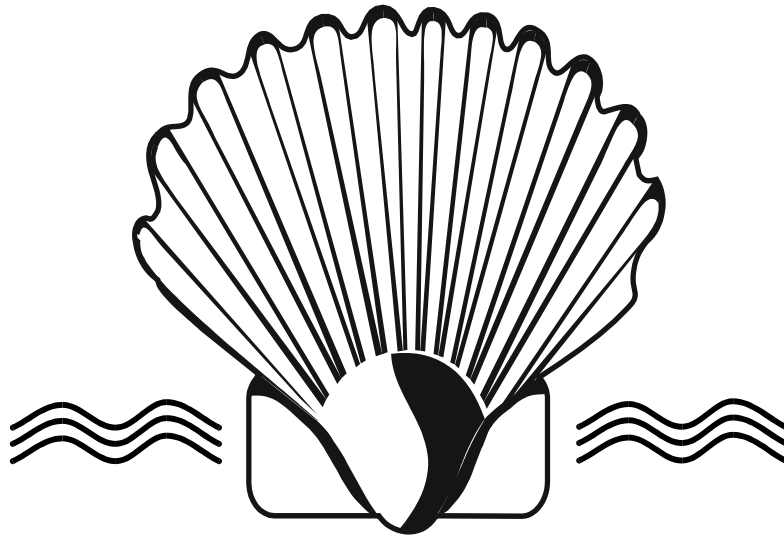


DEEPING ST JAMES COMMUNITY PRIMARY SCHOOL



eSafety and Data Security

ICT Acceptable Use

Introduction

Information and Communications Technology (ICT) in the 21st Century is an essential resource to support learning and teaching. It has a key role in the everyday lives of children, young people and adults. Schools need to build in the use of a wide range of technologies in order to enable children to access life-long learning and employment.

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

- Websites
- Email and Instant Messaging
- Chat Rooms and Social Networking
- Blogs and Wikis
- Podcasting
- Video Broadcasting
- Music Downloading
- Gaming
- Learning Platforms and Virtual Learning Environments
- 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, are not consistently policed. All users need to be aware of the range of risks associated with the use of these Internet technologies.

At Deeping St James Community Primary School, we understand our responsibility to educate our pupils on eSafety issues. We must be teaching appropriate behaviours and critical thinking skills to enable pupils to remain both safe and legal when using the internet and related technologies, in and beyond the context of the classroom.

Both this policy and the Acceptable Use Agreement (for all staff, governors, visitors and pupils) are inclusive of fixed and mobile internet technologies provided by the school (such as PCs, laptops, webcams, whiteboards, digital video equipment, etc).

Disclaimer: Due to the constant changes taking place within technology, this policy may not contain the most recent developments.

Roles and Responsibilities

As eSafety is an important aspect of strategic leadership within the school, the Headteacher and governors have ultimate responsibility to ensure that the policy and practices are embedded and monitored.

The governor responsible for ICT and ESafety will:

- Ensure regular meetings with the E-Safety Leader
- Ensure regular monitoring of e-safety incident logs
- Ensure regular monitoring of filtering / change control logs
- Ensure reporting to relevant Governors

Responsibilities of the Headteacher and Senior Leaders and esafety lead:

- The Headteacher is responsible for ensuring the safety (including eSafety) of members of the school community .
- The Headteacher and Senior Leaders are responsible for ensuring that relevant staff receive suitable skills to enable them to carry out their e-safety roles and to train other colleagues, as relevant.
- The Headteacher and Senior Leaders will ensure that there is a system in place to allow for rigorous monitoring and support of everyone in school regarding e-safety.
- The Headteacher will receive monitoring reports from the eSafety Leader.
- The Headteacher and all members of staff will be aware of the procedures to be followed in the event of a serious e-safety allegation being made against a member of staff.

The named ICT subject leader in our school is also responsible for eSafety provision. Currently the ICT subject leader is Mrs A Turner (Assistant HT). All members of the school community have been made aware of who holds this post. It is the role of the subject leader to keep abreast of current issues and guidance through organisations such as CEOP (Child Exploitation and Online Protection).

The ICT Subject Leader will:

- lead all staff in all aspects of ICT and e-safety
- take day to day responsibility for e-safety issues and take a lead role in establishing and reviewing the school e-safety policies and documents
- ensure that all staff are aware of the procedures that need to be followed in the event of an e-safety incident taking place.
- provide training and advice for staff
- liaise with the Local Authority
- liaise with school ICT technical staff
- receive reports of e-safety incidents and create a log of incidents to inform future e-safety developments.
- meet regularly with the E-Safety Governor to discuss current issues, review incident logs and filtering / change control logs
- report regularly to Senior Leadership Team

Technical staff (Currently ARK) will:

- ensure that the school's ICT infrastructure is secure and is not open to misuse or malicious attack
- ensure that the school meets the e-safety technical requirements outlined in the relevant Local Authority E-Safety Policy and guidance
- ensure that users may only access the school's networks through a properly enforced password protection policy
- ensure that the school's filtering policy is applied and updated on a regular basis and that its implementation is not the sole responsibility of any single person
- ensure that he / she keeps up to date with e-safety technical information in order to effectively carry out their e-safety role and to inform and update others as relevant
- ensure that the use of the network / Virtual Learning Environment (VLE) / remote access / email is regularly monitored in order that any misuse / attempted misuse can be reported to the E-Safety Co-ordinator/Headteacher for investigation / action / sanction
- ensure that monitoring software / systems are implemented and updated as agreed in school policies

Teaching and Support Staff are responsible for ensuring that:

- they have an up to date awareness of e-safety matters and of the current school e-safety policy and practices
- they have read, understood and signed the school Staff Acceptable Use Policy / Agreement (AUP)
- they report any suspected misuse or problem to the E-Safety Co-ordinator /Headteacher for investigation / action / sanction
- digital communications with pupils (email / voice/video conferencing etc) should be on a professional level and only carried out using official school systems
- e-safety issues are embedded in all aspects of the curriculum and other school activities
- students / pupils understand and follow the school e-safety and Acceptable Use Policy
- students / pupils have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations
- they monitor ICT activity in lessons, extra-curricular and extended school activities
- they are aware of e-safety issues related to the use of mobile phones, cameras and hand held devices and that they monitor their use and implement current school policies with regard to these devices
- **in lessons where internet use is pre-planned pupils must be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches**

Senior Management and Governors are updated by the Headteacher/subject leader 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 school's Acceptable Use Agreements for staff, governors, visitors and pupils (appendices), is to protect the interests and safety of

the whole school community . It is linked to the following school policies: child protection, health and safety, behaviour policy and PSHE.

ESafety skills development for staff

- Our staff receive information and training on eSafety issues in the form of staff meetings and notices.
- New staff receive information on the school's Acceptable Use Policy.
- All staff are 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 (appendix E).
- All staff are required to incorporate eSafety activities and awareness within their teaching of ICT.

Managing the school eSafety messages

- We endeavour to embed eSafety messages across the curriculum whenever the internet and/or related technologies are used.
- E-safety posters will be prominently displayed (Appendix F).
- Children in all year groups will be able to talk confidently about how to keep themselves safe online.

ESafety in the Curriculum

- The school embeds the teaching of eSafety across the curriculum.
- Educating pupils on the dangers of technologies that maybe encountered outside school is done as part of the on-going eSafety and wider curriculum.
- Pupils are aware of the relevant legislation when using the internet such as data protection, which may limit action but serves to protect them.
- Through discussion, modelling and activities, pupils are taught about copyright and respecting information belonging to others e.g images, uploaded documentation.
- Pupils are aware of the impact of online bullying and know how to seek help if they are affected by these issues. 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 adult, or an organisation such as Childline/ 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.**

Password Security

- All users read and sign an Acceptable Use Agreement to demonstrate that they have understood the school's e-safety Policy.
- 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, including ensuring that passwords are not shared and are changed periodically.
- Due consideration should be given to security when logging on to the server.

Data Security

The accessing of school data is something that the school takes very seriously. Staff are aware of their responsibility when accessing school data.

They must not;

- access data outside of school
- take copies of the data
- allow others to view the data
- edit the data, unless specifically requested to do so by the Headteacher.

Managing the Internet

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. Whenever any inappropriate use of the internet is detected it will be followed up.

- The school maintains students will have supervised access(where reasonable) to Internet resources 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.
- 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.

Infrastructure

- School internet access is controlled through a web filtering service.
- Deeping St James Community Primary School fulfils its 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 made aware that school-based email and internet activity can be monitored and explored further if required.
- If staff or pupils discover an unsuitable site, the screen must be switched off/ closed and the incident reported immediately to the teacher and then to the ICT subject leader.
- It is the responsibility of the school, by delegation to the network manager, to ensure that Anti-virus protection is installed on all school machines.
- Pupils and Staff using personal removable media are responsible for measures to protect against viruses, for example making sure that additional systems used have up-to-date virus protection software. It is not the school or the network manager's responsibility to install or maintain virus protection on personal systems.
- Pupils and staff are not permitted to download programs or files on school based technologies.
- If there are any issues related to viruses or anti-virus software, the ESafety co-ordinator should be informed.

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, 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 school chooses to manage the use of these devices in the following ways so that users exploit them appropriately.

Personal Mobile devices (including phones)

- The school allows staff to bring in personal mobile phones and devices for their own use. Under certain circumstances the school allows a member of staff to contact a parent/ carer using their personal device, for example when on a trip. However the use of the school mobile is usually insisted upon.
- The school is 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 .

Managing email

The use of email within most schools is an essential means of communication for both staff and pupils. In the context of school, email should not be considered private. Educationally, email can offer significant benefits including; direct written contact between schools on different projects, be they staff based or pupil based. We recognise that pupils need to understand how to style an email in relation to their age. In order to achieve ICT level 4 or above, pupils must have experienced sending and receiving emails.

- The school gives all staff their own email account to use for all school business. This is to minimise the risk of receiving unsolicited or malicious emails and avoids the risk of personal profile information being revealed.
- It is the responsibility of each account holder to keep the password secure. For the safety and security of users and recipients, all mail is filtered and logged; if necessary email histories can be traced. This 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 email addresses.
- The school requires a standard disclaimer to be attached to all email correspondence, stating that, "the views expressed are not necessarily those of the school or the LA". The responsibility for adding this disclaimer lies with the account holder.
- E-mail sent to an external organisation should be written carefully before sending, in the same way as a letter written on school headed paper.
- All e-mail users are expected to adhere to the generally accepted rules of network etiquette (netiquette) particularly in relation to the use of appropriate language, not revealing any personal details about themselves or others in e-mail communication, not arranging to meet anyone without specific permission and virus checking attachments.
- Pupils must immediately tell a teacher/ trusted adult if they receive an offensive e-mail.
- Staff must inform the ICT subject leader if they receive an offensive e-mail.
- Pupils are introduced to email as part of the ICT curriculum.

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 head teacher, images can be taken provided they are transferred immediately and solely to the school's network and deleted from the staff device.

Publishing pupils' images and work

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

- on the internet, such as the school web site
- general media appearances, eg local/ national media/ press releases sent to the press highlighting an activity (sent using traditional methods or electronically)
- Sporting event publicity

This consent form is considered valid for the entire period that the child attends this 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. Consent has to be given by both parents in order for it to be deemed valid.

E-mail and postal addresses of pupils will not be published.

Storage of Images

- Curriculum-based evidence of work e.g. images/ films of children are stored on the server
- 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, and then by use of their encrypted USB stick.
- Rights of access to this material are restricted to staff and pupils within the confines of the school network.
- Each member of staff has the responsibility of deleting stored items when they are no longer required, or the pupil has left the school.

Webcams and CCTV

- 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 will result in sanctions (as listed under the "inappropriate materials" section of this document)

Video Conferencing (Currently not applicable)

- 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.
- 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.

Additional points to consider:

- Participants in conferences offered by 3rd party organisations may not be DBS/CRB checked.
- Conference supervisors need to be familiar with how to use the video conferencing equipment, particularly how to end a call if at any point any person taking part becomes unhappy with the content of the conference.

Misuse and Infringements

Complaints

Complaints relating to eSafety should be made to the Headteacher. Incidents should be logged and the Chart for Managing an eSafety Incident should be followed (see appendix E).

Inappropriate material

- All users are aware of the procedures for reporting accidental access to inappropriate materials. The breach must be immediately reported to the Headteacher.
- Deliberate access to inappropriate materials by any user will lead to the incident being logged by the Headteacher, depending on the seriousness of the offence; investigation by the Headteacher/ governors, immediate suspension, possibly leading to dismissal and involvement of police for very serious offences (see appendix E)
- Any issues regarding inappropriate material will be reported to relevant Governors by the Headteacher

Equal Opportunities

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 school's 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.

Parental Involvement

- Parents/ carers and pupils are actively encouraged to contribute to the school ESafety policy by letter and by reporting unsuitable sites etc to the ESafety co-ordinator
- Parents/ carers are asked to read through and sign Acceptable Use Agreements on behalf of their child.
- The Acceptable Use Policy will need to be signed and returned to school before a child is allowed to access the internet at school.
- The school disseminates information to parents relating to ESafety where appropriate in the form of;
 - Website
 - Newsletter items
 - Parent information evenings/workshops

Writing and Reviewing this Policy

Stakeholder involvement in policy creation and review

- Governors have been involved in creating this ESafety policy
- Staff have been involved in reviewing the ESafety policy through staff meetings

Review Procedure

There will be an on-going opportunity for staff to discuss with the ESafety leader any issues regarding ESafety which concern them.

This policy will be reviewed every year and consideration will be 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.

Date approved by staff: _____

Date approved by Governors: _____

Signed: _____

**Deeping St James Community Primary School Acceptable Use Agreement/Code of Conduct:
Staff, Governors and Visitors**

ICT and the related technologies such as email, the internet and mobile devices are an expected part of our daily working life in school. This policy is designed to ensure that all staff are aware of their professional responsibilities when using any form of ICT. All staff are expected to sign this policy and adhere at all times to its contents. Any concerns or clarification should be discussed with the school ESafety coordinator (Headteacher).

Deliberate access to inappropriate materials by any user will lead to the incident being logged by the ESafety co-ordinator, depending on the seriousness of the offence; investigation by the head teacher/ governors, immediate suspension, possibly leading to dismissal and involvement of police for very serious offences.

- I will only use the school's email / Internet / Intranet / Learning Platform and any related technologies for professional purposes or for uses deemed 'reasonable' by the head teacher or Governing Body.
- I will comply with the ICT system security and not disclose any passwords provided to me by the school or other related authorities.
- I will ensure that all electronic communications with pupils and staff are compatible with my professional role.
- I will not give out my own personal details, such as mobile phone number and personal email address, to pupils.
- I will only use the approved, secure email system(s) for any school business.
- I will ensure that personal data is kept secure and is used appropriately, whether in school, taken off the school premises or accessed remotely. Personal data can only be taken out of school or accessed remotely when authorised by the head teacher or Governing Body.
- I will not install any hardware or software without seeking permission from the Headteacher.
- I will not browse, download, upload or distribute any material that could be considered offensive, illegal or discriminatory.
- Images of pupils and/ or staff will only be taken, stored and used for professional purposes in line with school policy and with written consent of the parent, carer or staff member. Images will not be distributed outside the school network without the permission of the parent/ carer, member of staff or head teacher.
- I understand that all my use of the Internet and other related technologies can be monitored and logged and can be made available, on request, to my line manager or head teacher.
- I will respect copyright and intellectual property rights.
- I will ensure that my online activity, both in school and outside school, will not bring my professional role into disrepute.
- I will support and promote the school's ESafety policy and help pupils to be safe and responsible in their use of ICT and related technologies.

User Signature

I agree to follow this code of conduct and to support the safe use of ICT throughout the school

SignatureDate
Full Name (printed) Job title

Agreement / ESafety Rules

- ✓ I will only use ICT in school for school purposes.
- ✓ I will only use the school email address when emailing.
- ✓ I will only open email attachments from people I know, or who my teacher has approved.
- ✓ I will not tell other people my ICT passwords.
- ✓ I will only open/delete my own files.
- ✓ I will make sure that all ICT contact with other children and adults is responsible, polite and sensible.
- ✓ I will not deliberately look for, save or send anything that could be unpleasant or nasty. If I accidentally find anything like this I will tell my teacher immediately.
- ✓ I will not give out my own details such as my name, phone number or home address. I will not arrange to meet someone I do not know.
- ✓ I will be responsible for my behaviour when using ICT because I know that these rules are to keep me safe.
- ✓ I will not access any websites that are designed for children who are older than me.
- ✓ I know that my use of ICT can be checked and that my parent/ carer will be contacted if a member of school staff is concerned about my ESafety.



SAFE

Keep **safe** by being careful not to give out personal information when you're chatting or posting online. Personal information includes your email address, phone number and password.



MEET Meeting someone you have only been in touch with online can be dangerous. Remember; online friends are still strangers, even if you have been talking to them for a long time.

ACCEPTING **Accepting** emails, or opening files, pictures or texts from people you don't know or trust can lead to problems – they may contain viruses or nasty messages!

RELIABLE Someone online might lie about who they are and information on the internet may not be true or **reliable**. Always check information with other websites, books or someone who knows. If you like chatting online it's best to only chat to your 'real world' friends and family.

TELL Always **tell** a parent, carer or a trusted adult if someone or something makes you feel uncomfortable or worried. Or if you or someone you know is being bullied online.

Appendix C

Dear Parent/ Carer

ICT, including the internet, email and mobile technologies is an integral part of learning at Deeping St James COMMUNITY Primary School. We work hard to ensure that all of our children are safe and responsible when using any aspect of ICT.

Please read and discuss these ESafety rules with your child. Sign and return the slip at the bottom of the page. The slip below will need to be signed and returned to school before your child is allowed to access the internet at school. If you have any concerns or would like further explanation please do not hesitate to contact me.

Yours sincerely

Mr. I. Wilkinson
Headteacher

.....
.....

Parent/Carer Signature

We have discussed this and (child's name) agrees to follow the ESafety rules and to support the safe use of ICT at Deeping St James COMMUNITY Primary School.

Parent/Carer Signature with legal responsibility.

Class Date.....

Appendix D

Appendix E

Managing an ESafety incident

1. Is it legal? Was illegal material or activity found?	
<p>No-</p> <ul style="list-style-type: none"> Record the incident in the log Keep any evidence Was the perpetrator a pupil or a member of staff? 	
<p>Child-</p> <ul style="list-style-type: none"> Follow Behaviour Policy Inform parents Review school policies and procedures 	<p>Staff-</p> <ul style="list-style-type: none"> Was it accidental or deliberate? Does a child need support? Is the member of staff unsafe to work with children? Is it a disciplinary issue?
<p>Yes-</p> <ul style="list-style-type: none"> Inform police and follow instructions Confiscate school laptops and computers Disable user account Save evidence but do not view or copy If a child is involved, inform Child Protection Officer Contact designated officer for allegations 	

Appendix F

Internet Safety Poster

Stay safe online

Remember the 5 SMART rules when using the internet and mobile phones.

S

SAFE: Keep safe by being careful not to give out personal information – such as your full name, email address, phone number, home address, photos or school name – to people you are chatting with online.

M

MEET: Meeting someone you have only been in touch with online can be dangerous. Only do so with your parents' or carers' permission and even then only when they can be present.

A

ACCEPTING: Accepting emails, IM messages, or opening files, pictures or texts from people you don't know or trust can lead to problems – they may contain viruses or nasty messages!

R

RELIABLE: Information you find on the internet may not be true, or someone online may be lying about who they are. Make sure you check information before you believe it.

T

TELL: Tell your parent, carer or a trusted adult if someone or something makes you feel uncomfortable or worried, or if you or someone you know is being bullied online.



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.hmsso.gov.uk/acts/acts1998/19980029.htm>

The Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000

<http://www.hmsso.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.hmsso.gov.uk/acts/acts2000/20000023.htm>

Human Rights Act 1998

<http://www.hmsso.gov.uk/acts/acts1998/19980042.htm>

Other Acts relating to ESafety

Racial and Religious Hatred Act 2006

It is 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

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 Appendix 10 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 person's 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 their 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 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.