OWLSMOOR PRIMARY

E-SAFETY POLICY AND GUIDANCE

Status of Policy	**Date**
BF recommended	
Reviewed	Annually
Policy written	Mar 2012
Last reviewed by governors	25th September 2018
Review due	25th September 2019

This policy has due regard to the requirements of the Equality Act.

This e-safety policy demonstrates the schools commitment to the United Nations Convention on the Rights of the Child (1989) Article 19 (protection from all forms of violence).

e-safety Policy and Guidance

Contents

1 Introduction

This policy provides guidance on effective approaches to e-safety for Owlsmoor Primary School

It covers:

- Policies and guidance to enable Owlsmoor Primary School to support the e-safety of children and young people
- The responses necessary when a risk to a child or a young person is discovered
- Awareness-raising for children and young people so that they are able to keep themselves as safe as possible when using the internet and other digital technologies

The focus of the policy and guidance is to ensure that existing policies are applied to the digital environment. In order for this to happen, it is essential that these policies are regularly reviewed against this e-safety guidance and updated as necessary.

E-safety is a safeguarding issue and we need to review our existing procedures to ensure that e-safety is addressed. This policy and guidance can be used as a stand-alone document or it can be used to inform existing policies.

This policy and guidance should also be read in conjunction with the Bracknell Forest LSCB's e-safety Strategy and Action Plan (http://www.bracknell-forest.gov.uk/e-safety) and the Berkshire LSCB Child Protection Procedures (http://proceduresonline.com/berks/).

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, tablets, ipads, 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 have done everything that they reasonably could in order to protect the children and young people 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 and young people also need to be 'savvy' 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 develop skills in selection and evaluation of internet-based information. Just because something is published in text or on-line does not make it fact. It is therefore important that any education programme links to activities to help pupils evaluate what is fact, what is fiction and what is opinion, and that children and young people consider 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 (child as recipient)
    - Commercial (adverts, spam, sponsorship, personal information)
    - Aggressive (violent/hateful content)
    - Sexual (pornographic or unwelcome sexual content)
    - Values (bias, racism, misleading info or advice)
- Contact (child as participant)
    - Commercial (tracking, harvesting personal information
    - Aggressive (being bullied, harassed or stalked)
    - Sexual (meeting strangers, being groomed)
    - Values (self-harm, unwelcome persuasions)
- Conduct (child as actor)
    - 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)

As Owlsmoor Primary School provides internet access for children and young people we have AUPs in place which set out guidance for the acceptable, safe and responsible use of on-line technologies. AUPs are typically about both child protection and being safe online and the correct and appropriate use of AUPs will safeguard not only children and young people 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 (our acceptable use policies are included in this document as appendices)

- Children and young people
    - consideration needs to be given to the age of the children/young people in the setting
    - it is recommended that all children and young people are made aware of the AUPs and be given a copy
- Parents and carers
- Organisation staff/volunteers (who should sign the AUP)

6 e-safety Lead

Owlsmoor Primary Schools' child protection/e-safety leads main roles and responsibilities include:

- Maintaining the AUPs
- Ensuring that the organisation's policies and procedures include aspects of e-safety. For example: the anti-bullying procedures include cyberbullying and the child protection policy includes internet grooming
- Working with the filter system provider to ensure that the filtering is set at the correct level for staff, children and young people
- 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

Please refer to Appendix D for a summary of what constitutes inappropriate and illegal acts involving internet and electronic communication technologies.

Please refer to Appendix F for a sample flowchart on how to respond to an incident. Further advice and guidance on how to respond is shown below.

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

Inappropriate Contact

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

Bullying

1. Report to the Headteacher/e-safety lead/child protection officer
2. Advise the child or young person 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 child or young person's 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 or young person

Malicious/Threatening Comments Towards a Child, Young Person or Organisation Staff

1. Report to the Headteacher/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 (101) as appropriate
6. Log the incident
7. Identify support for the child or young person

Viewing of an Inappropriate/Illegal Website

1. Report to the Headteacher/e-safety lead/child protection officer
2. If illegal (See Appendix D), 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/time stamp/time zone of access
4. If inappropriate (See Appendix D), refer the child/young person 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 or young person

Allegation against a Member of Owlsmoor Primary School Staff/Volunteer

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 manager, police (101) and Local Authority Designated Officer (LADO) (01344 352020), as appropriate

Note: Please refer to Appendix D 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

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.

OWLSMOOR PRIMARY SCHOOL

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.

For more information, go to http://www.bracknell-forest.gov.uk/esafety or contact the e-safety Lead Officer on 01344 352020.

OWLSMOOR PRIMARY SCHOOL

ZIP IT

Keep your personal stuff private and think about what you say and do online.

BLOCK IT

Block people who send nasty messages and don't open unknown links and attachments.

FLAG IT

Flag up with someone you trust if anything upsets you or if someone asks to meet you offline.

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

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

This page has been developed by the e-safety sub-group of the Bracknell Forest Local Safeguarding Children Board (LSCB). For more information, go to http://www.bracknell-forest.gov.uk/esafety or contact the e-safety Lead Officer on 01344 352020.

OWLSMOOR PRIMARY SCHOOL

Acceptable Use Policy (AUP): Staff

This covers use of digital technologies in the organisation: i.e. e-mail, internet, social networking sites, 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 the council's approved, secure e-mail system(s) for any organisation's business (web mail accounts are not secure e-mail system(s)). I will only use the school e-mail system(s) for any school business. I will not use a personal web mail service such as Hotmail, Yahoo or Gmail to contact professionals, partners or parents/carers regarding school matters.
- 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 not allow students to use a laptop that has been assigned to me. I understand that I will not loan my laptop to a colleague or to anyone else including family members.
- 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 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, tablet, ipad, USB flash drive 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. If personal equipment has been used, then I will allow the Headteacher to delete the images or check that the images have been deleted.
- I will delete ALL images of pupils from my computer, tablet, ipad, camera, and all other data saving devices at the end of each academic year. Unless, they are saved as part of a current, relevant document.
- I will not engage in any online activity that may compromise my professional responsibilities. I will not allow parents or children and young people from this school to add me as a friend to their social networking site nor will I add them as friends to my social networking site. Any staff who are also parents should take individual advice either from the Headteacher or Human Resources at Bracknell Forest Borough Council.
- At home, 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 will not use these forums to make any comments in relation to the school, colleagues or students or to post any information including photographs pertaining to the above.
- I will not carry my personal mobile phone while working, and will only ever use the school's camera, tablet or ipad, for taking pictures in school. My phone will be kept in an agreed area within the school. (See mobile phone and camera policy.)
- I will not share information about the school in internet forums as it is unacceptable and can bring the school and / or the local authority into disrepute and put children at risk. If I see or become aware of inappropriate information about staff or children through conversations with colleagues, parents, partners or on any social networking sites, I understand that I have a responsibility to alert the school. I will keep this information confidential in line with the Data Protection Act and within the school's safeguarding policy. However there may be times when I am required to disclose information to an appropriate authority such as the Police or Children's Social Care. In such cases, I can seek advice from the school's safeguarding officer or Local Authority HR.
- 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 ensure that I am aware of digital safeguarding issues so that they are appropriately embedded in my practice. If I am unsure of digital safeguarding issues, I know that I can contact the school's Safeguarding officer or the ICT subject leader for more information.
- I will ensure that all pupils are supervised while using the internet.
- 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 D

OWLSMOOR PRIMARY SCHOOL

Inappropriate and Illegal Online Acts

Children, young people and adults who work with them must be aware of what is classed as inappropriate and illegal behaviour when using the internet and electronic communication technologies. This should be reflected in the AUPs and education programmes delivered on an ongoing basis. While this list is not exhaustive, it is hoped to provide some guidance in assessing incidents and appropriate actions.

Minor incidents:

- Copyright infringement through copying diagrams, texts and photos without acknowledging the source
- Misuse of logins (using someone else's login)

Inappropriate actions: (some of these actions could be illegal depending on the exact activity)

- 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

Illegal actions: (Contact police)

- Viewing, production, distribution and possession of indecent images of children
- 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)

For further information on the civil and criminal laws that apply please refer to the BECTA publication 'E-safety, developing a whole school polices to support effective practice' Appendix 1 and 2.
http://www.wisekids.org.uk/BECTA%20Publications/esafety.pdf

Appendix E

Legal Framework

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 2018 and General Data Protection Regulations (GDPR).
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 school processes any personal data collected on their forms in line with its data protection policy. Further details can be found in the school's workforce privacy notice.

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.

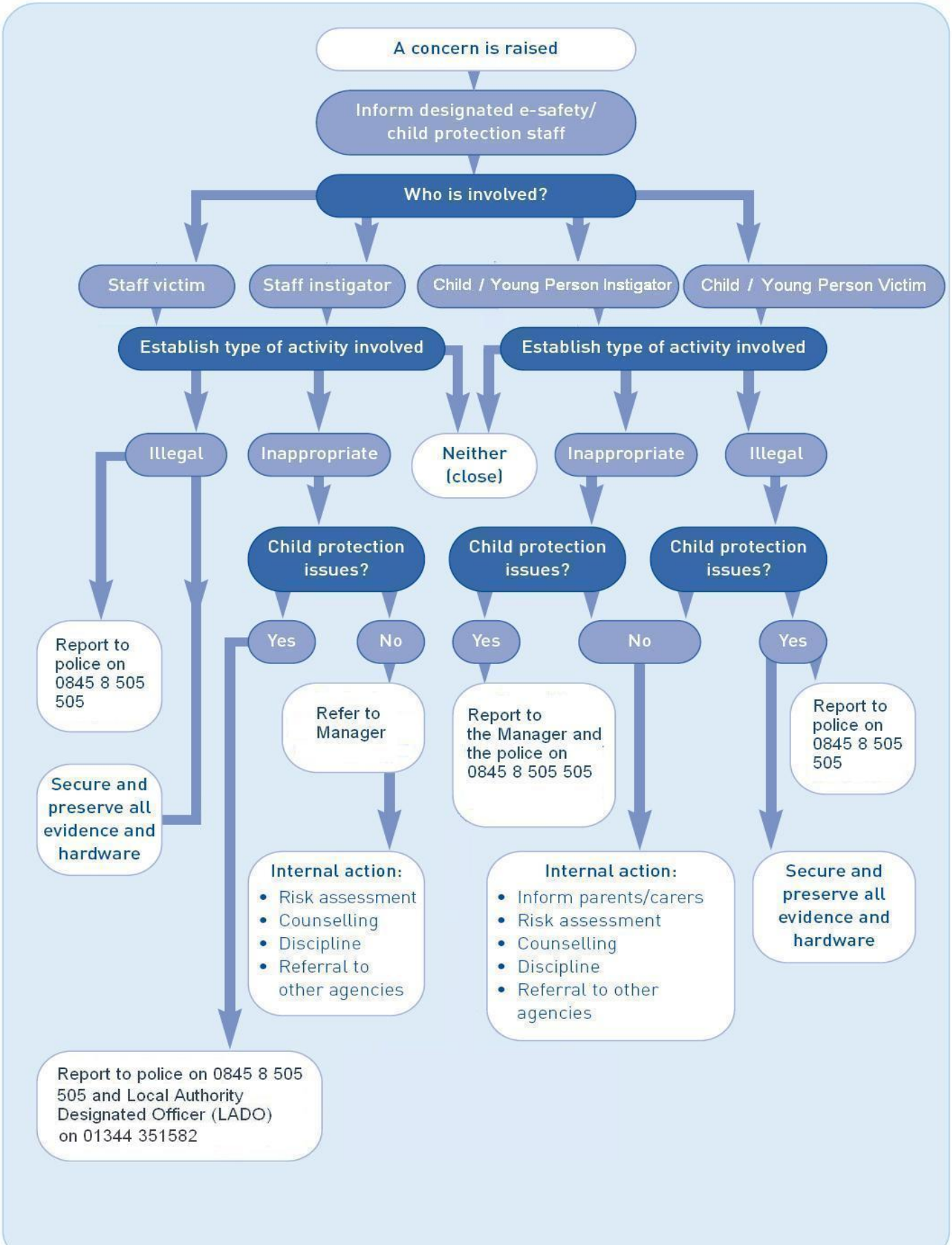
Criminal Justice and Immigration Act 2008
Section 63 offence to possess “extreme pornographic image”
63 (6) must be “grossly offensive, disgusting or otherwise obscene”
63 (7) this includes images of “threats to a person life or injury to anus, breasts or genitals, sexual acts with a corpse or animal 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.

Appendix F

OWLSMOOR PRIMARY SCHOOL

Responding to an Incident



e-safety Websites

CEOP (Child Exploitation and Online Protection Centre)

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.

http://www.ceop.gov.uk

Think U Know

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.

http://www.thinkuknow.co.uk

UKCCIS (UK Council for Child Internet Safety)
Click Clever Click Safe Campaign

This new strategy aims to create a safer online environment, gives everybody the skills, knowledge and understanding to help children and young people to stay safe online and inspire safe and responsible use and behaviour.

ZIP IT, BLOCK IT, FLAG IT: This campaign encourages children to keep safe online by keeping personal information private, blocking messages and reporting inappropriate online behaviour. This new digital code is intended for use by schools, retailers and social network sites and aims to be the 'green cross' code for internet safety. This campaign will be launched in primary schools from 2011 as a compulsory part of the curriculum.

Childnet

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

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.

Internet Watch Foundation (IWF)

IWF hosts the UK Hotline for reporting illegal online content specifically relating to child sexual abuse, criminally obscene as well as incitement to racial hatred.
http://www.iwf.org.uk

Digizen
Digizen provides information about using social network sites and social media sites creatively and safely. It provides tips for evaluating these online resources and examples of how to use them to support informal and formal learning.
http://www.digizen.org

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

Bracknell Forest Anti-Bullying Strategy
http://www.bracknell-forest.gov.uk/anti-bullying-strategy-and-action-plan.pdf

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

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.

Electronic Devices - Searching & Deletion

(June 2012)

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 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 (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 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 will need to authorise those staff who are allowed to carry out searches.

This policy has been written by and will be reviewed by: Headteacher and Governors

The Headteacher 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:

- Headteacher, Deputy Headteacher or Assistant Headteachers.

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

Training / Awareness

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 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:

This policy refers only to the searching for and of electronic devices and the deletion of data / files on those devices.

Pupils 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. (Please refer to our Mobile Phone and Camera Policy which stipulates that all phones belonging to children have to be handed into the school office where they are kept secure during the day)

The sanctions for breaking these rules can be found in 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 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 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 pupil being searched.

There is a limited exception to this rule: Authorised staff can carry out a search of a 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 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 pupil has or appears to have control – this includes desks, lockers and bags.

A pupil’s possessions can only be searched in the presence of the 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 (Headteacher) 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 Governor at regular intervals *(annually)*.

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.

Appendix I

Declaration of Consent for --------

This section is applicable for school activities during the current academic year and must be signed by both the parent/carer and the pupil.

I undertake to inform the Group Leader of any activities/visits that the above named child is participating in of any changes in the fitness of ---------- prior to commencement of any activities/visits.

1. **I consent to the above named participant taking part in the activities/visits organized by the school.**

2. **I agree/do not agree (*please delete as appropriate*) that the staff on these activities/visits can give permission for the Participant to have any medical treatment that medical authorities think necessary, including anesthetic and blood transfusion.**

3. **I agree/do not agree (*please delete as appropriate*) to the use of any photographs and/or videos taken of the Participant being used in the press or promotional material relating to the functions of the school, including the school website. I understand that by agreeing to this, I also agree to the Participant's name being used in any caption or article used with the photograph/video. I also understand that if and to the extent that any resultant photograph/video constitutes personal data within the meaning of the Data Protection Act 2018 and General Data Protection Regulations (GDPR) , my consent operates as consent on behalf of the Participant, required by the Act, but only for the purpose indicated above.**

4. **I hereby give/do not give (*please delete as appropriate*) permission for my child to use the internet during school as the curriculum dictates.**

Signed (parent/carer): **Date:**

Relationship to the Participant:

To be completed by the pupil:

I understand that for the safety of all pupils in the group, I will agree to obey to the rules and instructions of members of staff.

Signature of pupil: **Date:**

(The school processes any personal data collected on this form in line with its data protection policy. Further details can be found in the school's workforce privacy notice.)