

## E-Safety - Online Safety Policy

Believing in Excellence means that the school has key values that all members of our school community live by. These are:

- Respect;
- Resilience;
- Responsibility.

These values apply to three important spheres of life:

- Believing in Excellence for ourselves;
- Believing in Excellence for others;
- Believing in Excellence for our environment.

Date of Policy	October 2016
Date agreed by Governing Body	November 2016
Date of next review	October 2017
Lead Member of Staff	Ian Swingler, Head of Secondary Phase

# Summary Statement

The requirement to ensure that children and young people are able to use the Internet and related communications technologies appropriately and safely is addressed as part of the wider duty of care to which all who work with children and young people are bound.

Digital technologies have become integral to the lives of children and young people in today's society. The Internet and other digital and information technologies are powerful tools, which open up new opportunities for everyone. It should be noted, however, that alongside this there is a growing expression of opinion that unlimited use of mobile devices is not necessarily healthy for under 16 year olds and so safe use needs to be integral to safe learning.

It is our vision that every pupil has an entitlement to online learning and the use of appropriate learning technologies. Pupils must have access to quality online learning opportunities in a variety of forms which meet their individual needs. In achieving this vision children / young people, staff and volunteers also have a right to safer internet access at all times.

However, the use of these new and rapidly developing technologies can put users at risk. Some of the dangers may include:

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

Many of these risks reflect situations in the offline world and it is essential that this online safety policy is used in conjunction with other policies (eg safeguarding / child protection policies).

As with all other risks, it may not be possible to eliminate all risks but it is our intention to mitigate them to a safe level. By providing good examples / role models and by raising awareness, it is possible to build the resilience of children and young people, so that they have the confidence and skills to deal with these risks.

All groups within the school should be able to demonstrate that they have provided the necessary safeguards to help ensure that they have done everything that could reasonably be expected to manage and reduce these risks. The online safety policy that follows explains how we intend to do this.

Within this document can be found policies and procedures which address a variety of issues related to ensuring that students and adults remain safe on-line. These include statements:

- Roles and Responsibilities
- E-safety training for students, parents and staff
- Guidance for staff on their professional conduct in their online profiles
- Acceptable use of online communication tools
- The use of digital and video images
- Data security
- Unsuitable/ inappropriate activities with sanctions related to each
- Guidance for dealing with e-safety issues

These are supported by policies on:

- Acceptable Use for Students
- Acceptable Use Agreement for Staff and Volunteers
- Use of Digital/ Video Images Consent form
- Personal Data
- Guidance for Reviewing Internet Sites (for suspected harassment and distress)
- Password Security

# Development / Monitoring / Review of this Policy

This online safety policy was approved by (if relevant)	<i>Governors</i>
On	
The implementation of this online safety policy will be monitored by the:	<ul style="list-style-type: none"><li>• <i>SLT</i></li><li>• <i>Safeguarding / Child Protection Designated Person</i></li><li>• <i>Governors</i></li></ul>
Monitoring will take place at regular intervals:	<i>Annually</i>
Monitoring reports will be presented to:	<i>Governors</i>
The Online Safety Policy will be reviewed annually, or more regularly in the light of any significant new development. The next anticipated review date will be:	<i>Annually</i>
<b>Should serious online incidents take place, the following external persons / agencies should be informed:</b>	<p><i>Insert titles of relevant persons / agencies eg:</i></p> <ul style="list-style-type: none"><li>• <b>Local Authority Child Protection Lead Person or Area Social Work team</b> <i>(as relevant locally)</i></li><li>• <b>Local Authority Designated Officer (LADO)</b> <i>(if it involves an allegation against member of staff / volunteer)</i></li><li>• <b>Police</b></li></ul>

# Scope of the Policy

This policy applies to all members of Cavendish School (including staff, volunteers, children and young people, parents / carers, visitors, community users) who have access to and are users of communications technologies (whether these belong to the group or to the users themselves) within the school or using school technology beyond the school.

## General Policy Statement

The Headteacher and governors of The Cavendish School believe that the online safety of persons within the school is of paramount importance. The first requirement for maintaining high standards of safety is that everyone is vigilant and undertakes personal responsibility for their own safety and of others. Safe and acceptable use refers to both school and personal equipment when at school or when accessing school related software. In the special circumstances of a school it is also important that adults recognise their additional responsibility for modelling safe practice for young people.

We believe that health and safety standards will be maintained only with the cooperation of all staff, pupils and visitors to the school. We require all staff to comply fully with this policy. In addition we will ensure that all pupils, visitors and contractors are provided with the information they require to enable them to comply with this policy. It is the intention of the Head teacher and governors that procedures to ensure relevant health and safety issues are embedded within the curriculum at all levels where appropriate.

The effectiveness of the policy will be regularly monitored to ensure that health and safety arrangements are being implemented and that the people named in the policy are carrying out their duties. It is therefore important that all involved in delivering this policy maintain access to readily available evidence which supports good practice and so instils confidence in that practice.

The policy will be reviewed annually and revised where necessary.

# Roles and Responsibilities

## **The Governing Body will:**

- review approve the policy in line with the review cycle
- monitor the implementation of the policy
- regularly review safety procedures through governor moderation of evaluations report by SLT

## **The Senior Leadership Team will:**

- ensure the policy is regularly monitored and report to the governing body on its implementation and regular updating of procedures
- designate from within SLT an Online Safety leader with the roles set out below
- ensure that all members of the school have appropriate e-safety training

## **The Safeguarding Leader will:**

- have overall responsibility for ensuring the safety (including online safety) of all staff, volunteers and members of the school, though the day to day responsibility for online safety may be delegated to others - ICT Technical Manager and e-Safety officer.
- be aware of the procedures to be followed in the event of a serious online safety allegation being made against a member of staff or volunteer. (see flowchart on dealing with online safety incidents)
- ensuring that the Online Safety Lead and other relevant staff / volunteers receive suitable training to enable them to carry out their online safety roles and to train other colleagues, as relevant
- The Safeguarding Leader will ensure that there is a system in place to allow for the monitoring of online safety in the group and that they receive regular monitoring reports

## **The e-Safety Officer will:**

- ensure that staff / volunteers have an up to date awareness of the school's current online safety policy and practices
- ensure that all staff / volunteers are aware of the procedures that need to be followed in the event of an online safety incident taking place.
- take day to day responsibility for online safety issues and has a leading role in establishing and reviewing the online safety policies / documents
- offer advice and support for all users
- keep up to date with developments in online safety
- understand and know where to obtain additional support and where to report issues
- ensure provision of training and advice for staff and volunteers
- liaises with the national / local organisation / association as relevant
- receives reports of online safety incidents and creates a log of incidents to inform future online safety developments
- monitors incident logs
- reports regularly to the Safeguarding Leader

The e-Safety Officer will be trained in up to date online safety issues and be aware of the potential for serious child protection issues. (Nb. it is important to emphasise that these are child protection issues, not technical issues; simply that the technology provides additional means for child protection issues to develop).

**The ICT Technical Manager will:**

- create systems that enable the school to monitor online safety related to school equipment and its online presence
- monitor the appropriate use of ICT resources by students on a daily basis
- report issues to the e-Safety Officer
- support the e-Safety Officer in providing training for all staff

**The Curriculum Leader for ICT will:**

- support e-safety policies by ensuring that e-safety is taught effectively within the curriculum for all year groups
- Support the e-Safety Officer in developing educational materials for students which can be delivered outside of the curriculum

**All staff will:**

- have an up to date awareness of the school's current online safety policy and practices
- have read, understood and signed the Staff / Volunteer Acceptable Use Policy (AUP)
- report any suspected misuse or problem to the relevant person (e-Safety Officer) – particularly where it is believed that a child's welfare is at risk
- use digital communications with children and young people on a professional level and where possible only carried out using the official systems of the group.
- ensure young people in their care are aware of online safety
- be aware of online safety issues particularly those related to the use of mobile phones, cameras, gaming consoles and handheld devices and that they monitor their use and implement the group policies with regard to these devices
- undertake and evaluate regular training

**Parents/ carers will:**

- ensure that their children understand the need to use the internet / mobile devices in an appropriate way
- endorse (by signature) the Acceptable Use Policy for Young People which is included as part of the home school agreement
- sign the relevant permission forms on the taking and use of digital and video images

**Students will:**

- abide by the Acceptable Use Policy / Rules, which they may be expected to sign before being given access to the organisation's systems and devices
- understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so
- should demonstrate positive online behaviour

# Policy Statements

## Educating children and young people to stay safe online

Whilst regulation and technical solutions are very important, their use should be balanced by making children and young people aware of the need to take a responsible approach to online safety. Children and young people need help and support to recognise and avoid online safety risks and build their resilience. Online safety awareness will be provided in the following ways:

- key online safety messages should be reinforced as part of all relevant planned programmes of study for students particularly through the ICT curriculum
- online safety issues should be discussed / highlighted, when possible, in informal conversations with young people
- when the opportunity arises young people should be advised to be critically aware of the materials/ content they access on-line and be guided to validate the accuracy of information
- young people should be made aware of the need to respect copyright when using material accessed on the internet and, if applicable, acknowledge the source of information used
- rules for the use of devices / internet will be posted in areas where these devices are in use and, where possible, displayed on logon screens
- staff and volunteers should act as good role models in their use of online technologies

## Awareness raising for parents / carers

The school will provide online safety information to parents and carers through:

- Letters, newsletters, web site
- Meetings with parents / carers (formal and informal)
- Sharing the group's policies with parents and carers
- Engaging parents in the signing of acceptable usage policies

## Training – staff and volunteers

It is essential that all staff and volunteers receive online safety awareness training and understand their responsibilities, as outlined in this policy. Training will be offered as follows:

- a planned programme of training about online safety is available to, and required of all staff and volunteers
- all new staff and volunteers will receive awareness training as part of their induction programme, ensuring that they fully understand the online safety policy and acceptable use policies
- an audit of the online safety training needs of all staff will be carried out regularly
- retain details of their training needs and outcomes of associated training as part of their individual professional development portfolios
- the e-Safety Officer person will provide advice / guidance / training to individuals as required
- this online safety policy and its updates will be presented to and discussed by staff and volunteers at staff / team meetings

# Protecting the professional identity of staff and volunteers

This information applies to any adult, but particularly those working with children and young people (paid or unpaid) within the school. Consideration should be given to how your online behaviour may affect your own safety and reputation and that of the school.

Communication between adults and between children/ young people and adults, by whatever method, should take place within clear and explicit boundaries. This includes the wider use of technology such as mobile phones, text messaging, social networks, emails, digital cameras, videos, webcams, websites and blogs.

## When using digital communications, staff and volunteers should:

- only make contact with students for professional reasons and in accordance with the policies and professional guidance of the school
- not share any personal information with a student eg should not give their personal contact details to children and young people including e-mail, home or mobile telephone numbers
- not request, or respond to, any personal information from the child/young person, other than that which might be appropriate as part of their professional role, or if the child is at immediate risk of harm
- be aware of and use the appropriate reporting routes available to them if they suspect any of their personal details have been compromised
- ensure that all communications are transparent and open to scrutiny
- be careful in their communications with children so as to avoid any possible misinterpretation
- ensure that if they have a personal social networking profile, details are not shared with children and young people in their care (making every effort to keep personal and professional online lives separate)
- not add students as “friends” on any social network
- not post information online that could bring the school into disrepute
- be aware of the sanctions that may be applied for breaches of policy related to professional conduct
- e-mail, text or other web based communications between staff / volunteers and a child / young person should (wherever possible) take place using the school’s official equipment / systems
- any communications outside the agreed protocols (above) may lead to disciplinary and/or criminal investigations

## Wider personal use of digital communications:

While the section above refers to communications between staff / volunteers and young people consideration is also given to how the use of digital communications by staff and volunteers in their private lives could have an impact on the reputation of themselves and the school. Everyone should be able to enjoy the benefits of digital technologies. Staff and volunteers should, wherever possible, seek to separate their professional online presence from their online social life and take the following into account when using these digital communications:

- careful consideration should be given as to who should be included as “friends” on social networking profiles and which information / photos are available to those friends
- privacy settings should be frequently reviewed
- the amount of personal information visible to those on “friends” lists should be carefully managed and users should be aware that “friends” may still reveal or share this information
- be aware that people on your “friends” list may themselves be “friends” with students at the school
- “Digital footprint” – information, including images, posted on the web may remain there for ever. Many people subsequently regret posting information that has become embarrassing or harmful to them
- as an employer the school engages in searches of the internet when selecting candidates and is influenced by the content, both current and historic, we may find.

## Your technology

The school will be responsible for ensuring that all systems and devices will be as safe and secure as is reasonably possible and that policies and procedures approved within this policy are implemented. Systems and devices will be managed in ways that ensure that the school meets accepted online safety requirements, as below:

- each user must report immediately any concern, about e-safety or unacceptable use, experienced as part of their normal use of the school's facilities
- Web filtering software will be used to record the browsing history of each student to identify issues
- systems and devices will be regularly monitored and users are made aware of this in the Acceptable Use Policy
- personal data must not be sent over the internet or taken away from the school's offices / facilities unless safely encrypted or otherwise secured
- the systems and devices needing protection will be identified. These could be: computers; any device with Internet access; networks (hard wired or wireless); TV / media services
- devices in use are protected against online security threats, such as: viruses; unauthorised access; spyware and malware
- passwords will be provided, where required, for those who need access to these systems / devices and access will be restricted for those who do not. Users will be made responsible for the security of their username and password, must not allow other users to access the systems using their logon details and must immediately report any suspicion or evidence that there has been a breach of security
- where relevant, parental controls or PINs will be enabled on devices
- an effective filtering system will be used. The filtering will reflect the age, ability and responsibility of the users. There will be regular discussion with all users about filtering to promote wider ownership
- requests from staff and volunteers for sites to be removed from the filtered list will be considered by the ICT Technical Manager
- changes to systems and devices can only be made by those who have permission to do so eg installing software or changing security systems

## Personal Devices

- an agreed policy is in place regarding the use of devices belonging to others
- some areas are signposted as "No Mobile" areas (eg toilets or changing rooms) while others are areas where people know they can use their mobiles freely and safely.
- an agreed policy is in place regarding the use of removable media (eg memory sticks / CDs / DVDs) by users school data should not be held on unencrypted memory sticks

# How you use technology to communicate

The following table shows how this school currently considers the benefit of using these technologies outweighs their risks / disadvantages:

Communication Technologies	Staff & volunteers				Young people			
	Allowed	Allowed at certain times	Allowed for selected staff / volunteers	Not allowed	Allowed	Allowed at certain times	Allowed with staff / volunteers permission	Not allowed
Mobile phones		X				X		
Taking photos on mobile phones or other camera devices			X				X	
Use of handheld devices eg gaming consoles		X				X		
Use of the organisation's email for personal emails		X				X		
Use of online communication technologies eg social networking, chat rooms, instant messaging, email				X				X

## When using communication technologies the school considers the following as good practice:

- the school's official email service may be regarded as safe and secure and is monitored. Staff and volunteers should therefore use only the school's email service, where available, to communicate with others when that communication is related to the school
- users must immediately report, to a nominated person (e-Safety Officer) – in accordance with the school's policy, the receipt of any communication that makes them feel uncomfortable, is offensive, threatening or bullying in nature and must not respond to any such communication
- any communication between staff / volunteers and the children / young people or their parents / carers must be professional in tone and content. These communications should, where possible, only take place on official (monitored) systems.
- young people should be taught about online safety issues, such as the risks attached to the use of personal details. They should also be informed of strategies to deal with inappropriate communications
- Personal information should not be posted on the school website and, where possible, only official email addresses should be used to identify members of staff.

# Use of digital and video images

The development of digital imaging technologies has created significant benefits, allowing users instant use of images that they have recorded themselves or downloaded from the internet. However, staff and students need to be aware of the risks associated with sharing images and with posting digital images on the internet. Those images may remain available on the internet forever and may cause harm or embarrassment to individuals in the short or longer term. There are many reported incidents of employers carrying out internet searches for information about potential and existing employees. The school will raise awareness about these risks and will implement policies to reduce the likelihood of the potential for harm:

- when using digital images, staff should raise awareness among students about the risks associated with the taking, use, sharing, publication and distribution of images. In particular they should recognise the risks attached to publishing their own images on the internet eg on social networking sites
- written permission from parents or carers will be obtained to allow images to be taken of their children and also allowing their use for legitimate activities or for publicity that reasonably celebrates success and promotes the work of the school
- parents / carers are allowed to take digital / video images of their children at school special events within the guidelines contained in the Parents / Carers Permission Form in the Supporting Policies
- staff and volunteers are allowed to take digital / video images, where appropriate, but must follow the school policies concerning the sharing, distribution and publication of those images. Those images should be taken, where possible, on the organisation's equipment, not the personal equipment of staff and volunteers
- care should be taken when taking digital / video images that young people are appropriately dressed and are not participating in activities that might bring the individuals or the school into disrepute
- if photos are taken, their storage and use must not cause risk or embarrassment.
- photographs published on the website, or elsewhere that include young people will be selected carefully and will comply with good practice guidance on the use of such images
- the full names of young people will not be used anywhere on a website, blog, or published article, particularly in association with photographs. Consideration should be given to media coverage and journalists should be made aware of this policy.

# Data Security

Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 1998 which states that personal data must be:

- Fairly and lawfully processed.
- Processed for limited purposes.
- Adequate, relevant and not excessive.
- Accurate.
- Kept no longer than is necessary.
- Processed in accordance with the data subject's rights.
- Secure.
- Only transferred to others with adequate protection.

## Staff and volunteers must ensure that they:

- At all times take care to ensure the safekeeping of personal data, minimising the risk of its loss or misuse.
- Use personal data only on secure password protected computers and other devices, ensuring that they are properly "logged-off" at the end of any session in which they are using personal data.
- Transfer personal data using encryption and secure password protected devices.
- When personal data is stored on any portable computer system, USB stick or any other removable media:
  - the data must be **encrypted and password** protected
  - the device should be password protected (many memory sticks / cards and other mobile devices cannot be password protected)
  - the device should offer approved virus and malware checking software
  - the data should be securely deleted from the device, once it has been transferred or its use is complete

# Unsuitable / inappropriate activities

The school believes that the activities referred to in the following section would be inappropriate in a context of working with young people. The school policy restricts certain internet usage as follows:

## User Actions

**Users shall not visit Internet sites, make, post, download, upload, data transfer, communicate or pass on, material, remarks, proposals or comments that contain or relate to:**

	Acceptable	Acceptable at certain times	Acceptable for nominated users	Unacceptable	Unacceptable and illegal
Child sexual abuse images –The making, production or distribution of indecent images of children. Contrary to The Protection of Children Act 1978					√
Grooming, incitement, arrangement or facilitation of sexual acts against children Contrary to the Sexual Offences Act 2003.					√
Possession of an extreme pornographic image (grossly offensive, disgusting or otherwise of an obscene character) Contrary to the Criminal Justice and Immigration Act 2008					√
Criminally racist material in UK – to stir up religious hatred (or hatred on the grounds of sexual orientation) - contrary to the Public Order Act 1986					√
Pornography				√	
Promotion of any kind of discrimination				√	
Threatening behaviour, including promotion of physical violence or mental harm				√	
Any other information which may be offensive to colleagues or breaches the integrity of the ethos of the school or brings the school into disrepute				√	
Use systems, applications, websites or other mechanisms that bypass the filtering or other safeguards that are in place				√	
Infringing copyright				√	
Revealing or publicising confidential information (eg financial / personal information, computer / network access codes and passwords)				√	
Creating or propagating computer viruses or other harmful files				√	
Unfair usage (downloading / uploading large files that hinders others in their use of the internet)				√	
On-line gaming (educational)		√			
On-line gaming (non educational)			√		
On-line gambling				√	
On-line shopping / commerce		√			

File sharing (eg Bit Torrent, Limewire)					√
Use of personal social networking sites(while "at work")				√	
Use of an official school social networking site			√		
Use of video broadcasting eg Youtube	√				

## Sanctions Chart

The school needs to have clear and manageable procedures when dealing with misuse. Whilst it is more likely that the school will need to deal with incidents that involve inappropriate rather than illegal misuse. It is important that any incidents are dealt with quickly and proportionately and are recorded and well communicated.

If staff / volunteers suspect that misuse might have taken place, but that the misuse is not illegal (as above) it is essential that correct procedures are used to investigate, preserve evidence and protect those carrying out the investigation. In such event the "Procedure for Reviewing Internet Sites for Suspected Harassment and Distress" should be followed. This guidance recommends that more than one member of staff / volunteer is involved in the investigation which should be carried out on a "clean" designated computer.

It is intended that incidents of misuse will be dealt with through any accepted disciplinary procedures as follows:

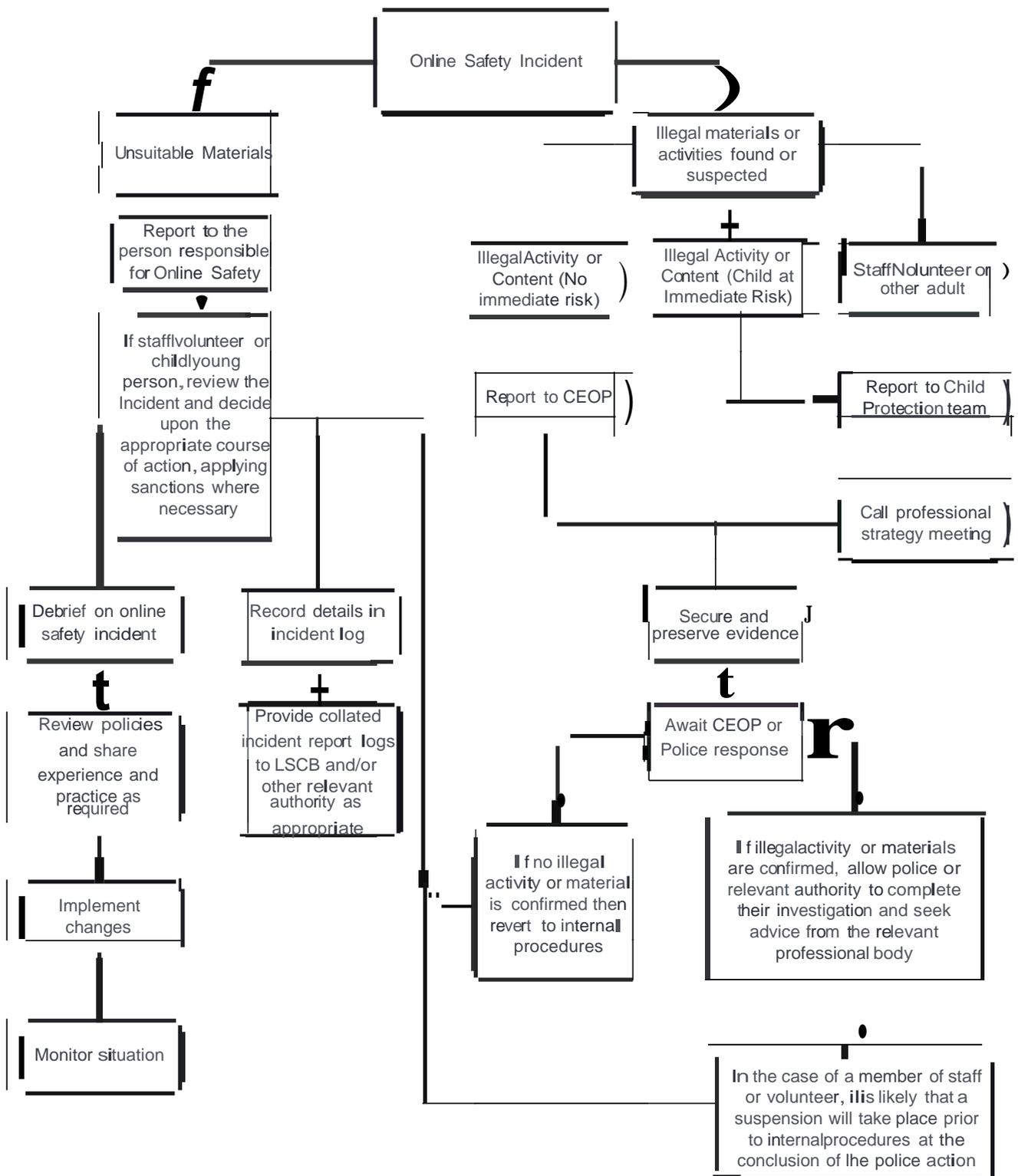
# Young People

Incidents:	Refer to e-Safety Officer	Refer to Police	Requires technical response / support	Inform parents / carers	Removal of access to technology / devices	Warning
Accessing or trying to access illegal material (see list in earlier section on unsuitable / inappropriate activities).	√	√		√		
Unauthorised downloading or uploading	√			√	√	
Allowing others to access technology / devices by sharing username and passwords						√
Attempting to access or accessing the technology / devices, using another person's account (hacking)	√			√	√	
Corrupting or destroying the data of other users	√			√	√	
Sending a communication that is regarded as offensive, harassment or of a bullying nature	√	√		√		
Actions which could bring the organisation into disrepute.	√					
Deliberately accessing materials that the school has agreed is inappropriate	√				√	
Activities that infringe copyright or data protection.	√	√				
<i>Using proxy by-pass sites or other means to subvert the filtering system</i>	√				√	
<i>Accidentally accessing materials that the school has agreed is inappropriate and failing to report it.</i>	√					√
<i>Unauthorised use of mobile phone / digital camera / other handheld device</i>						√
<i>Unauthorised use of social networking / instant messaging / personal email</i>					√	√

# Staff and volunteers

Incidents:	Refer to line manager / e-Safety Officer	Refer to National / Local Organisation / body	Refer to Police	Warning	Suspension	Disciplinary action
Accessing or trying to access illegal material (see list in earlier section on unsuitable / inappropriate activities).	√	√	√			
Excessive or inappropriate personal use of the internet / social networking sites / instant messaging / personal email "while at work"	√			√		
Unauthorised downloading or uploading of files	√			√		
Disclosing passwords or any information relating to the security of technology and devices.	√					√
Accidental infringement of the organisation's personal data policy	√			√		
Deliberate infringement of the organisation's personal data policy	√					√
Corrupting or destroying the data of other users	√					√
Deliberate damage to hardware or software	√					√
Sending a communication that is offensive, harassment or of a bullying nature	√		√			√
Using personal communication technologies eg email / social networking / instant messaging / text messaging to communicate with young people (except where allowed in the policy)	√	√				√
Actions which could compromise the professional integrity of staff / volunteers	√				√	
Bringing the organisation into disrepute	√				√	
Deliberately accessing materials that the school has agreed is inappropriate	√				√	√
Breaching copyright or licensing regulations	√	√				√
Using proxy bypass sites or other means to subvert the filtering system	√					√
Accidentally accessing materials that the school has agreed is inappropriate and failing to report it.	√				√	

# Flowchart for responding to online safety incidents



# Supporting Policies

## Management:

- 1 Acceptable use policy for students
- 2 Acceptable use policy for staff and volunteers (including professional identity)
- 3 Consent form for parents and carers (including use of images)
- 4 Personal data policy

## People:

- 1 Flowchart for responding to online safety incidents
- 2 Guidance for reviewing internet sites (for suspected harassment and distress)
- 3 Reporting log
- 4 Training needs audit

## Technology

- 1 Password security policy
- 2 Monitoring log

## At the end of this document you will find:

### Links to other organisations and documents

### Legislation

### Glossary

### Acknowledgements

# Policies - Acceptable Use Policy for Students

## Acceptable Use Policy Agreement

I understand that while I am a member of Cavendish School I must use technology in a responsible way.

### For my own personal safety:

- I understand that my use of technology will be supervised and monitored.
- I will keep my password safe and will not use anyone else's (even with their permission).
- I will keep my own personal information safe as well as that of others.
- I will tell a trusted adult if anything makes me feel uncomfortable or upset when I see it online.

### For the safety of others:

- I will not interfere with the way that others use their technology.
- I will be polite and responsible when I communicate with others.
- I will not take or share images of anyone without their permission.

### For the safety of the school:

- I will not try to access anything illegal.
- I will not download anything that I do not have the right to use.
- I will only use my personal device if I have permission and use it within the agreed rules.
- I will not deliberately bypass any systems designed to keep the school safer.
- I will tell a responsible person if I find any damage or faults with technology, however this may have happened.
- I will not attempt to install programmes of any type on the devices belonging to the school, without permission.
- I will not use social networking, gaming and chat sites without the express permission of a member of staff.

I understand that I am responsible for my actions and the consequences. I have read and understood the above and agree to follow these guidelines:

**Name**

**Signature**

**Date**

# Policy - Acceptable Use Agreement for Staff and Volunteers

## Background

Technology has transformed learning, entertainment and communication for individuals and for all organisations that work with young people. However, the use of technology can also bring risks. All users should have an entitlement to safe internet access at all times.

## This Acceptable Use Policy is intended to ensure that:

- Staff and volunteers will act responsibly to stay safer while online, being a good role model for younger users.
- Effective systems are in place for the online safety of all users and the security of devices, systems, images, personal devices and data.
- Staff and volunteers are aware of and can protect themselves from potential risk in their use of online technologies.

The term “professional” is used to describe the role of any member of staff, volunteer or responsible adult.

## For my professional and personal safety I understand that:

- I will ensure that my on-line activity does not compromise my professional responsibilities, nor bring my school into disrepute.
- My use of technology could be monitored.
- When communicating professionally I will use the technology provided by the school (eg email) and only use my school email address.
- These rules also apply when using the school’s technology either at home or away from the school.
- Personal use of the school’s technology is only acceptable within the guidelines laid out in this policy.

## For the safety and security of others:

- I will not access, copy, remove or otherwise alter any other user’s files, without authorisation.
- I will communicate with others in a professional manner.
- I will share other’s personal data only with their permission.
- I understand that any images I publish will be with the owner’s permission and follow the school’s code of practice.
- Wherever possible I will use the school’s equipment to record any digital and video images, unless I have permission to do otherwise.

## For the safety of the school, I understand that:

- I will not try to access anything illegal, harmful or inappropriate.
- It is my responsibility to immediately report any illegal, harmful or inappropriate incident.
- I will not share my online personal information (eg social networking profiles) with the children and young people in my care.
- I will not deliberately bypass any systems designed to keep the school safe.
- I will only transport, hold, disclose or share personal information about myself or others, as outlined in the Personal Data Policy. Where personal data is transferred, externally, it must be encrypted.
- I understand that data protection policy requires that any personal data to which I have access, will be kept private and confidential, except when it is deemed necessary that I am required by law or by the school’s policy to disclose such information to an appropriate authority.
- Personal passwords and those of other users should always be confidential.
- I will not download anything that I do not have the right to use.
- I will only use my personal device if I have permission and use it within the agreed rules
- I will inform the appropriate person if I find any damage or faults with technology.
- I will not attempt to install programmes of any type on the devices belonging to the school, without permission.

Staff / Volunteer Name

Signed

Date

# Consent Form for Parents and Carers

A copy of the Student Acceptable Use Policy is attached to this permission form, so that parents / carers will be aware of the organisation's / school's expectations of the young people in their care.

**Parent / Carers Name:**

**Name of Child / Young person:**

As the parent / carer, I give permission for my child to use the school's technology and devices.

I know that my child *has signed an Acceptable Use Agreement and* has received guidance to help them understand the importance of online safety.

I understand that the school will take reasonable precautions to ensure that my child will be safer when online, however, I understand that this manages risk but cannot eliminate it.

I understand that my child's online activity will be supervised and monitored and that the school will contact me if they have concerns about any possible breaches of the Acceptable Use Policy.

I understand that the school will take appropriate action in the event of any incidents.

I will encourage my child to adopt safe use of the internet and digital technologies and I will support the school in the implementation and development of its ICT policies.

**Signed**

**Date**

# Use of Digital / Video Images

The use of digital / video images plays an important part in our activities. Students, staff and volunteers may use digital cameras or other devices to record evidence of those activities. These images may then be used to present evidence of learning and may also be used to celebrate success through their publication in newsletters, on the website and occasionally in the public media.

The school will comply with the Data Protection Act and request parents / carers permission before taking images of their children. We will also ensure that, wherever possible, full names will not be published alongside images.

*It's a great thing to film your child at our events and we know they provide a lot of precious memories. You can support us in keeping our children safe by considering the following:*

- *Images and video should be for your own or family's personal use only*
- *Think about privacy and who has the right to see your images, not only of your own child but of others*
- *If you do share the images online, then you must make sure they are limited to immediate family only and not public*
- *If you need help in knowing how to do this then come and have a chat with us*

Parents / carers are requested to sign the permission form below to allow the school to take and use images of their children.

## Permission Form

**Parent / Carers Name**

**Name of Child / Young Person**

As the parent / carer of the above child, I agree to the school taking and using digital / video images of my child / children. I understand that the images will only be used to support legitimate activities or in publicity that reasonably celebrates success and promotes the work of the school.

I agree that if I take digital or video images at school events which include images of children, other than my own, I will abide by these guidelines in my use of the images.

**Signed**

**Date**

# Personal Data Policy

## Introduction

### Personal Data

The school and individuals within the organisation has access to a wide range of personal information and data, held in digital format or on paper records. Personal data is defined as any combination of data items that identifies an individual and provides specific information about them, their families or circumstances. This will include:

- Personal information about children / young people, members of staff / volunteers and parents and carers eg. names, addresses, contact details, legal guardianship / contact details, health records, disciplinary records
- Professional records eg. employment history, taxation and national insurance records, appraisal records and references
- Any other information that might be disclosed by parents / carers or by other agencies working with families

It is the responsibility of all staff and volunteers to take care when handling, using or transferring personal data that it cannot be accessed by anyone who does not have permission to access that data or does not need to have access to that data. Anyone who has access to personal data must know, understand and adhere to this policy.

The Data Protection Act (1998) lays down a set of rules for processing of personal data (both structured manual records and digital records). It provides individuals (data subjects) with rights of access and security and requires users of data (data processors) to be open about how it is used and to follow “good information handling principles”.

Guidance for organisations on the DPA is available on the Information Commissioners Office website:

<https://ico.org.uk/>

### Policy Statements

The school will hold the minimum personal information necessary to enable it to perform its function and information will be erased once the need to hold it has passed.

Every effort will be made to ensure that information is accurate, up to date and that inaccuracies are corrected without unnecessary delay.

### Responsibilities

The safeguarding officer will keep up to date with current legislation and guidance and will carry out risk assessments.

We aim to follow guidance from the Information Commissioner’s Office:

<http://www.nationalarchives.gov.uk/information-management/>

This outlines the responsibilities of other appointed staff such as Senior Information Risk Officers.

### Registration

Most schools holding personal data must register as a Data Controller on the Data Protection Register held by the Information Commissioner.

Staff and volunteers will receive data handling awareness / data protection training and will be made aware of their responsibilities, as described in this policy through: (groups should amend or add to as necessary)

- Induction training for new staff
- Meetings / briefings / training for staff / volunteers
- Day to day support and guidance from the Group Leader.

## **Risk Assessments**

*Information risk assessments will be carried out by staff / volunteers to establish key areas of the group where data might be at risk and how the risk could be reduced*

### **Storing personal data**

Personal data must be held securely on the group's premises and only accessed by those with permission to do so. Any personal data removed from the premises should have the appropriate level of protection to prevent loss of data.

The school has a clear policy and procedures for the automatic backing up, accessing and restoring all data held on systems, including off-site backups.

The school recognises that under Section 7 of the Data Protection Act, data subjects have a number of rights in connection with their personal data, the main one being the right of access. Procedures are in place to deal with Subject Access Requests ie. a written request to see all or a part of the personal data held.

### **Disposal of data**

The school will comply with the requirements for the safe destruction of personal data when it is no longer required. Such data must be destroyed, rather than deleted and be conducted in a way that makes reconstruction highly unlikely. Electronic files must be securely overwritten, and other (paper based) media must be shredded, incinerated or otherwise disintegrated.

# Guidance for Reviewing Internet Sites (for suspected harassment and distress)

This guidance is intended for use when schools need to manage incidents that involve the use of online services. It encourages a safe and secure approach to the management of the incident. Incidents might typically include cyber-bullying, harassment, anti-social behaviour and deception. These may appear in emails, texts, social networking sites, messaging sites, gaming sites or blogs etc.

**Do not follow this procedure if you suspect that the website(s) concerned may contain child abuse images. If this is the case please refer to the Flowchart for responding to online safety incidents and report immediately to the police.**

**Please follow all steps in this procedure:**

- Have more than one senior member of staff / volunteer involved in this process. This is vital to protect individuals if accusations are subsequently reported.
- Conduct the procedure using a designated computer that will not be used by young people and if necessary can be taken off site by the police should the need arise. Use the same computer for the duration of the procedure.
- It is important to ensure that the relevant staff should have appropriate internet access to conduct the procedure, but also that the sites and content visited are closely monitored and recorded (to provide further protection).
- Record the url of any site containing the alleged misuse and describe the nature of the content causing concern. It may also be necessary to record and store screenshots of the content on the machine being used for investigation. These may be printed, signed and attached to the form (except in the case of images of child sexual abuse – see below)
- Once this has been completed and fully investigated the group will need to judge whether this concern has substance or not. If it does then appropriate action will be required and could include the following
  - Internal response or discipline procedures
  - Involvement by Local Authority or national / local organisation (as relevant).
  - Police involvement and/or action
- **If content being reviewed includes images of Child abuse then the monitoring should be halted and referred to the Police immediately. Other instances to report to the police would include:**
  - incidents of 'grooming' behaviour
  - the sending of obscene materials to a child
- **Isolate the computer in question as best you can. Any change to its state may affect a later police investigation.**

It is important that all of the above steps are taken as they will provide an evidence trail for the school, possibly the police and demonstrate that visits to these sites were carried out for child protection purposes. The completed form should be retained by the group for evidence and reference purposes.

## Record of reviewing internet sites (for suspected harassment / distress)

School	Cavendish School
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

--

### Web site(s) address Reason for concern

1.	
2.	
3.	
4.	
5.	
6.	
7.	
8.	
9.	
10.	

### Conclusion and Action proposed or taken

1.	
2.	
3.	
4.	
5.	
6.	
7.	





# Password Security Policy

## Introduction

The group will be responsible for ensuring that the technology is as safe and secure as is reasonably possible and that:

- Users can only access data to which they have permission.
- Access to personal data is securely controlled in line with the group's personal data policy.

## Responsibilities

- The management of the password security policy will be the responsibility of the ICT Technical Manager.
- Each user (adults and students) should have their own password and be responsible for its security.
- Passwords for new users, and replacement passwords for existing users will be allocated by ICT support team.
- Users will change their passwords periodically.

## Training / Awareness

- It is essential that users should be made aware of the need for keeping passwords secure.
- Adult users will be made aware of the password policy:
  - at induction
  - through the Acceptable Use Agreement
- Children / young people will be made aware of the password policy:
  - when joining the school
  - informally through reminders from staff / volunteers
  - through the Acceptable Use Agreement

## Policy Statements

All users will be provided with a username and password by the ICT team who will keep an up to date record of users and their usernames.

The following rules apply to the use of passwords:

- *the password should be a minimum of 8 characters long and:*
- *should include a mixture of types of character*
- *should not include proper names*
- *temporary passwords e.g. users with new user accounts or replacement passwords will be forced to change the temporary password when they next log-on*
- *there should be an agreed system for requests for password changes (ICT Helpdesk)*





# Implementation Plan

Actions	When/ Due Date	Leads
<ul style="list-style-type: none"> <li>Incoming Year 7- Acceptable usage policy contained within induction pack</li> </ul>	In place	I Swingler/ Admin team
Publication and enforcement of Acceptable usage policy for staff and volunteers <ul style="list-style-type: none"> <li>Whole e-safety policy published to staff</li> <li>All staff and volunteers with accompanying training. All staff required to sign form</li> <li>All new staff have Policy in induction pack</li> </ul>	In place  Ongoing	I Swingler  I Swingler/J Brown
E- Safety education for students <ul style="list-style-type: none"> <li>Review of E-safety in PSHE with emphasis E-safety linked to SRE and implementation of updates</li> <li>Review of e-safety education in Computer Technology lessons and implementation of updates</li> <li>Review and update cyberbullying support</li> <li>Use of Images/ Video protocols</li> <li>Monitoring of appropriate use of email (Language)</li> </ul>	Term 2 2016/17  Term 2 2016/17  Ongoing In place In place	I Swingler/ S Barrow  I Swingler/ N Sheridan  G Stolarek/ I Swingler
E-Safety training for staff <ul style="list-style-type: none"> <li>Ongoing training linked with publication of policy</li> </ul>	Ongoing	I Swingler/ E Howarth
E-safety support for parents <ul style="list-style-type: none"> <li>School website updated to included e-safety resources for parents</li> <li>Sessions offered throughout the year as part of Parents Forum programme</li> <li>E-safety tips part of 'Resource' Newsletter</li> </ul>	Ongoing	I Swingler/ G Stolarek T Godfrey
Password Security Policy	In place	G Stolarek
Personal Data Policy <ul style="list-style-type: none"> <li>Linked directly to Data Protection Policy</li> <li>Encryption of data on laptops</li> <li>Introduction of encrypted USB storage</li> </ul>	In place Ongoing Ongoing	J Brown G Stolarek I Swingler/ G Stolarek

## Links to other organisations or documents

The following sites will be useful as general reference sites, many providing good links to other sites:

Childnet: <http://www.childnet.com>

CEOP Think U Know: <http://www.thinkuknow.co.uk/>

Netsmartz: <http://www.netsmartz.org/index.aspx>

Teach Today: <http://www.teachtoday.eu/>

Internet Watch Foundation - report criminal content: <http://www.iwf.org.uk/>

UK Council for Child Internet Safety: <http://www.education.gov.uk/ukccis>

Safer Internet Centre: <http://www.saferinternet.org.uk/>

Information Commissioner's Office ICO: <https://ico.org.uk/for-organisations/education/>

### People

NSPCC: <http://www.nspcc.org.uk/what-you-can-do/>

Google guidance for parents: <http://www.teachparentstech.org/>

Training - SQA Internet Safety qualification: <http://www.sqa.org.uk/sqa/34591.html>

Practical Participation - Tim Davies: <http://www.practicalparticipation.co.uk/yes/>

Connect Safely Parents Guide to Facebook: <http://www.connectsafely.org/facebook-for-parents/>

Mobile guidance: <http://www.mobile-broadband.org.uk/guides/complete-resource-of-internet-safety-for-kids/>

Anti-Bullying Network: <http://www.antibullying.net/cyberbullying1.htm>

### Technology

CEOP Report abuse button: <https://www.ceop.police.uk/Ceop-Report>

Information Commissioners Office guidance on use of photos in schools: [https://ico.org.uk/media/for-organisations/documents/1136/taking\\_photos.pdf](https://ico.org.uk/media/for-organisations/documents/1136/taking_photos.pdf)

Which Parental control guidance: <http://www.which.co.uk/technology/software/reviews/security-software/>

How to encrypt files: <http://www.dummies.com/how-to/content/how-to-encrypt-important-files-or-folders-on-your-.html>

Childnet Parents and Teachers on downloading / music, film, TV and the internet -

<http://www.childnet.com/resources/downloading/home>

Microsoft Family safety software: <http://windows.microsoft.com/en-us/windows/set-up-family-safety>

# Legislation

Groups should be aware of the legislative framework under which this Online Safety Policy and guidance has been produced. It is important to note that in general terms an action that is illegal if committed offline is also illegal if committed online. It is recommended that legal advice is sought in the event of an online issue or situation.

## **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 person 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.

## **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.

#### **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.

#### **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.

#### **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 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 who 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.

### **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 context of work with young people, 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 school 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.

# Glossary of terms

<b>AUP</b>	Acceptable Use Policy – see earlier in this document
<b>Becta</b>	British Educational Communications and Technology Agency (Ceased to exist in March 2011, though resources are available from National Archives website)
<b>CEOP</b>	Child Exploitation and Online Protection Centre (part of UK Police, dedicated to protecting children from sexual abuse, providers of the Think U Know programmes.
<b>CPD</b>	Continuous Professional Development
<b>CYPS</b>	Children and Young Peoples Services (in Local Authorities)
<b>DfE</b>	Department for Education
<b>ECM</b>	Every Child Matters
<b>FOSI</b>	Family Online Safety Institute
<b>ICO</b>	Information Commissioners Office
<b>ICT</b>	Information and Communications Technology
<b>INSET</b>	In-Service Education and Training
<b>IP address</b>	The label that identifies each computer to other computers using the IP (internet protocol)
<b>ISP</b>	Internet Service Provider
<b>ISPA</b>	Internet Service Providers' Association
<b>IWF</b>	Internet Watch Foundation
<b>LA</b>	Local Authority
<b>LAN</b>	Local Area Network
<b>Learning Platform</b>	A learning platform brings together hardware, software and supporting services to support teaching, learning, management and administration.
<b>LSCB</b>	Local Safeguarding Children Board
<b>NEN</b>	National Education Network – works with the Regional Broadband Consortia (eg SWGfL) to provide the safe broadband provision to schools across Britain.
<b>Ofcom</b>	Office of Communications (Independent communications sector regulator)
<b>Ofsted</b>	Office for Standards in Education, Children's Services and Skills
<b>RBC</b>	Regional Broadband Consortia (eg SWGfL) have been established to procure broadband connectivity for schools in England. There are 10 RBCs covering 139 of the 150 local authorities:
<b>SIC</b>	Safer Internet Centre – a partnership of SWGfL, Childnet and the Internet Watch Foundation which receives European Commission funding to organise Safer Internet Day each February and promote safer internet activities.
<b>SWGfL</b>	South West Grid for Learning Trust – the Regional Broadband Consortium of SW Local Authorities – is the provider of broadband and other services for schools and other organisations in the SW
<b>TUK</b>	Think U Know – educational e-safety programmes for schools, young people and parents.

- VLE** Virtual Learning Environment (a software system designed to support teaching and learning in an educational setting)
- WAP** Wireless Application Protocol

