeguarding issues so that they are appropriately embedded in my practice.
- I understand that failure to comply with this Acceptable Use Policy (AUP) could lead to disciplinary action.

User Signature

I understand that it is my responsibility to ensure that I remain up-to-date and read and understand the organisation’s most recent Acceptable Use Policy (AUP).

I agree to abide by the organisation’s most recent Acceptable Use Policy (AUP).

Signature …………………….…………… Date ……………………

Full Name ……………………………....................................... (print)

Job title . . . .

Organisation . . . .

Authorised Signature/Manager

I approve this user to be set-up.

Signature ……………………………….…..... Date ……………………

Full Name ……………………………….....… (print)

Appendix F

Inappropriate and Illegal Online Acts

Children, young people, vulnerable adults as well as organisation staff and volunteers who work with them must be aware of what is considered to be criminal when using the internet and electronic communication technologies. This should be reflected in the AUPs and education programmes delivered on an ongoing basis. While the list below is not exhaustive, it is hoped to provide some guidance in assessing the seriousness of incidents as well as determining appropriate actions.

It is noted that all incident types below are considered criminal in nature but would be subject a full investigation in order to determine whether a crime has been committed or not.

- Copyright infringement through copying diagrams, texts and photos without acknowledging the source
- Misuse of logins (using someone else's login)
- Distributing, printing or viewing information on the following:
  - Soft-core pornography
  - Hate material
  - Drugs
  - Weapons
  - Violence
  - Racism
- Distributing viruses
- Hacking sites
- Gambling
- Accessing age restricted material
- Bullying of anyone
- Viewing, production, distribution and possession of indecent images of children[1]
- Grooming and harassment of a child or young person
- Viewing, production, distribution and possession of extreme pornographic images
- Buying or selling stolen goods
- Inciting religious hatred and acts of terrorism
- Downloading multimedia (music and films) that has copyright attached. (Although this is illegal most police forces would treat this as a lower priority than the cases above)[2]

[1] Where the victim is under the age of 18 (recently changed from 16 years old by Section 1 of the Protection of Children Act 1988, as amended by the Criminal Justice and Public Order Act 1994 and Schedule 6 of the Sexual Offences Act 2003) and where the offender has attained the age of 10 (criminal age of responsibility). It is noted that the viewing of information of this nature may, in some circumstances, be appropriate i.e. research on hate crime, drugs etc.

[2] Compiled in consultation with Thames Valley Police and SEGfL

Legal Framework

Appendix G

Notes on the legal framework

This section is designed to inform users of potential legal issues relevant to the use of electronic communications. It is not professional advice and organisations should always consult with their legal team or the police.

Many young people and indeed some organisation staff and volunteers use the internet regularly without being aware that some of the activities they take part in are potentially illegal. Please note that the law around this area is constantly updating due to the rapidly changing nature of the internet.

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 in this category of trust). Any sexual intercourse with a child under the age of 13 commits the offence of rape. N.B. Schools should have a copy of "Children & Families: Safer from Sexual Crime" document as part of their child protection packs.

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 (e.g. using someone else's password to access files);
- gain unauthorised access, as above, in order to commit a further criminal act (such as fraud); or
- impair the operation of a computer or program (e.g. 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 (e-mail) 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.

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 attach (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 advisable always 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 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.

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 (please see Appendix J for a more detailed template/policy).

Appendix H

Facebook Guidance for Schools (Cyberbullying/Inappropriate Behaviour)

1. If you know the identity of the perpetrator, contacting their parents or, in the case of older children, the young person themselves to ask that the offending content be removed, often works.

2. Failing that, having kept a copy of the page or message in question, delete the content.

3. For messages, the ‘delete and report / block user facilities’ are found in the ‘Actions’ dropdown on the page on which the message appears.

4. For whole pages, the ‘unfriend and report / block user facilities’ are at the bottom of the left hand column. Always try to cite which of the Facebook Terms and Conditions have been violated (see note 10 for the most likely ones) at http://www.facebook.com/terms.php or Community Standards at http://www.facebook.com/communitystandards/. Note that Facebook are more alert to US law than UK. The process should be anonymous.

5. If the page is by someone under 13 click on http://www.facebook.com/help/contact.php?show_form=underage (Facebook say they will delete any such page).

6. To remove a post from a profile, hover over it and on the right there will be a cross to delete it.

7. Does the incident trigger the need to inform the police or child protection agencies?

8. To report abuse or harassment, email abuse@facebook.com (Facebook will acknowledge receipt of you email and start looking into your complaint within 24 hours. They will get back to you within 72 hours of receiving your complaint).

9. If all else fails, support the victim, if they wish, to click the ‘Click CEOP’ button http://www.thinkuknow.co.uk/

CEOP REPORT
ceop.police.uk

10. If the victim is determined to continue using Facebook, they might want to delete their account and start again under a different name. Deletion can be done here https://ssl.facebook.com/help/contact.php?show_form=delete_account. They should be made aware of the privacy issues that might have given rise to their problem in the first place:

    - You will not bully, intimidate, or harass any user (1.3.6)
    - You will not provide any false personal information on Facebook, or create an account for anyone other than yourself without permission (4.1)

- You will not post content or take any action on Facebook that infringes or violates someone else's rights or otherwise violates the law (5.1)

NOTE: An effective education programme can help to reduce the number of times that this sort of incident arises, over the medium term. Such a programme should help young people to match their online behaviour with their offline behaviour by helping them to develop understanding, skills and behaviours in these sorts of areas:

- possible consequences
- understanding the effects of bullying on others
- understanding how technology can magnify impact
- understanding how comments or other actions can be perceived differently by the originator and the target

Appendix I

Example Policy: Parents and Carers

Internet and ICT: As the parent or legal guardian of the student(s) named below, I am aware that my *daughter / son* will have access to:

- the internet at school
- the school’s chosen e-mail system
- the school’s online managed learning environment
- ICT facilities and equipment at the school ✓

I accept that ultimately the school cannot be held responsible for the nature and content of materials accessed through the internet and mobile technologies but I understand that the school takes every reasonable precaution to keep students safe and to prevent students from accessing inappropriate materials. ✓

I understand that the school can, if necessary, check my child’s computer files and the internet sites they visit at school and, if there are concerns about my child’s e-safety or behaviour online, they will contact me. ✓

Use of digital images, photography and video: I understand the school has a clear policy on “The Use of Digital Images and Video” and I support this. ✓

I understand that the school will necessarily use photographs of my child or include them in video material to support learning activities. ✓

(The school should make a judgement with the inclusion of the following statement):

I accept that the school may use photographs / video that includes my child in publicity that reasonably promotes the work of the school and for no other purpose. ✓

I will not take, and then share online, photographs of other children (or staff) at school events without permission. ✓

Social networking and media sites: I understand that the school has a clear policy on *“The Use of Social Networking and Media Sites” (schools may have a similar document with a different title)* and I support this. ✓

I understand that the school takes any inappropriate behaviour seriously and will respond to observed or reported inappropriate or unsafe behaviour. ✓

I will support the school by promoting safe use of the internet and digital technology at home. I will inform the school if I have any concerns. ✓

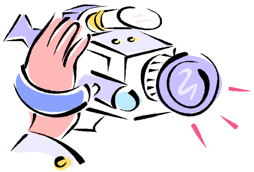
I acknowledge that schools now have powers under the Education Act 2011 to search students for ‘prohibited items’ which covers any article that a member of staff suspects has been, or could be, used to commit an offence. These powers also allow the item to be seized, delivered to the police, returned to its owner, retained or disposed. *(Note: A more detailed separate exemplar policy on these powers is available from Bracknell Forest Council)* ✓

My daughter / son name(s): _______________________________________

Parent / guardian signature: ______________________________

Date: ___/___/___

The Use of Digital Images and Video



To comply with the Data Protection Act 1998, we need your permission before we can photograph or make recordings of your daughter/son.

We follow these rules for any external use of digital images:

If the student is named, we avoid using their photograph.

If their photograph is used, we avoid naming the student.

Where showcasing examples of students' work, we only use their first names, rather than their full names.

(The school should make a judgement with the inclusion of the following statement):

If showcasing digital video work to an external audience, we take care to ensure that students are not referred to by name on the video, and that students' full names are not given in credits at the end of the film.

Only images of students in suitable dress are used.

Staffs are not allowed to take photographs or videos on their personal equipment.

Examples of how digital photography and video may be used at school include:

- Your child being photographed (by the class teacher or teaching assistant) as part of a learning activity e.g. taking photos or a video of progress made by a nursery child, as part of the learning record, and then sharing with their parent / guardian.

- Your child's image being used for presentation purposes around the school e.g. in class or wider school wall displays or PowerPoint© presentations.

(The school should make a judgement with the inclusion of the following statement):

- *Your child's image being used in a presentation about the school and its work in order to share its good practice and celebrate its achievements, which is shown to other parents, schools or educators e.g. within a CDROM / DVD or a document sharing good practice; in our school prospectus or on our school website.*
  In rare events, your child's picture could appear in the media if a newspaper photographer or television film crew attends an event.

Note: If we, or you, actually wanted your child's image linked to their name we would contact you separately for permission e.g. if your child won a national competition and wanted to be named in local or government literature.

The Use of Social Networking and On-Line Media

This school asks its whole community to promote the 3 ‘common’ approaches to online behaviour:

- **Common courtesy**
- **Common decency**
- **Common sense**

How do we show common courtesy online?

- We ask someone’s permission before uploading photographs, videos or any other information about them online.
- *We do not write or upload ‘off-hand’, hurtful, rude or derogatory comments and materials. To do so is disrespectful and may upset, distress, bully or harass.*

How do we show common decency online?

- We do not post comments that can be considered **intimidating, racist, sexist, homophobic or defamatory.** This is **cyber-bullying** and may be harassment or libel (i.e. a criminal act).
- When such comments exist online, we do not forward such emails, tweets, videos, etc. to other people/groups. This could be considered criminal behaviour.

How do we show common sense online?

- We think before we click.
- We think before we upload comments, photographs and videos.
- We think before we download or forward any materials.
- We think carefully about what information we share with others online, we check where it is saved and we check our privacy settings.
- We make sure we understand changes in any websites we use.
- We block harassing communications and report any abuse.

NOTE: Any actions online that impact on the school and can potentially lower the school’s (or someone in the school’s) reputation in some way or are deemed as being inappropriate will be responded to.

In the event that any member of staff, student or parent/carer is found to be posting libellous or inflammatory comments on Facebook or other social networking sites, this will be addressed by the school in the first instance. However, if necessary, the police may be involved and/or legal action pursued.

The whole school community is reminded of the CEOP report abuse process:
https://www.thinkuknow.co.uk/parents/browser-safety/

Appendix J

School Policy Template:
Electronic Devices - Searching & Deletion

(June 2012)

The Education Act 2012, the basis of this template, sets out what the law is presumed to be, based on prior legal and educational knowledge, and common sense. Rights and responsibilities regarding physical contact and personal data are still evolving rapidly. So too are social, entertainment and educational technologies and the skills necessary to use them safely and prudently. This is particularly so where those who are under 18 are involved.

No existing law or policy can fully insulate anyone from the risk involved in searching for, access to or deletion of the personal data of others. Anyone refraining from any such search, access or deletion when hindsight shows circumstances merit such actions may however be at significant risk and may put seriously at risk the wellbeing of children entrusted to their care. This template cannot therefore be relied on as justification for any act or lack of action by anyone – there is no substitute for the proper and well documented exercise of adequately informed professional judgement. .

It is for each school's head teacher and governors to set apply and monitor application of their own policies as guided by their head teacher, local authority and official guidance, especially if the school is local authority maintained. This template is intended as an aide to this. South West Grid for Learning Trust does not and cannot accept and does not have responsibility for any school's policy on this or any other matter.

Within this template, sections which include information or guidance are shown in RED. It is anticipated that schools will remove these sections from their completed policy documents, though this will be for the school's relevant policy advisory group to recommend and for the head teacher and other governors to decide upon.

Where sections in the template are written in ITALICS it is anticipated that schools would wish to consider whether or not to include that section or statement in their completed policy.

Where sections are highlighted in BOLD text, it is the view of the SWGfL E-Safety Group that these ought to be an essential part of a school e-safety policy.

The template uses the term students / pupils to refer to the children / young people attending the learning institution and the term Head teacher / Principal. Schools will need to choose which terms to use and delete the others accordingly.

Introduction

The changing face of information technologies and ever increasing pupil / student use of these technologies has meant that the Education Acts have had to change in an attempt to keep pace. Within Part 2 of the Education Act 2011 (Discipline) there have been changes to the powers afforded to schools by statute to search pupils in order to maintain discipline and ensure safety. Schools are required to ensure they have updated policies which take these changes into account. No such policy can on its own guarantee that the school will not face legal challenge, but having a robust policy which takes account of the Act and applying it in practice will however help to provide the school with justification for what it does.

The particular changes we deal with here are the added power to search for items 'banned under the school rules' and the power to 'delete data' stored on seized electronic devices.

Items banned under the school rules are determined and publicised by the Headteacher (section 89 Education and Inspections Act 1996).

An item banned by the school rules may only be searched for under these new powers if it has been identified in the school rules as an item that can be searched for. It is therefore important that there is a school policy which sets out clearly and unambiguously the items which:

- are banned under the school rules; and
- are banned AND can be searched for by authorised school staff

The new act allows authorised persons to examine data on electronic devices if they think there is a good reason to do so. In determining a 'good reason' to examine or erase the data or files the authorised staff member must reasonably suspect that the data or file on the device in question has been, or could be, used to cause harm, to disrupt teaching or could break the school rules.

Following an examination, if the person has decided to return the device to the owner, or to retain or dispose of it, they may erase any data or files, if they think there is a good reason to do so.

The Head Teacher / Principal must publicise the school behaviour policy, in writing, to staff, parents / carers and students / pupils at least once a year. (There should therefore be clear links between the search etc. policy and the behavior policy).

DfE advice on these sections of the Education Act 2011 can be found in the document: "Screening, searching and confiscation – Advice for head teachers, staff and governing bodies"
http://www.education.gov.uk/schools/pupilsupport/behaviour/behaviourpolicies/f0076897/screening-searching-and-confiscation

It is recommended that Headteachers / Principals (and, at the least, other senior leaders) should be familiar with this guidance.

Relevant legislation:

- Education Act 1996
- Education and Inspections Act 2006
- Education Act 2011 Part 2 (Discipline)
- The School Behaviour (Determination and Publicising of Measures in Academies) Regulations 2012
- Health and Safety at Work etc. Act 1974
- Obscene Publications Act 1959
- Children Act 1989
- Human Rights Act 1998
- Computer Misuse Act 1990

This is not a full list of Acts involved in the formation of this advice. Further information about relevant legislation can be found via the above link to the DfE advice document.

Responsibilities

The *Headteacher/Principal* is responsible for ensuring that the school policies reflect the requirements contained within the relevant legislation. The formulation of these policies may be delegated to other individuals or groups. The policies will normally be taken to Governors for approval. The Headteacher/Principal will need to authorise those staff who are allowed to carry out searches.

This policy has been written by and will be reviewed by: insert relevant names / roles / group

The *Headteacher / Principal* has authorised the following members of staff to carry out searches for and of electronic devices and the deletion of data / files on those devices: (the policy should here list those staff / roles given such authority. A Headteacher / Principal may choose to authorise all staff willing to be authorised, but should consider training needs in making this decision).

The *Headteacher / Principal* may authorise other staff members in writing in advance of any search they may undertake, subject to appropriate training.

Members of staff (other than Security Staff) cannot be required to carry out such searches. They can each choose whether or not they wish to be an authorised member of staff.

Training / Awareness

It is essential that all staff should be made aware of and should implement the school's policy.

Members of staff should be made aware of the school's policy on "Electronic devices – searching and deletion":

- at induction
- at regular updating sessions on the school's e-safety policy

Members of staff authorised by the *Headteacher / Principal* to carry out searches for and of electronic devices and to access and delete data / files from those devices should receive training that is specific and relevant to this role.

Specific training is required for those staff who may need to judge whether material that is accessed is inappropriate or illegal.

Policy Statements

Search:

The school Behaviour Policy refers to the policy regarding searches with and without consent for the wide range of items covered within the Education Act 2011 and lists those items. This policy refers only to the searching for and of electronic devices and the deletion of data / files on those devices.

The school will already have a policy relating to whether or not mobile phones and other electronic devices are banned, or are allowed only within certain conditions. The school should therefore consider including one of the following statements in the policy:

Either:
Pupils/students are not allowed to bring mobile phones or other personal electronic devices to school or use them in the school.
Or
*Pupils / students are allowed to bring mobile phones or other personal electronic devices to school and use them only within the rules laid down by the school. (*You should refer to the relevant policy or to list here the conditions under which they are allowed*)*

If pupils / students breach these roles:

Either:
The sanctions for breaking these rules will be: (list here)
Or
The sanctions for breaking these rules can be found in the (name the policy - for many schools this will be the Behaviour Policy)

Authorised staff (defined in the responsibilities section above) have the right to search for such electronic devices where they reasonably suspect that the data or file on the device in question has been, or could be, used to cause harm, to disrupt teaching or break the school rules.

- Searching with consent - Authorised staff may search with the pupil's consent for any item.
- Searching without consent - Authorised staff may only search without the pupil's consent for anything which is either 'prohibited' (as defined in Section 550AA of the Education Act 1996) or appears in the school rules as an item which is banned and may be searched for.

In carrying out the search:

The authorised member of staff must have reasonable grounds for suspecting that a *student / pupil* is in possession of a prohibited item i.e. an item banned by the school rules and which can be searched for. (Whether there are 'reasonable grounds' is a matter decided on by reference to the circumstances witnessed by, or reported to, someone who is authorised and who exercises properly informed professional judgment and has received appropriate training).

The authorised member of staff carrying out the search must be the same gender as the *student / pupil* being searched; and there must be a witness (also a staff member) and, if at all possible, they too should be the same gender as the *student/ pupil* being searched.

There is a limited exception to this rule: Authorised staff can carry out a search of a *student / pupil* of the opposite gender including without a witness present, but **only where you reasonably believe that there is a risk that serious harm will be caused to a person if you do not conduct the search immediately and where it is not reasonably practicable to summon another member of staff.**

Extent of the search:

The person conducting the search may not require the *student/ pupil* to remove any clothing other than outer clothing.

Outer clothing means clothing that is not worn next to the skin or immediately over a garment that is being worn as underwear (outer clothing includes hats; shoes; boots; coat; blazer; jacket; gloves and scarves).

'Possessions' means any goods over which the *student / pupil* has or appears to have control – this includes desks, lockers and bags.

A student's / pupil's possessions can only be searched in the presence of the *student / pupil* and another member of staff, except where there is a risk that serious harm will be caused to a person if the search is not conducted immediately and where it is not reasonably practicable to summon another member of staff.

The power to search without consent enables a personal search, involving removal of outer clothing and searching of pockets; but not an intimate search going further than that, which only a person with more extensive powers (e.g. a police officer) can do.

Use of Force – force cannot be used to search without consent for items banned under the school rules regardless of whether the rules say an item can be searched for.

Electronic devices

An authorised member of staff finding an electronic device may access and examine any data or files on the device if they think there is a good reason to do so (i.e. the staff member must reasonably suspect that the data or file on the device in question has been, or could be, used to cause harm, to disrupt teaching or break the school rules).

The examination of the data / files on the device should go only as far as is reasonably necessary to establish the facts of the incident. Any further intrusive examination of personal data may leave the school open to legal challenge. It is important that authorised staff should have training and sufficient knowledge of electronic devices and data storage.

If inappropriate material is found on the device it is up to the authorised member of staff to decide whether they should delete that material, retain it as evidence (of a criminal offence or a breach of school discipline) or whether the material is of such seriousness that it requires the involvement of the police. Examples of illegal activity would include:

- **child sexual abuse images (including images of one child held by another child)**
- **adult material which potentially breaches the Obscene Publications Act**
- **criminally racist material**
- **other criminal conduct, activity or materials**

Members of staff may require support in judging whether the material is inappropriate or illegal. One or more Senior Leaders should receive additional training to assist with these decisions. Care should be taken not to delete material that might be required in a potential criminal investigation.

The school should also consider their duty of care responsibility in relation to those staff that may access disturbing images or other inappropriate material whilst undertaking a search. Seeing such material can be most upsetting. There should be arrangements in place to support such staff. The school may wish to add further detail about these arrangements.
Further guidance on reporting the incident to the police and the preservation of evidence can be found in the SWGfL flow chart – http://www.swgfl.org.uk/safety/default.asp. Local authorities / LSCBs may also have further guidance, specific to their area.

Deletion of Data

Following an examination of an electronic device, if the authorised member of staff has decided to return the device to the owner, or to retain or dispose of it, they may erase any data or files, if they think there is a good reason to do so. (i.e. the staff member must reasonably suspect that the data or file on the device in question has been, or could be, used to cause harm, to disrupt teaching or break the school rules).

If inappropriate material is found on the device, it is up to the authorised member of staff to decide whether they should delete that material, retain it as evidence (of a possible criminal offence or a breach of school discipline) or whether the material is of such seriousness that it requires the involvement of the police. (It is recommended that members of staff should know who to contact, within school, for further guidance before taking action and that the person or persons is or are named within this policy).

A record should be kept of the reasons for the deletion of data / files. (DfE guidance states and other legal advice recommend that there is no legal reason to do this, best practice suggests that the school can refer to relevant documentation created at the time of any search or data deletion in the event of a pupil /student, parental or other interested party complaint or legal challenge. Records will also help the school to review e-safety incidents, learn from what has happened and adapt and report on application of policies as necessary).

Audit / Monitoring / Reporting / Review

The responsible person (insert title) will ensure that full records are kept of incidents involving the searching for and of mobile phones and electronic devices and the deletion of data / files.

These records will be reviewed by ... *(E-Safety Officer / E-Safety Committee / E-Safety Governor)* at regular intervals *(state the frequency)*.

This policy will be reviewed by the head teacher and governors annually and in response to changes in guidance (DfE guidance will be reviewed in 2013) and evidence gained from the records.

The school is required is publish its Behaviour Policy to parents annually – the Behaviour Policy should be cross referenced with this policy on search and deletion.

Copyright of the SWGfL School E-Safety Policy Templates is held by SWGfL. Schools and other educational institutions are permitted free use of the templates. Any person or organisation wishing to use the document for other purposes should seek consent from SWGfL and acknowledge its use.

Every reasonable effort has been made to ensure that the information included in this template is accurate, as at the date of publication in June 2012. However, SWGfL cannot guarantee its accuracy, nor can it accept liability in respect of the use of the material whether in whole or in part and whether modified or not. Suitable legal / professional advice should be sought if any difficulty arises in respect of any aspect of this new legislation or generally to do with school conduct or discipline.

South West Grid for Learning Trust, Belvedere House, Woodwater Park, Pynes Hill, Exeter, EX2 5WS
Tel: 0845 601 3203 Fax: 01392 366494 Email: enquiries@swgfl.org.uk Website: www.swgfl.org.uk

Appendix K

Further Guidance

CEOP (Child Exploitation and Online Protection Centre)
http://www.ceop.gov.uk

The Child Exploitation and Online Protection (CEOP) Centre is dedicated to eradicating the sexual abuse of children. That means that they are part of UK policing and very much about tracking and bringing offenders to account either directly or in partnership with local and international forces.

Think U Know
http://www.thinkuknow.co.uk

Think U Know is CEOP's support, guidance and resource site for children, young people, parents, carers and adults who work with children and young people.

UK Safer Internet Centre
http://www.saferinternet.org.uk/

This website provides the latest advice on how to use the internet and new technologies safely and responsibly. Also find a range of practical resources, news and events focussing on the safe and responsible use of the internet and new technologies.

Childnet
http://www.childnet-int.org

Childnet is a non-profit organisation working with others to "help make the Internet a great and safe place for children". The website gives news and background to Childnet's work and serves as a portal to Childnet's award-winning projects**.**

Bracknell Forest e-safety webpage
http://bracknell-forest.gov.uk/esafety

These pages define e-safety, describe the possible risks and also detail what Bracknell Forest is doing to safeguard vulnerable users of the internet and other digital technologies in the Borough. It also includes useful resources such as leaflets, videos and guidance which can be downloaded and used within organisations/settings to raise awareness of the risks and how to be safe.

Teach Today
http://www.teachtoday.eu/en/Teacher-advice/Cyberbullying.aspx

Teachtoday provides information and advice for teachers, head teachers, governors and other members of the school workforce about the positive, responsible and safe use of new technologies. The above link provides advice and guidance on cyberbullying towards teaching staff.

NASUWT: The Teachers’ Union

NASUWT
The Teachers’ Union

http://www.nasuwt.org.uk/Whatsnew/Campaigns/StopCyberbullying/index.htm

The NASUWT is the largest teachers' union in the UK.The NASUWT is the only TUC-affiliated teachers’ union to represent teachers in England, Northern Ireland, Scotland and Wales. NASUWT organises in all sectors from early years to further education and represents teachers in all roles including heads and deputies. NASUWT is politically independent and is deeply committed to working to influence the education policy of the Government and employers. The above link provides guidance and support on the subject of cyberbullying towards teaching staff.