ESafety

Guidance Policies for ICT Acceptable Use

May 2017

Approved by The Main Board on:

12 May 2017

Next review date: May 2018

Contents

Introduction

ICT in the 21st Century is seen as an essential resource to support learning and teaching, as well as playing an important role in the everyday lives of children, young people and adults. Consequently, schools need to build in the use of these technologies in order to arm our young people with the skills to access life-long learning and employment.

Information and Communications Technology covers a wide range of resources including, web-based and mobile learning. It is also important to recognise the constant and fast paced evolution of ICT within our society as a whole. Currently the internet technologies children and young people are using both inside and outside of the classroom include:

- Websites
- Learning Platforms and Virtual Learning Environments
- E-mail and Instant Messaging
- Chat Rooms and Social Networking
- Blogs and Wikis
- Podcasting
- Video Broadcasting
- Music Downloading
- Gaming
- Mobile/Smart phones with text, video and/or web functionality
- Other mobile devices with web functionality

Whilst exciting and beneficial both in and out of the context of education, much ICT, particularly web-based resources, is not consistently policed. All users need to be aware of the range of risks associated with the use of these Internet technologies.

At Uffculme School and Uffculme Primary School we understand the responsibility to educate our pupils about eSafety issues; teaching them the appropriate behaviours and critical thinking skills to enable them to remain both safe and legal when using the internet and related technologies, in and beyond the context of the classroom.

Schools hold personal data on learners, staff and other people to help them conduct their day-to-day activities. Some of this information is sensitive and could be used by another person or criminal organisation to cause harm or distress to an individual. The loss of sensitive information can result in media coverage, and potentially damage the reputation of the school. This can make it more difficult for our schools to use technology to benefit learners.

Everybody in the schools has a shared responsibility to secure any sensitive information used in their day to day professional duties and even staff not directly involved in data handling should be made aware of the risks and threats and how to minimise them.

Both this policy and the Acceptable Use Agreement (for all staff and pupils) are inclusive of both fixed and mobile internet; technologies provided by the school (such as PCs, laptops, personal digital assistants (PDAs), tablets, webcams, whiteboards, voting systems, digital video equipment, etc); and technologies owned by pupils and staff, but brought onto school premises (such as laptops, mobile phones, camera phones, PDAs and portable media players, etc).

Monitoring

Authorised ICT staff may inspect any ICT equipment owned or leased by the School at any time without prior notice. ICT authorised staff may also monitor, intercept, access, inspect, record and disclose telephone calls, e-mails, instant messaging, internet/ intranet use and any other electronic communications (data, voice or image) involving its employees or contractors, without consent, to the extent permitted by law. This may be to confirm or obtain School business related information; to confirm or investigate compliance with School policies, standards and procedures; to ensure the effective operation of School ICT; for quality control or training purposes; to comply with a Subject Access Request under the Data Protection Act 1998, or to prevent or detect crime.

ICT authorised staff may, without prior notice, access the e-mail or any data stored in the school system, or voice-mail account where applicable, of someone who is absent in order to deal with any business-related issues retained on that account.

All monitoring, surveillance or investigative activities are conducted by ICT authorised staff and comply with the Data Protection Act 1998, the Human Rights Act 1998, the Regulation of Investigatory Powers Act 2000 (RIPA) and the Lawful Business Practice Regulations 2000.

Please note that personal communications using School ICT may be unavoidably included in any business communications that are monitored, intercepted and/or recorded.

All internet activity is logged by the School. These logs are monitored by the Network Manager reporting to the DSL.

Breaches

Any policy breach may be grounds for disciplinary action in accordance with the School Disciplinary Procedure.

Policy breaches may also lead to criminal or civil proceedings.

Incident Reporting

Any security breaches or attempts, loss of equipment and any unauthorised use or suspected misuse of ICT must be immediately reported to the school's e-safety coordinator. Additionally, all security breaches, lost/stolen equipment or data virus notifications, unsolicited emails, misuse or unauthorised use of ICT and all other policy non-compliance must be reported to the School IT Manager.

Acceptable Use of the School's IT System and the Internet (by Students)

This is for use with all secondary school pupils. Pupils at the primary school are made aware of the AUP but are not expected to sign it.

The school's IT system (inc access to the Internet, e-mail and other digital resources) are there to support your learning. To help keep you safe and everyone else safe and to ensure that you make use of these resources in a way that is appropriate and legal the following rules have been put in place. Please read them carefully and if there is anything you don't understand, please ask your tutor or ICT teacher.

I agree that:

- I will never share my password with anyone or use anyone else's password. If I become aware that my own password has become known to someone else, or I find out someone's password I will immediately inform the ICT Technical Support Team
- I will never infringe the security or privacy of another user. I will never attempt to access or alter their files or folders, or tamper with their storage area on the school system or any removable media (e.g. flash drive) they may have.
- I will do everything I can to keep myself and others safe on the Internet. I will never disclose or publicise personal information about myself or others (e.g. home address or telephone / mobile number), nor will I respond to requests using SMS or agree to meet with someone.
- I will always treat other IT users with respect and will never harass, threaten, harm, insult or offend them.
- During lessons, I will only use the school's IT systems and equipment for educational purposes linked to the learning objectives of the lesson. At break and lunchtimes students I may use the facilities for personal purposes provided they meet the other sections of the policy
- I will take care of all IT equipment and the IT environment and I will not remove any IT equipment from its current location, either temporarily or permanently.
- I will not download or bring into school unauthorised programs, or attempt to install or store them on the school's IT system or on any of its equipment.
- I will never knowingly introduce a virus or other malware to the school's systems
- I will not access or download inappropriate (e.g. pornographic, racist or offensive) materials and will ensure that none of my files contains such material. This includes viewing, displaying, downloading, and printing, sending, or otherwise transmitting materials.
- I will switch off or close my screen immediately and report to a teacher if I discover an unsuitable site.

- I will not access Internet chat rooms, social media websites, or messaging services (inc chat sites) using the school's system. I will not access online games sites during lessons
- I am aware of the 'Report It' button and know when to use it.
- I will not make audio or video recordings of another student or member of staff without their permission.
- I will never send or forward inappropriate images of myself (or others) to another person and understand that to do so is criminal offence.
- I will not copy information into assignments without fully acknowledging the source of it. I understand that if I break this rule it could be classed as plagiarism and/or copyright infringement and so have serious consequences, particularly where the work is being submitted for exam purposes.
- I will not copy or distribute any copyrighted material (inc software, video, music etc) and understand that it is illegal to do so.
- I will only use my school email account for school work and school related activities. When writing, or replying to emails I will always be polite towards others and tolerant of their views in what I say. The same applies to any attachments I may send.
- I will only open emails (and any attachments) if they come from someone I already know and trust.
- I will not forward chain e-mails, send spam or spoof e-mails or e-mails containing hoax virus warnings.
- Staff may review my files and communications (inc. e-mails) where there are concerns about the content and/or to ensure that the system, equipment and other media are being used responsibly. This may include random checks.

Please remember that if you act in an inappropriate manner your access rights may be withdrawn, which would adversely affect your learning, and further sanctions may also be imposed.

Acceptance of the above conditions:

Full Name: ___________________________________Tutor Group: _____________

Signature: ____________________________________Date: _______________

Parent's Signature: _______________________________ Date: ___________

Acceptable Use of the School's IT System and the Internet (by Staff)

The school's IT systems (inc the Uffculme School 'Cloud', e-mail Internet access and other digital resources) and equipment have been put in place to support teaching and learning and the general administrative processes of the school. They are provided and maintained for the benefit of the whole school community, and all staff are encouraged to make use of these resources in support of their work. This Acceptable Use Policy (AUP) exists to guide and inform staff on the appropriate use of the school's IT systems and equipment thereby providing protection for them and the school community.

I agree to the following:

General system or equipment use

- During normal working hours I will only use the school's IT systems and equipment for school business, other than at break and lunchtimes (and during the non-contact time of teaching staff).
- I will take care of all IT equipment and the IT environment and will not remove any IT equipment from its current location, either temporarily or permanently without the express permission of the ICT Technical Support Team.
- I will similarly ensure that any pupils for whom I am responsible also take reasonable care of all the school IT systems and equipment.
- I will not download or bring into school unauthorised programs, or attempt to install or store them on the school's IT system or on any of its equipment. Where I require that a piece of software be installed to support me in my work I will ask the ICT Technical Support Team to complete this and give them a minimum of 48 hours to do so.
- I will never knowingly introduce a virus or other malware to the school's systems
- I will never use the school's IT systems for any business or commercial purposes (with the exception of the finance staff for school business).
- If I have been issued with a school laptop or other mobile device I understand that this Acceptable Use Policy extends to both its use in school and out. I agree that I will take reasonable care for it (including its protection from theft) and that I may only install my own software on it where it does not impair the operation or performance of the laptop in any way.

Security and privacy

- I will never share my password with anyone or use anyone else's password. If I become aware that my own password has become known to someone else, or I find out someone's password I will immediately inform the ICT Technical Support Team
- I will not leave a PC or laptop unattended once I have logged in and will always lock my computer before leaving it.

- I will never infringe the security or privacy of another user. I will never attempt to access or alter their files or folders, or tamper with their storage area on the school system or any removable media (e.g. flash drive) they may have.
- I will always take care to ensure that no one else can view or gain access to information held on the school's Management Information System.
- I will ensure that all data relating to students and staff to which I have access is kept secure (whether in school or accessed remotely from outside). I will only take personal or sensitive data off site if it is encrypted.

Use of the Uffculme School 'Cloud' and the Internet

- I will not access or download inappropriate (e.g. pornographic, racist or offensive) materials and will ensure that none of my files contains such material. This includes viewing, displaying, downloading, and printing, sending, or otherwise transmitting materials.
- I will not intentionally access any websites that contain sexually inappropriate, obscene, illegal, hateful or otherwise objectionable materials. (This includes viewing, displaying, downloading, and printing, sending, or otherwise transmitting materials.) In the event that I should accidentally do so I will immediately report it to a member of the ICT Technical Support Team. (Note - Failure to report the incident will result in the incident being dealt with in the same way as if the website had been accessed deliberately.)
- I will switch off/close my screen immediately and report to the e-safety coordinator if I discover an unsuitable site.
- I will ensure that my online activity, both in school and outside school, will not bring my professional role into disrepute.
- I will never send or forward inappropriate images of myself (or others) to another person and understand that to do so is criminal offence.
- I will always treat other IT users with respect and will never harass, threaten, harm, insult or offend them.
- I will ensure that any pupils for whom I am responsible also act appropriately on the school's IT systems (including the Uffculme School 'Cloud') and the Internet and deal with any incidents brought to my attention in line with the school's Behaviour Policy.
- I will do everything I can to keep myself and others (both students and other staff) safe on the Internet. I will never disclose or publicise personal information about myself or others (e.g. home address or telephone / mobile number).
- I will only set-up and use forums, message boards, blogs, wikis with students that are part of the Uffculme School 'Cloud'. In such cases I understand that I am responsible for clearly defining the purpose of the forum, controlling its membership and moderating all entries to the forum.
- I will never agree to be a 'friend' of a pupil on a social networking site or have contact with pupils through internet chat rooms.

- Images (still and video) of school pupils may only be taken by school staff for use on the Uffculme School 'Cloud' or website. Only school equipment should be used for this purpose unless authorised by a member of the Leadership Group. At the earliest possible time these images must be transferred to an appropriate area of the 'Cloud' and deleted from the camera or other storage media. (Note - Images of pupils must never be stored on personal computers or laptops or retained on other storage media in their possession.)
- I understand that digital content focusing on individual pupils (including photographs, audio or video clips) should not be placed in 'open areas' unless the pupil's parents have given permission.
- I will always respect the work and ownership rights of people (including companies) outside the school, as well as other staff and pupils. This includes abiding by all licensing and copyright laws. (This extends to software, media files, DVDs, CDs etc)

E-mail

- I will use my school e-mail accounts for **all** school business and activities.
- I will never give out my personal e-mail address(es) to students or parents or contact them using such an account.
- I will check my school e-mail accounts regularly and make an appropriate response to all emails within 48 hours of receipt on school days in term time. If I know I will be away from e-mail contact for more than 2 days (i.e. during a school holiday) I will set an appropriate automated 'out-of office' notification.
- When sending e-mails to anyone outside of the school I will always attach a 'signature' that contains the school's name, address, telephone and fax numbers.
- When writing, or replying to emails I will treat the content of the e-mail in the same way I would any other paper based letter or document from a legal point of view. I will always be polite towards others and tolerant of their views in what I say and will reflect the expectations of me as an employee of Uffculme School. The same applies to any attachments I may send.
- I will always exercise extreme care with any attachments (and hyperlinks) received by email and will only open attachments when I have fully assessed the risk they pose
- I will not forward chain e-mails, send spam or spoof e-mails or e-mails containing hoax virus warnings.
- I understand that individual e-mails to staff may be opened in the absence of the member of staff at the discretion of the Headteacher or the member of the school's Leadership Group responsible for Strategic Development of ICT where:
    - it is essential for school business and
    - the member of staff cannot be contacted.
- I will inform the Designated Safeguarding Lead and Network Manager if I receive an offensive e-mail.

Monitoring and Sanctions

- I understand that all content on the school systems and activities conducted through these systems will be subject to automatic monitoring for inappropriate content and that where such content is detected this will be flagged to the Headteacher or member of the school's Leadership Group responsible for Strategic Development of ICT for further investigation.
- I understand that I am responsible for my behaviour and conduct in respect of the school's IT systems including the Uffculme School 'Cloud' and that failure to follow the terms of this Policy will be dealt with under the terms of the school's Conduct Policy.
- I understand that should I breaks the law in respect of the school's IT systems or equipment I will be reported to the appropriate authorities.

E-Mail

The use of e-mail within schools is an essential means of communication for both staff and pupils. In the context of school, e-mail should not be considered private.

Educationally, e-mail can offer significant benefits including; direct written contact between schools on different projects, be they staff based or pupil based, within school or international. We recognise that pupils need to understand how to style an e-mail in relation to their age and good network etiquette.

Managing E-Mail

The schools give all staff their own e-mail account to use for all school business as a work based tool. For the safety and security of users and recipients, all mail is filtered and logged; if necessary e-mail histories can be traced. The school email account should be the account that is used for all school business

- Under no circumstances should staff contact pupils, parents or conduct any school business using personal e-mail addresses
- Staff sending e-mails to external organisations, parents or pupils should check the email carefully before sending, in the same way as a letter written on school headed paper
- Pupils may only use school approved accounts on the school system and only under direct teacher supervision for educational purposes
- E-mails created or received by staff as part of their School job will be subject to disclosure in response to a request for information under the Freedom of Information Act 2000. Staff must therefore actively manage their e-mail account as follows:
  - Delete all e-mails of short-term value
  - Organise e-mail into folders and carry out frequent house-keeping on all folders and archives
- All pupil e-mail users are expected to adhere to the generally accepted rules of netiquette particularly in relation to the use of appropriate language and not revealing any personal details about themselves or others in e-mail communication.
- Pupils must immediately tell a teacher/trusted adult if they receive an offensive e-mail
- Staff must inform the Designated Safeguarding Lead and Network Manager if they receive an offensive e-mail
- Pupils are introduced to e-mail as part of the ICT Scheme of Work

Sending E-Mails

Staff should follow the following guidelines:

- If sending e-mails containing personal, confidential, classified or financially sensitive data to external third parties or agencies, refer to the Section E-mailing Personal, Sensitive, Confidential or Classified Information.

- Use their own school e-mail account so that they are clearly identified as the originator of a message.
- Keep the number and relevance of e-mail recipients, particularly those being copied, to the minimum necessary and appropriate.
- Do not send or forward attachments unnecessarily. Whenever possible, send the location path to the shared drive rather than sending attachments.
- School e-mail is not to be used for personal advertising.

Receiving e-Mails

Staff should follow the following guidelines:

- Check their e-mail regularly.
- Activate their 'out-of-office' notification when away for extended periods.
- Never open attachments from an untrusted source; consult their network manager first.
- Do not use the e-mail systems to store attachments. Detach and save business related work to the appropriate shared drive/folder.
- The automatic forwarding and deletion of e-mails is not allowed.

E-mailing Personal, Sensitive, Confidential or Classified Information

Staff should assess whether the information can be transmitted by other secure means before using e-mail - e-mailing confidential data is not recommended and should be avoided where possible.

Staff should follow the following guidelines:

- Do not send the information to any body/person whose details staff have been unable to separately verify (usually by phone).
- Send the information as an encrypted document attached to an e-mail.
- Provide the encryption key or password by a separate contact with the recipient(s).
- Do not identify such information in the subject line of any e-mail.
- Request confirmation of safe receipt.

Pupils with Additional Needs

The school endeavours to create a consistent message with parents for all pupils and this in turn should aid establishment and future development of the schools' eSafety rules.

However, staff are aware that some pupils may require additional teaching including reminders, prompts and further explanation to reinforce their existing knowledge and understanding of eSafety issues.

Where a pupil has poor social understanding, careful consideration is given to group interactions when raising awareness of eSafety. Internet activities are planned and well managed for these children and young people.

eSafety - Roles and Responsibilities

As eSafety is an important aspect of strategic leadership within the schools, the Head and governors have ultimate responsibility to ensure that the policy and practices are embedded and monitored. The named eSafety co-ordinator in these schools are at the secondary school Mr C Lepper (Safeguarding) and Mrs J Dentith at the primary school, who has been designated this role as a member of the senior leadership team. All members of the school communities have been made aware of who holds this post. It is the role of the eSafety co-ordinator to keep abreast of current issues and guidance through organisations such as SWGfL, Becta, CEOP (Child Exploitation and Online Protection) and Childnet.

Senior Management and Governors are updated by the Head/eSafety co-ordinator and all governors have an understanding of the issues and strategies at our school in relation to local and national guidelines and advice.

This policy, supported by the schools' acceptable use agreements for staff and pupils, is to protect the interests and safety of the whole school community. It is linked to the following mandatory school policies: child protection, health and safety, home–school agreements, and behaviour/pupil discipline (including the anti-bullying) policy and PSHE.

eSafety in the Curriculum

ICT and online resources are increasingly used across the curriculum. We believe it is essential for eSafety guidance to be given to the pupils on a regular and meaningful basis. eSafety is embedded within our curriculum and we continually look for new opportunities to promote eSafety.

- The school has a framework for teaching internet skills in ICT and PSHE lessons.
- The schools provide opportunities within a range of curriculum areas to teach about eSafety
- Educating pupils on the dangers of technologies that may be encountered outside school is done informally when opportunities arise and as part of the eSafety curriculum
- Pupils are aware of the relevant legislation when using the internet such as data protection and intellectual property which may limit what they want to do but also serves to protect them
- Pupils are taught about copyright and respecting other people's information, images, etc through discussion, modeling and activities
- Pupils are aware of the impact of Cyberbullying and know how to seek help if they are affected by any form of online bullying. Pupils are also aware of where to seek advice or help if they experience problems when using the internet and related technologies; i.e. parent/carer, teacher/trusted staff member, or an

organisation such as Childline or CEOP report abuse button

- Pupils are taught to critically evaluate materials and learn good searching skills through cross curricular teacher models, discussions and via the ICT curriculum

eSafety Skills Development for Staff

- Our staff receive regular information and training on eSafety issues in the form of annual briefings each September
- New staff receive information on the school's acceptable use policy as part of their induction
- All staff have been made aware of individual responsibilities relating to the safeguarding of children within the context of eSafety and know what to do in the event of misuse of technology by any member of the school community
- All staff are encouraged to incorporate eSafety activities and awareness within their curriculum areas

Internet Access

The internet is an open communication medium, available to all, at all times. Anyone can view information, send messages, discuss ideas and publish material which makes it both an invaluable resource for education, business and social interaction, as well as a potential risk to young and vulnerable people. All use of the internet is logged. Any inappropriate use will be detected by the system and acted upon.

Managing the Internet

- The schools maintain a list of students who will have supervised access to Internet resources (where reasonable) through the school's fixed and mobile internet technology
- Staff will preview any recommended sites before use
- Raw image searches are discouraged when working with pupils
- If Internet research is set for homework, specific sites will be suggested that have previously been checked by the teacher. It is advised that parents recheck these sites and supervise this work. Parents will be advised to supervise any further research
- All users must observe software copyright at all times. It is illegal to copy or distribute school software or illegal software from other sources
- All users must observe copyright of materials from electronic resources

Infrastucture

- Our schools also employ some additional web filtering which is the responsibility of the Network Manager
- Uffculme School and Uffculme Primary School are aware of their responsibility when monitoring staff communication under current legislation and takes into account; Data Protection Act 1998, The Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000, Regulation of Investigatory Powers Act 2000, Human Rights Act 1998
- Staff and pupils are aware that school based email and internet activity can be monitored and explored further if required
- The schools do not allow pupils access to internet logs
- The schools use management control tools for controlling and monitoring workstations
- If staff or pupils discover an unsuitable site, the screen must be switched off/ closed and the incident reported immediately to the e-safety coordinator or teacher as appropriate
- It is the responsibility of the schools, by delegation to the network manager, to

ensure that Anti-virus protection is installed and kept up-to-date on all school machines

- Pupils and staff are not permitted to download programs on school based technologies without seeking prior permission from subject leader teacher or other appropriate adult in school.

- If there are any issues related to viruses or anti-virus software, the network manager should be informed.

Managing the Web & Social Media

The Web including social networking sites, if used responsibly both outside and within an educational context can provide easy to use, creative, collaborative and free facilities. However it is important to recognise that there are issues regarding the appropriateness of some content, contact, culture and commercialism. To this end, we encourage our pupils to think carefully about the way that information can be added and removed by all users, including themselves, from these sites.

- At present, the schools endeavour to deny access to social networking sites to pupils within school

- All pupils are advised to be cautious about the information given by others on sites, for example users not being who they say they are

- Pupils are taught to avoid placing images of themselves (or details within images that could give background details) on such sites and to consider the appropriateness of any images they post due to the difficulty of removing an image once online

- Pupils are always reminded to avoid giving out personal details on such sites which may identify them or where they are (full name, address, mobile/home phone numbers, school details, IM/email address, specific hobbies/interests)

- Our pupils are advised to set and maintain profiles on such sites to maximum privacy and deny access to unknown individuals

- Pupils are encouraged to be wary about publishing specific and detailed private thoughts online

- Our pupils are asked to report any incidents of bullying to the school

- Staff may only create blogs, wikis or other web 2 spaces in order to communicate with pupils using systems approved by the Headteacher.

- The Headteacher and Senior Deputy Headteacher are the only people who can post on the schools' FaceBook and Twitter accounts.

Sexting

Sharing photos and videos online is part of daily life for many young people, enabling them to share their experiences, connect with friends and record their lives. Photos and videos can be shared as text messages, email, posted on social media or increasingly via mobile messaging apps, such as Snapchat, WhatsApp or Facebook Messenger. This increase in the speed and ease of sharing imagery has brought concerns about young people producing and sharing sexual imagery of themselves. This can expose them to risks, particularly if the imagery is shared further, including embarrassment, bullying and increased vulnerability to sexual exploitation. Making, possessing and distributing any imagery of someone under 18 which is 'indecent' is also illegal. This includes imagery of yourself if you are under 18. Although the production of such imagery is most likely to take place outside of school and college, these issues often manifest in school.

The National Police Chiefs Council (NPCC) made clear in 2016 that "incidents involving youth produced sexual imagery should primarily be treated as safeguarding issues". The NPCC also stated that "Schools should respond to incidents without involving the police provided that the young person shared the imagery consensually and there is no intended malice. Any such cases should be dealt with by the school directly". They went on to say however that incidents should be referred to the Police if there were aggravating factors such as a young person sharing imagery "without consent and with malicious intent".

When an incident involving youth produced sexual imagery comes to the school's attention:

- The incident should be referred to the DSL as soon as possible
- The DSL should hold an initial review meeting with appropriate school staff
- There should be subsequent interviews with the young people involved, if appropriate
- Parents should be informed at an early stage and involved in the process unless there is good reason to believe that involving parents would put the young person at risk of harm
- At any point in the process if there is a concern a young person has been harmed or is at risk of harm a referral should be made to children's social care and/or the police immediately.

The initial review meeting should consider the initial evidence and aim to establish:

- Whether there is an immediate risk to a young person or young people
- If a referral should be made to the police and/or children's social care
- If it is necessary to view the imagery in order to safeguard the young person. In most cases the imagery should not be viewed
- What further information is required to decide on the best response
- Whether the imagery has been shared widely and via what services and/or platforms.

- Whether immediate action should be taken to delete or remove images from devices or online services
- Any relevant facts about the young people involved which would influence risk assessment
- If there is a need to contact another school, college, setting or individual
- Whether to contact parents or carers of the pupils involved - in most cases parents will be involved

An immediate referral to police and/or children's social care should be made if at this initial stage:

1. The incident involves an adult
2. There is reason to believe that a young person has been coerced, blackmailed or groomed, or if there are concerns about their capacity to consent (for example owing to special educational needs)
3. What you know about the imagery suggests the content depicts sexual acts which are unusual for the young person's developmental stage, or are violent
4. You have reason to believe any pupil is at immediate risk of harm owing to the sharing of the imagery, for example, the young person is presenting as suicidal or self-harming

If none of the above apply then the school may decide to respond to the incident without involving the police or children's social care. The decision to respond to the incident without involving the police or children's social care would be made in cases when the DSL is confident that they have enough information to assess the risks to pupils involved and the risks can be managed within the school's pastoral support and disciplinary framework.

Searching devices, viewing and deleting imagery

Viewing the imagery

Adults should **never** view youth produced sexual imagery unless there is good and clear reason to do so. The decision to view imagery should be based on the professional judgement of the DSL and should always comply with the child protection policy and procedures of the school. Imagery should never be viewed if the act of viewing will cause significant distress or harm to the pupil. If a decision is made to view imagery the DSL would need to be satisfied that viewing is the only way to make a decision about whether to involve other agencies i.e. it is not possible to establish the facts from the young people involved.

If it is necessary to view the imagery then the DSL should:

- Never copy, print or share the imagery; this is illegal.
- Discuss the decision with the Headteacher.
- Ensure viewing is undertaken by the DSL or another member of the safeguarding team with delegated authority from the Headteacher.

- Ensure viewing takes place with another member of staff present in the room, ideally the Headteacher or a member of the senior leadership team. This staff member does not need to view the images.
- Ensure viewing takes place on school or college premises, ideally in the Headteacher or a member of the senior leadership team's office.
- Ensure wherever possible that images are viewed by a staff member of the same sex as the young person in the imagery.
- Record the viewing of the imagery in the school's safeguarding records including who was present, why the image was viewed and any subsequent actions
- Ensure this is signed and dated.

If youth produced sexual imagery has been unavoidably viewed by a member of staff either following a disclosure from a young person or as a result of a member of staff undertaking their daily role (such as IT staff monitoring school systems) then the DSL should ensure that the staff member is provided with appropriate support. Viewing youth produced sexual imagery can be distressing for both young people and adults and appropriate emotional support may be required.

Deletion of images

If the school has decided that other agencies do not need to be involved, then consideration should be given to deleting imagery from devices and online services to limit any further sharing of the imagery. The Searching, Screening and Confiscation advice highlights that schools have the power to search pupils for devices, search data on devices and delete youth produced sexual imagery.

The Education Act 2011 amended the power in the Education Act 1996 to provide that when an electronic device, such as a mobile phone has been seized, a teacher who has been formally authorised by the headteacher can examine data or files, and delete these, where there is good reason to do so. This power applies to all schools and there is no need to have parental consent to search through a young person's mobile phone. If during a search a teacher finds material which concerns them and they reasonably suspect the material has been or could be used to cause harm or commit an offence, they can decide whether they should delete the material or retain it as evidence of a criminal offence or a breach of school discipline. They can also decide whether the material is of such seriousness that the police need to be involved.

In most cases young people should be asked to delete imagery and to confirm that they have deleted the imagery. In normal circumstances adults in should not search through devices and delete imagery unless there is good and clear reason to do so. Young people should be reminded that possession of youth produced sexual imagery is illegal. They should be informed that if they refuse or it is later discovered they did not delete the image they are committing a criminal offence and the police may become involved. All of these decisions need to be recorded, including times, dates and reasons for decisions made and logged in the safeguarding records. Parents and carers should also be informed unless this presents a further risk to the young person. At this point the school may want to invoke their own disciplinary measures to discourage young people from sharing, creating or receiving images but this is at the discretion of the school in line with its own behaviour policies.

Recording incidents

All incidents relating to youth produced sexual imagery must to be recorded either in a safeguarding chronology or in the Sims Behaviour module whichever is most appropriate. This includes incidents that have been referred to external agencies and those that have not.

Teaching young people about sexual imagery

We recognise that teaching about safeguarding issues in the classroom can prevent harm by providing young people with skills, attributes and knowledge to help them navigate risks. Learning about youth produced sexual imagery cannot be taught in isolation. Learning about youth produced sexual imagery will be taught through the PSHE programme, as well as in the school's computing programme where it will reflect the requirements of the National Curriculum programme of study for computing. Given the potential sensitivity of these lessons it is essential that this issue is taught within an emotionally safe classroom climate where clear ground rules have been negotiated and established and where boundaries around teacher confidentiality have been clarified. If during any lesson teachers suspect any child or young person is vulnerable or at risk the school's safeguarding protocols should always be followed.

Parental Involvement

We believe that it is essential for parents/carers to be fully involved with promoting eSafety both in and outside of school and also to be aware of their responsibilities. We regularly consult and discuss eSafety with parents/carers and seek to promote a wide understanding of the benefits related to ICT and associated risks.

- Parents/carers and pupils are actively encouraged to contribute to adjustments or reviews of the school eSafety policy.

- Parents/carers are asked to read through and sign acceptable use agreements on behalf of their child on admission to school

- Parents/carers are required to make a decision as to whether they consent to images of their child being taken/used in the public domain (e.g. on school website)

- Parents/carers are expected to sign a Home School agreement containing the following statement:

  > “Ensure my child understands and signs the School’s ICT Acceptable Use Policy”

- The school disseminates information to parents relating to eSafety where appropriate in the form of:

  - Information and celebration evenings
  - Posters
  - Website/Learning Platform postings
  - Newsletter items
  - Learning platform training

Passwords and Password Security

Passwords

Staff should follow the following guidelines:

- Always use their own personal passwords to access computer based services.
- Make sure they enter their personal passwords each time they logon. Do not include passwords in any automated logon procedures.
- Change temporary passwords at first logon.
- Change passwords whenever there is any indication of possible system or password compromise.
- Do not record passwords or encryption keys on paper or in an unprotected file.
- Only disclose their personal password to authorised ICT support staff when necessary, and never to anyone else. Ensure that all personal passwords that have been disclosed are changed once the requirement is finished.
- User ID and passwords for staff and pupils who have left the School are removed from the system within one month.

If staff think their password may have been compromised or someone else has become aware of their password report it to the ICT support team.

Password Security

Password security is essential for staff, particularly as they are able to access and use pupil data. Staff are expected to have secure passwords which are not shared with anyone. The pupils are expected to keep their passwords secret and not to share with others, particularly their friends. Staff and pupils are regularly reminded of the need for password security.

- All users read and sign an Acceptable Use Agreement to demonstrate that they have understood the school’s e-safety Policy and Data Security
- Users are provided with an individual network, email, Learning Platform and Management Information System (where appropriate) log-in username.
- Pupils are not allowed to deliberately access on-line materials or files on the school network, of their peers, teachers or others
- Staff are aware of their individual responsibilities to protect the security and confidentiality of school networks. Individual staff users must also make sure that workstations are not left unattended and are locked. The automatic log-off time for the school network is 10 minutes
- Due consideration should be given when logging into the Learning Platform to the browser/cache options (shared or private computer)

Safe Use of Images

Taking of Images and Film

Digital images are easy to capture, reproduce and publish and, therefore, misuse. We must remember that it is not always appropriate to take or store images of any member of the school community or public, without first seeking consent and considering the appropriateness.

- With the written consent of parents (on behalf of pupils) and staff, the school permits the appropriate taking of images by staff and pupils with school equipment

- Staff are not permitted to use personal digital equipment, such as mobile phones and cameras, to record images of pupils, this includes when on field trips. However with the express permission of the Headteacher, images can be taken provided they are transferred immediately and solely to the school's network and deleted from the staff device

- Pupils are not permitted to use personal digital equipment, including mobile phones and cameras, to record images of the others, this includes when on field trips. However with the express permission of the Headteacher, images can be taken provided they are transferred immediately and solely to the school's network and deleted from the pupil's device

Consent of Adults Who Work at the School

- Permission to use images of all staff who work at the school is sought on induction and a copy is located in the personnel file

Publishing Pupil's Images and Work

On a child's entry to the school, all parents/carers will be asked to give permission to use their child's work/photos in the following ways:

- on the school web site.

- on the school's Learning Platform.

- in the school prospectus and other printed publications that the school may produce for promotional purposes.

- recorded/transmitted on a video or webcam.

- in display material that may be used in the schools' communal areas.

- in display material that may be used in external areas, ie exhibition promoting the school.

- general media appearances, eg local/national media/press releases sent to the press highlighting an activity (sent using traditional methods or electronically).

This consent form is considered valid for the entire period that the child attends the school unless there is a change in the child's circumstances where consent could be an issue, eg divorce of parents, custody issues, etc.

Parents/carers may withdraw permission, in writing, at any time.

Pupils' names will not be published alongside their image and vice versa. E-mail and postal addresses of pupils will not be published. Pupils' full names will not be published.

Before posting student work on the Internet, a check needs to be made to ensure that permission has been given for work to be displayed.

Only the Press Officer and IT Manager has authority to upload to the site.

Storage of Images

- Images/films of children are stored on the schools' network.
- Pupils and staff are not permitted to use personal portable media for storage of images (e.g. USB sticks) without the express permission of the Headteacher.
- Rights of access to this material are restricted to the teaching staff and pupils within the confines of the school network/Learning Platform.

Webcams and CCTV

- The schools use CCTV for security and safety.
- We do not use publicly accessible webcams in school
- Webcams in school are only ever used for specific learning purposes, i.e. monitoring hens' eggs and never using images of children or adults
- Misuse of the webcam by any member of the school community may result in disciplinary action being taken

Video Conferencing

- Permission is sought from parents and carers if their children are involved in video conferences
- Permission is sought from parents and carers if their children are involved in video conferences with end-points outside of the school
- All pupils are supervised by a member of staff when video conferencing
- All pupils are supervised by a member of staff when video conferencing with end-points beyond the school
- The school keeps a record of video conferences, including date, time and

participants.

- Approval from the Headteacher is sought prior to all video conferences within school
- The school conferencing equipment is not set to auto-answer and is only switched on for scheduled and approved conferences
- No part of any video conference is recorded in any medium without the written consent of those taking part

School ICT Equipment including Portable & Mobile ICT Equipment & Removable Media

School ICT Equipment

- As a user of ICT, staff are responsible for any activity undertaken on the school's ICT equipment provided to them.

- It is recommended that schools log ICT equipment issued to staff and record serial numbers as part of the school's inventory.

- Visitors to the school should not be allowed to plug their ICT hardware into the school network points (unless special provision has been made). They should be directed to the wireless ICT Facilities if available.

- Staff should ensure that all ICT equipment that they use is kept physically secure.

- Staff must not attempt unauthorised access or make unauthorised modifications to computer equipment, programs, files or data. This is an offence under the Computer Misuse Act 1990.

- It is imperative that staff save their data on a frequent basis to the school's network drive. Staff are responsible for the backup and restoration of any of their data that is not held on the school's network drive.

- Personal or sensitive data should not be stored on the local drives of desktop PCs. If it is necessary to do so the local drive must be encrypted.

- A time locking screensaver is applied to all machines. Any PCs etc accessing personal data must have a locking screensaver as must any user profiles.

- Privately owned ICT equipment should not be used on a school network.

- On termination of employment, resignation or transfer, staff must return all ICT equipment to their Manager. Staff must also provide details of all their system logons so that they can be disabled.

- It is your responsibility to ensure that any information accessed from staff's own PC or removable media equipment is kept secure, and that no personal, sensitive, confidential or classified information is disclosed to any unauthorised person.

- All redundant ICT equipment is disposed of in accordance with Waste Electrical and Electronic Equipment (WEEE) directive and Data Protection Act (DPA).

Portable & Mobile ICT Equipment

This section covers such items as laptops, PDAs and removable data storage devices. Please refer to the relevant sections of this document when considering storing or transferring personal or sensitive data

- All activities carried out on School systems and hardware will be monitored in accordance with the general policy

- Staff must ensure that all school data is stored on school's network. Any equipment where personal data is likely to be stored must be encrypted
- Equipment must be kept physically secure in accordance with this policy to be covered for insurance purposes. When travelling by car, best practice is to place the laptop in the boot of your car before starting your journey
- Synchronise all locally stored data, including diary entries, with the central school network server on a frequent basis
- Ensure portable and mobile ICT equipment is made available as necessary for anti-virus updates and software installations, patches or upgrades
- The installation of any applications or software packages must be authorised by the ICT support team, fully licensed and only carried out by your ICT support
- In areas where there are likely to be members of the general public, portable or mobile ICT equipment must not be left unattended and, wherever possible, must be kept out of sight
- Portable equipment must be transported in its protective case if supplied

Mobile Technologies

Many emerging technologies offer new opportunities for teaching and learning including a move towards personalised learning and 1:1 device ownership for children and young people. Many existing mobile technologies such as portable media players, PDAs, gaming devices, mobile and Smart phones are familiar to children outside of school too. They often provide a collaborative, well-known device with possible internet access and thus open up risk and misuse associated with communication and internet use.

Emerging technologies will be examined for educational benefit and the risk assessed before use in school is allowed. Our schools choose to manage the use of these devices in the following ways so that users exploit them appropriately.

Personal Mobile Devices (including phones)

- The schools allows staff to bring in personal mobile phones and devices for their own use. Under no circumstances do the schools allow a member of staff to contact a pupil or parent/carer using their personal device.
- Pupils at the secondary school are allowed to bring personal mobile devices/phones to school but must not use them for personal purposes within lesson time. At all times the device must be switched onto silent.
- Pupils at the primary school are not allowed to bring personal mobile phones into school unless they have prior permission from the Headteacher and agree that the mobile will be left in the school office during the school day.

- This technology may be used, however for educational purposes, as mutually agreed with the Headteacher. The device user, in this instance, must always ask the prior permission of the bill payer
- The schools are not responsible for the loss, damage or theft of any personal mobile device
- The sending of inappropriate text messages between any member of the school community is not allowed
- Permission must be sought before any image or sound recordings are made on these devices of any member of the school community
- Users bringing personal devices into school must ensure there is no inappropriate or illegal content on the device

School Provided Mobile Devices (including phones)

- The sending of inappropriate text messages between any member of the school community is not allowed
- Permission must be sought before any image or sound recordings are made on the devices of any member of the school community
- Where the school provides mobile technologies such as phones, laptops and PDAs for offsite visits and trips, only these devices should be used
- Where the school provides a laptop for staff, only this device may be used to conduct school business outside of school

Removable Media

- Only recommended removable media should be used.
- All removable media must be stored securely.
- Removable media must be disposed of securely by the ICT support team.

Telephone Services

Mobile Phones

- Staff are responsible for the security of their school mobile phone. They should always set the PIN code on their school mobile phone and must not leave it unattended and on display (especially in vehicles).

- Staff must report the loss or theft of any school mobile phone equipment immediately.

- The school remains responsible for all call costs until the phone is reported lost or stolen.

- Staff must read and understand the user instructions and safety points relating to the use of their school mobile phone prior to using it.

- School SIM cards must only be used in school provided mobile phones.

- Staff must not send text messages to premium rate services.

- Staff must never use a hand-held mobile phone whilst driving a vehicle. Only genuine 999 or 112 emergency calls may be made if it would be unsafe to stop before doing so.

Writing and Reviewing this Policy

Staff and Pupil Involvement in Policy Creation

Staff and pupils have been involved in making/reviewing the Policy for ICT Acceptable Use through via Student Council Meetings and staff meetings. Key reminders are provided for staff during the September Inset Days.

Review Procedure

There will be an on-going opportunity for staff to discuss with the eSafety coordinator any issue of eSafety that concerns them.

There will be an on-going opportunity for staff to discuss with either the network manager or the Designated Safeguarding Lead any issue of data security that concerns them.

This policy will be reviewed every (12) months and consideration given to the implications for future whole school development planning.

The policy will be amended if new technologies are adopted or Central Government change the orders or guidance in any way.

Current Legislation

Acts Relating to Monitoring of Staff eMail

Data Protection Act 1998

The Act requires anyone who handles personal information to comply with important data protection principles when treating personal data relating to any living individual. The Act grants individuals rights of access to their personal data, compensation and prevention of processing.

http://www.hmso.gov.uk/acts/acts1998/19980029.htm

The Telecommunications (Lawful Business Practice)

(Interception of Communications) Regulations 2000

http://www.hmso.gov.uk/si/si2000/20002699.htm

Regulation of Investigatory Powers Act 2000

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

http://www.hmso.gov.uk/acts/acts2000/20000023.htm

Human Rights Act 1998

http://www.hmso.gov.uk/acts/acts1998/19980042.htm

Other Acts Relating to eSafety

Racial and Religious Hatred Act 2006

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.

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.   Schools should already have a copy of "*Children & Families: Safer from Sexual Crime*" document as part of their child protection packs.

For more information www.teachernet.gov.uk

Communications Act 2003 (section 127)

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

The Computer Misuse Act 1990 (sections 1 – 3)

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

- access to computer files or software without permission (for example using another persons password to access files)
- unauthorised access, as above, in order to commit a further criminal act (such as fraud)
- impair the operation of a computer or program

UK citizens or residents may be extradited to another country if they are suspected of committing any of the above offences.

Malicious Communications Act 1988 (section 1)

This legislation makes it a criminal offence to send an electronic message (e-mail) that conveys indecent, grossly offensive, threatening material or information that is false; or is of an indecent or grossly offensive nature if the purpose was to cause a recipient to suffer distress or anxiety.

Copyright, Design and Patents Act 1988

Copyright is the right to prevent others from copying or using work without permission. Works such as text, music, sound, film and programs all qualify for copyright protection. The author of the work is usually the copyright owner, but if it was created during the course of employment it belongs to the employer. Copyright infringement is to copy all or a substantial part of anyone's work without obtaining them author's permission. Usually a licence associated with the work will allow a user to copy or use it for limited purposes. It is advisable always to read the terms of a licence before you copy or use someone else's material. It is also illegal to adapt or use software without a licence or in ways prohibited by the terms of the software licence.

Public Order Act 1986 (sections 17 – 29)

This Act makes it a criminal offence to stir up racial hatred by displaying, publishing or distributing written material which is threatening. Like the Racial and Religious Hatred Act 2006 it also makes the possession of inflammatory material with a view of releasing it a criminal offence.

Protection of Children Act 1978 (Section 1)

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 a 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.

Obscene Publications Act 1959 and 1964

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

Protection from Harassment Act 1997

A person must not pursue a course of conduct, which amounts to harassment of another, and which he knows or ought to know amounts to harassment of the other.

A person whose course of conduct causes another to fear, on at least two occasions, that violence will be used against him is guilty of an offence if he knows or ought to know that his course of conduct will cause the other so to fear on each of those occasions.

Acts Relating to the Protection of Personal Data

Data Protection Act 1998

http://www.opsi.gov.uk/acts/acts1998/ukpga_19980029_en_1

The Freedom of Information Act 200

http://www.ico.gov.uk/for_organisations/freedom_of_information_guide.aspx