DIGITALLY
CONFIDENT

First Line Information Support for Esafety Incidents

Esafety is a key element of safeguarding, subject to inspection by Ofsted and applies to adults and children of all ages.

The consequences of esafety incidents will cover a range of challenges, with consequences that range from those that may appear trivial to serious abuse and loss of life. This means First line colleagues must ensure that they treat all reports with appropriate professionalism and follow correct and agreed procedures.

This resource is intended to provide support for those who are new to esafety and first line support.

You are encouraged to regularly view *digitallyconfident.org* where we provide links to current news, opinion and resources in the areas of digital literacy and online safety.

We gratefully acknowledge the assistance of the following people in collating the following resources;

Penny Patterson – London Grid for Learning
David Wright and Ken Corish – South West Grid for Learning
Alan Mackenzie – Independent esafety advisor

Types of incidents

Predators

There will be cases where children will agree to meet face to face with abusers who they know or who have become 'friends' via online networks. Some children will be victims of emotional, sexual and physical abuse. There are cases where these relationships result in the death of a child.

Some children will be more vulnerable than others however it is important to recognise that all young people can seek comfort and friendship in online relationships. These relationships can appear more open, trusting and supportive than face to face interactions – and as such can pose new and different challenges and dangers.

Bullying & Cyberbullying

Cyberbullying typically takes two forms; by peers and strangers. Most common are the incidents where young people are bullied by other young people who are known to them in their school or wider community. There are incidents where individuals are victims of online bullying by strangers, members of the wider online communities and 'trolls'.

It is also important to note that adults who work with young people can be bullied and threatened by young people, parents and even colleagues.

Illegal or Inappropriate?

It is important to recognise the difference between illegal and inappropriate content and activity. For example; most pornography, whilst inappropriate within a school or work environment, is not illegal. Images of child exploitation (we do not use labels such as 'child pornography' – these images are child abuse and exploitation) are illegal. This can be complicated and sensitive where, for example, children under the age of eighteen are sharing sexual images of themselves. A young person is, in the UK, a child until the age of eighteen and it is understandable that there is ignorance around this when the age of consent is sixteen.

Young people need to be helped to understand that they are creating illegal content which will possibly lead to their friends and relatives becoming convicted and placed on the sex offenders register.

It is also worth noting that using the labels legal and illegal is not always helpful and it is more effective to ascertain; is the activity an offence?

This distinction is important and **if in doubt, err on the side of caution**. It is an offence to open, view, forward, copy and distribute images of child sex abuse. This means you must not forward or copy files and links to share with colleagues, authorities or the police.

Offence

- Opening an attachment or URL that proves to hold illegal content is an illegal act and is classed as possession of illegal material.
- Showing anyone else illegal material that you have received is an illegal act
- Printing and sharing a copy of the material is an illegal act and is classed as distributing illegal material.

Not an Offence

- Receiving unsolicited emails that may contain potentially illegal material (either as an attachment or in a URL) is not an illegal offence

Never open unsolicited URLs or attachments. If you are suspicious that the content could be illegal report it and log that you have received it.

Sexting and the law

1. You could end up with a police caution

Sending a naked image of yourself via text message, or social media, when you're below the age of 18 is technically illegal. It counts as an offence of distributing an indecent image of a child. You could even end up on the sex offenders register.

"The law doesn't distinguish between an indecent image of you and an indecent image of someone else."

2. It's worse to send a photo of a sexual act

Even though the age of sexual consent is 16, the age for distributing indecent images is 18. That means that a 17-year-old who can legally have sex cannot legally send a naked image.
It's just as bad for a 15-year-old as a 17-year-old to sext.

But, what's worse for a 15-year-old is to send a photo showing them having sex. It's illegal for anyone below the age of 16 to have sex, so if the photo shows this, it could lead to them having doubly bad consequences.

If a 17-year-old sent a sext showing them having sex, they'd still be committing an offence by sending a naked image - but it wouldn't break the law around consent. A 15-year-old doing the same would be committing two offences.

3. An unwanted sext could be seen as a crime

But if you do send a naked selfie to someone who is likely to be upset by it, that could be a crime under the Malicious Communications Act.

Sexting and the law

4. Forwarding them on breaches civil law

"When you create a photo, as the creator you automatically become the owner of the copyright. Anyone who's taking a risqué picture and sending it to their partner, they'll own the copyright."

If the receiver of the image then circulates it, or posts it on a website, they're then infringing that copyright.

5. You could become a victim of revenge porn

One serious risk of sending explicit pictures is that someone could pass them on – either by circulating them or posting them onto a website. Once the pictures are there, it's hard to get them taken down.

You could approach websites with claims of breaching harassment laws and copyright laws, but it's often too late.

However someone who posts photos of an ex, perhaps, in a moment of anger, could be prosecuted for this.

6. You could break privacy law

Another issue with forwarding on images –

"*We'd argue that communication was being made in the private constraints and any wider dissemination of that content would be breach of privacy.*"

So...can you sext safely?

If you're under 18, it is an offence to take and/or send a naked picture of yourself. It's not illegal to be naked with someone, even if you're 15, but you can't send that picture.

As strange as it seems, it's the law and it's best to know the risks now.

Source:
www.telegraph.co.uk/women/womens-health/10985660/Sexting-scare-6-sexting-myths-busted.html

The law with regard to illegal activity

Computer Misuse Act 1990

This Act makes it an offence to:

- Erase or amend data or programs without authority.
- Obtain unauthorised access to a computer.
- "Eavesdrop" on a computer.
- Make unauthorised use of computer time or facilities.
- Maliciously corrupt or erase data or programs.
- Deny access to authorised users.

Data Protection Act 1998

This protects the rights and privacy of individual's data. To comply with the law, information about individuals must be collected and used fairly, stored safely and securely and not disclosed to any third party unlawfully.

The Act states that personal data must be:

- Fairly and lawfully processed.
- Processed for limited purposes.
- Adequate, relevant and not excessive.
- Accurate.
- Not kept longer than necessary.
- Processed in accordance with the data subject's rights.
- Secure.
- Not transferred to other countries without adequate protection.

Freedom of Information Act 2000

The Freedom of Information Act gives individuals the right to request information held by public authorities. All public authorities and companies wholly owned by public authorities have obligations under the Freedom of Information Act. When responding to requests, they have to follow a number of set procedures.

The law with regard to illegal activity

Communications Act 2003

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.

Malicious Communications Act 1988

It is an offence to send an indecent, offensive, or threatening letter, electronic communication or other article to another person.

Regulation of Investigatory Powers Act 2000

It is an offence for any person to intentionally and without lawful authority intercept any communication. Monitoring or keeping a record of any form of electronic communications is permitted, in order to:

- Establish the facts;
- Ascertain compliance with regulatory or self-regulatory practices or procedures;
- Demonstrate standards, which are or ought to be achieved by persons using the system;
- Investigate or detect unauthorised use of the communications system;
- Prevent or detect crime or in the interests of national security;
- Ensure the effective operation of the system.
- Monitoring but not recording is also permissible in order to:
- Ascertain whether the communication is business or personal;
- Protect or support help line staff.
- The school reserves the right to monitor its systems and communications in line with its rights under this act.

Trade Marks Act 1994

This provides protection for Registered Trade Marks, which can be any symbol (words, shapes or images) that are associated with a particular set of goods or services. Registered Trade Marks must not be used without permission. This can also arise from using a Mark that is confusingly similar to an existing Mark.

The law with regard to illegal activity

Copyright, Designs and Patents Act 1988

It is an offence to copy all, or a substantial part of a copyright work. There are, however, certain limited user permissions, such as fair dealing, which means under certain circumstances permission is not needed to copy small amounts for non-commercial research or private study. The Act also provides for Moral Rights, whereby authors can sue if their name is not included in a work they wrote, or if the work has been amended in such a way as to impugn their reputation. Copyright covers materials in print and electronic form, and includes words, images, and sounds, moving images, TV broadcasts and other media (e.g. youtube).

Telecommunications Act 1984

It is an offence to send a message or other matter that is grossly offensive or of an indecent, obscene or menacing character. It is also an offence to send a message that is intended to cause annoyance, inconvenience or needless anxiety to another that the sender knows to be false.

Criminal Justice & Public Order Act 1994

This defines a criminal offence of intentional harassment, which covers all forms of harassment, including sexual. A person is guilty of an offence if, with intent to cause a person harassment, alarm or distress, they:

- Use threatening, abusive or insulting words or behaviour, or disorderly behaviour; or
- Display any writing, sign or other visible representation, which is threatening, abusive or insulting, thereby causing that or another person harassment, alarm or distress.

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.

The law with regard to illegal activity

Protection from Harrassment 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.

Protection of Children Act 1978

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). A person convicted of such an offence may face up to 10 years in prison

Sexual Offences Act 2003

The new grooming offence 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 fall in this category of trust). Any sexual intercourse with a child under the age of 13 commits the offence of rape.

Public Order Act 1986

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. Children, Families and Education Directorate page 38 April 2007.

The law with regard to illegal activity

Obscene Publications Act 1959 and 1964

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

Human Rights Act 1998

This does not deal with any particular issue specifically or any discrete subject area within the law. It is a type of "higher law", affecting all other laws. In the school context, human rights to be aware of include:

- The right to a fair trial
- The right to respect for private and family life, home and correspondence
- Freedom of thought, conscience and religion
- Freedom of expression
- Freedom of assembly
- Prohibition of discrimination
- The right to education

These rights are not absolute. The school is obliged to respect these rights and freedoms, balancing them against those rights, duties and obligations, which arise from other relevant legislation.

The Education and Inspections Act 2006

Empowers Headteachers, to such extent as is reasonable, to regulate the behaviour of students / pupils when they are off the school site and empowers members of staff to impose disciplinary penalties for inappropriate behaviour.

The Education and Inspections Act 2011

Extended the powers included in the 2006 Act and gave permission for Headteachers (and nominated staff) to search for electronic devices. It also provides powers to search for data on those devices and to delete data.

(see template policy in these appendices and for DfE guidance - www.education.gov.uk/schools/pupilsupport/behaviour/behaviourpolicies/f0076897/screening-searching-and-confiscation)

The law with regard to illegal activity

The Protection of Freedoms Act 2012

Requires schools to seek permission from a parent / carer to use Biometric systems.

The School Information Regulations 2012

Requires schools to publish certain information on its website:
www.education.gov.uk/schools/toolsandinitiatives/cuttingburdens/b0075738/reducing-bureaucracy/requirements/changestoschoolinformationregulations

Dealing with a device where there is suspicion of illegal content

It is advised that if there is suspicion of something illegal on a school device (and this would now also relate to a device brought in by a student), then the device is to be powered off at the plug (not Shut Down), locked away in a secure cabinet and nobody allowed to access that cabinet until the police have arrived and determined, upon investigation, whether the device warrants seizure or not.

As many devices such as phones, tablets and laptops have their own power supply via a battery, the advice to power off via the mains supply is not relevant. In such cases the device can be turned off and secured immediately in a safe location to ensure no one has further access to it prior to investigation.

It is also good practice that when the member of staff seizes the device they record the date and time.

We can see in the following materials by SWGFL that the decision to search a student or adult's device must be made with care. There is a balance between infringing people's rights and protecting the individual. With this in mind it would be prudent to ensure that responsible individuals (Senior leaders and those with responsibility for safeguarding and esafety) follow an agreed and documented procedure to search a device. The act of searching a personal device may be seen as sensitive as a physical search of the child or adult involved.

Extract from SWGfL School E-Safety Policy Template Document

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 / academy's Headteacher / Principal and Governors / Directors 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.

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 Headteacher / Principal.
Schools will need to choose which terms to use and delete the others accordingly.

Dealing with a device where there is suspicion of illegal content

Extract from SWGfL School E-Safety Policy Template Document

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 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 behaviour 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"
`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.

Dealing with a device where there is suspicion of illegal content

Extract from SWGfL School E-Safety Policy Template 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.

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.

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

Dealing with a device where there is suspicion of illegal content

Extract from SWGfL School E-Safety Policy Template Document

Policy Statements relating to searching devices

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 should take reasonable steps to check the ownership of the mobile phone / personal electronic device before carrying out a search. (The powers included in the Education Act do not extend to devices owned (or mislaid) by other parties eg

Dealing with a device where there is suspicion of illegal content

Extract from SWGfL School E-Safety Policy Template Document

a visiting parent or contractor, only to devices in the possession of pupils / students.)

The authorised member of staff should take care that, where possible, searches should not take place in public places e.g. an occupied classroom, which might be considered as exploiting the student / pupil being searched.

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. (schools will need to take account of their normal policies regarding religious garments / headwear and may wish to refer to it in this policy)

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.

Further information relating to searching students can be found in this Department of Education document (published Feb 14)
`www.gov.uk/government/publications/searching-screening-and-confiscation`

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.

Dealing with a device where there is suspicion of illegal content

Extract from SWGfL School E-Safety Policy Template Document

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 who 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 in the main School Template Policies document. 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).

A record should be kept of the reasons for the deletion of data / files. (DfE guidance states and other legal advice recommends 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).

CARE OF CONFISCATED DEVICES

School staff are reminded of the need to ensure the safe keeping of confiscated devices, to avoid the risk of compensation claims for damage / loss of such devices (particularly given the possible high value of some of these devices).

The school may wish to add a disclaimer to the relevant section of the Behaviour Policy which may assist in covering the school against damage / loss claims.

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. (a template log sheet can be found in the

Dealing with a device where there is suspicion of illegal content

Extract from SWGfL School E-Safety Policy Template Document

appendices to the School E-Safety Template Policies)

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 (including on its website) – the Behaviour Policy should be cross referenced with this policy on search and deletion.

E safety Log

Schools must have rigorous and meaningful reporting procedures in place and this includes an esafety log. The purpose of the log is to record all illegal/inappropriate/accidental/deliberate incidents. The log ensures that appropriate action is taken and child safeguarding is the priority. Over time the log will also act to inform policy and practice reviews by highlighting the types and frequency of incidents. Training and teaching can then be set in place to help minimise the likelihood of similar incidents in future.

Further to completing the incident log, all adults involved in the reporting process should email a brief summary of the incident to the headteacher. This means that they have a time/date stamped record of when they notified their headteacher, and leaves a clear audit trail for future reference if required.

E safety Log

Example esafety incident log

[school name] - **Esafety Incident Log**

Details of ALL esafety incidents to be recorded by the esafety Coordinator. This incident log will be monitored termly by the Headteacher, Member of SLT or Chair of Governors.

Date & Time	Name of pupil or staff member	Room and computer / device number	Details of incident (including evidence)	Actions	Name and role of person completing this entry

Record of reviewing devices / internet sites (responding to incidents of misuse)

Group	
Date	
Reason for investigation	

Details of first reviewing person

Name	
Position	
Signature	

Details of second reviewing person

Name	
Position	
Signature	

Name and location of computer used for review (for web sites)

Web site(s) address / device	**Reason for concern**

Conclusion	**Action proposed or taken**

Managing incidents

Thanks to Hertfordshire County Council and Southwest Grid
For Learning for their assistance and resources

For Headteachers, Senior Leaders and Governors

Involving staff as victims

All incidents should be reported to the Headteacher and/or Governors who will:

- Record in the school esafety Incident Log
- Keep any evidence – printouts and/ screen shots
- Use the 'Report Abuse' button, if appropriate
- Consider involving the Chair of Governors and /or reporting the incident to the Governing Body

Parents/carers as instigators

Contact the person and invite into school and discuss using some of the examples below:

- You have become aware of discussions taking place online …
- You want to discuss this..
- You have an open door policy so disappointed they did not approach you first

- They have signed the Home School Agreement which clearly states …
- Request the offending material be removed

If this does not solve the problem:

- Consider involving the Chair of Governors
- Consider involving the police (Communications Act 2003 & Malicious Communications Act 1988)

Staff/colleagues as instigators

Contact Schools HR for initial Advice and/ or contact Schools esafety Adviser In all serious cases this is the first step.

- Contact the member of staff and request the offending material be removed immediately, (in serious cases you may be advised not to discuss the incident with the staff member)
- Refer to the signed ICT Acceptable Use Agreement, Professional Code of Conduct and consider if this incident has an impact on the Contract of Employment of the member of staff.
- Provide additional training
- Invoke disciplinary procedures

Pupils as instigators

Follow some of the steps below:

- Identify the pupils involved
- Ask pupil to remove offensive material. Refer to the signed Acceptable Use Agreement.
- If the perpetrator refuses to remove the material and is under 13 contact the Social Network who will close the account

Managing incidents

- Take appropriate actions inline with school policies/ rules
- Inform parents/ carers if serious or persistent incident
- For serious incidents or further advice:
- Inform your Local Police Safer Neighbourhood team
- Local authority support services re bullying
- If the child is at risk inform your school Child Protection Officer

Further Support

- School HR contact [insert details]
- Governor Services [insert details]
- Teachers' union [insert details]
- Police [insert details]
- Local Authority HR, Legal, School Improvement Service [insert details]

- **Where a child is believed to be at risk, contact Child Protection officer/ team. [insert details]**

Illegal Esafety Incident

For Headteachers, Senior Leaders and Governors

Examples of illegal activity/content

- Downloading child abuse images/files
- Sharing images or video containing child abuse
- Inciting racial or religious hatred
- Extreme cases of Cyberbullying
- Promoting illegal acts

If illegal material or activity found or suspected:

- Isolate device securely. (do not view or share content)
- Inform esafety officer, SLT, Police, Chair of governors, LA School Improvement Leader (insert contact details)
- If a student is involved notify Child Protection Officer
- If a member of staff is involved contact LA Designated Officer for allegations against staff.

Non illegal Esafety Incident

For Headteachers, Senior Leaders and Governors

Involving staff as victims

Incident could be:

- Using another person's password, online identity or log on details.
- Accessing websites which are against school policy e.g. games, social networks.
- Using a mobile phone to take video during a lesson.
- Using the technology or social media to upset or bully or bring the individual, profession or organisation into disrepute.

If member of staff has:

- Behaved in a way that has harmed a child, or may have harmed a child.
- Possibly committed a criminal offence against or related to a child; or
- Behaved towards a child or children in a way that indicates he or she would pose a risk of harm if they work regularly or closely with children.
- Contact the LADO on: [insert number]
- Review evidence and determine if the incident is accidental or deliberate
- Decide upon the appropriate course of action
- Follow school disciplinary procedures

Non illegal Esafety Incident

Pupils as instigators

- Review incident and identify if other pupils were involved
- Decide appropriate sanctions and/ or support based on school rules/ guidelines Inform parents/ carers if serious or persistent incident. In serious incidents consider informing the Child Protection Officer as the child instigator could be at risk
- Review school procedures/policies to develop best practice

Pupils as victims

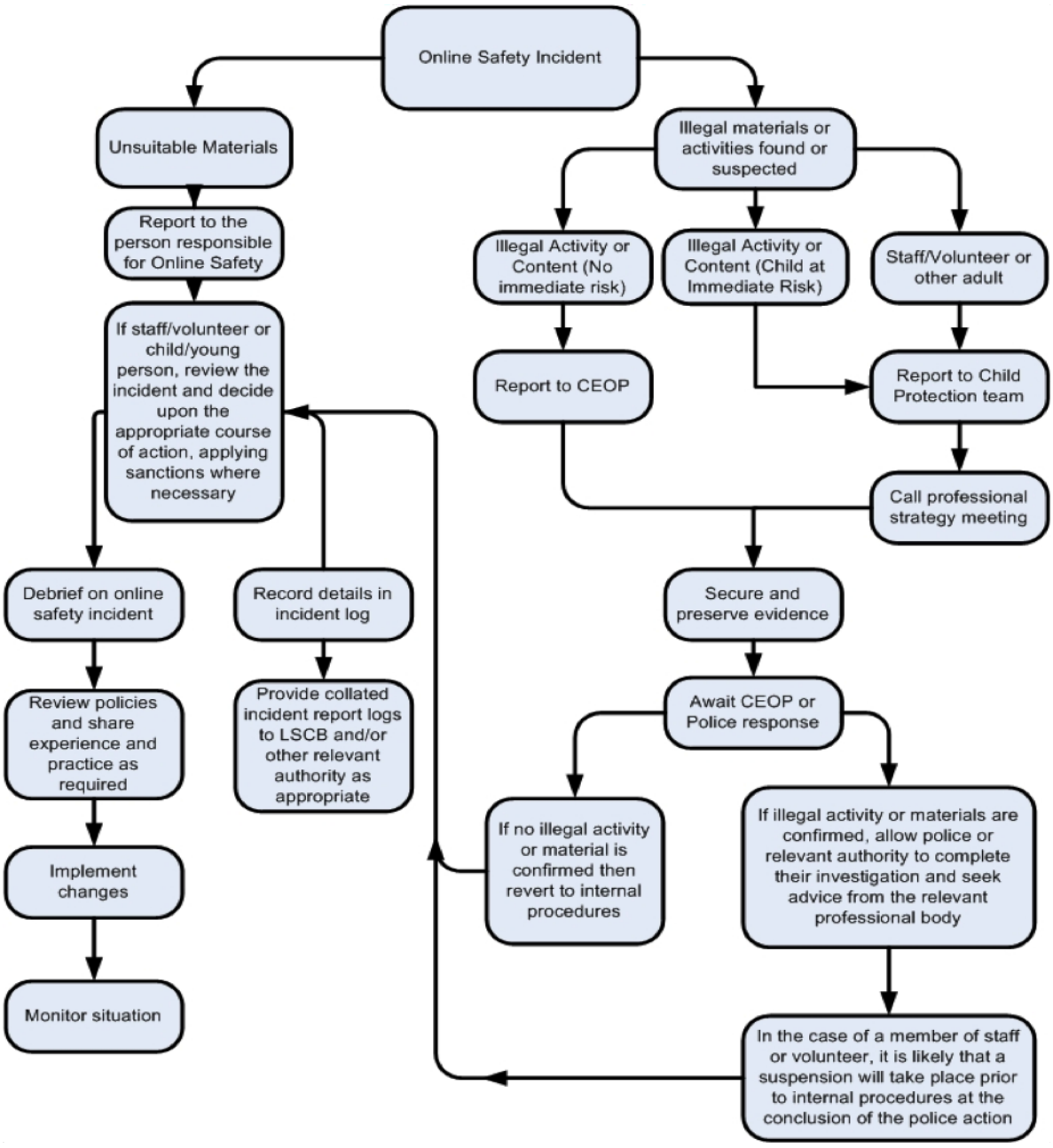
In –school action to support pupil by one or more of the following:

- Class teacher
- Esafety Coordinator
- Senior Leader or Headteacher
- Designated Senior Person for Child Protection (DSP)
- School Police Community Support Officer

Then do the following:

- Inform parents/ carer as appropriate.
- If the child is at risk inform CSPLO immediately.
- Confiscate the device, if appropriate.

SWFgL Esafety School Template Policies



Useful Links

Digitally Confident
www.digitallyconfident.org

South West Grid for Learning
www.swgfl.org.uk/Staying-safe

Childnet
www.childnet.com

Thinkyouknow
www.thinkyouknow.co.uk

Internet Watch Foundation
www.iwf.org.uk

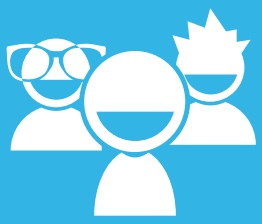
CEOP
http://ceop.police.uk

Beat Bullying
www.beatbullying.org/gb/who-is-on-this-site

Reporting links for popular online services
http://cyberbullying.us/report

Guidelines on prosecuting cases involving communications sent via social media
www.cps.gov.uk/legal/a_to_c/communications_sent_via_social_media

Dealing with indecent images of children in the workplace: A Best Practice Guide
www.iwf.org.uk/resources/best-practice-guide



DIGITALLY
CONFIDENT

First Line Information Support for Esafety Incidents

MADE BY PHILIP & SIMON AT

www.digitallyconfident.org