DIOCESE OF

ST ALBANS

MULTI-ACADEMY TRUST

Caldecote Church of England Academy

E-Safety Policy

Policy name: E-Safety Policy

Written by: Sarah Campbell

Date written: November 2023

Review date: November 2024

Caldecote Church of England Academy

E-safety policy

Rationale

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 inside or outside of the classroom include:

- Websites
- Learning Platforms and Virtual Learning Environments (VLE's)
- Email 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, are not consistently policed. All users need to be aware of the range of risks associated with the use of these Internet technologies.

At Caldecote CE Academy, we understand the responsibility to educate our pupils on E- Safety 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. This applies across the school from Foundation to Year 4 and is taught and dealt with in an age appropriate manner.

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

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

- Information and celebration evenings
- Website postings
- Newsletter items

Roles and Responsibilities

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

It is the role of the Head Teacher to keep abreast of current issues and guidance through organisations such as the LA, Becta, CEOP (Child Exploitation and Online Protection) and Childnet.

This policy, supported by the school's Acceptable Use Policies for staff, governors, trainees and pupils is to protect the interests and safety of the whole school community. It is linked to the following mandatory school policies: safeguarding policy, health and safety and behaviour (including the anti-bullying) policy and RSE.

All staff read and sign an Acceptable Use Policy to demonstrate that they have understood the school's E-Safety Policy.

Managing the school E-Safety messages

We endeavour to embed E-Safety messages across the curriculum whenever the internet and/or related technologies are used.

The E-Safety policy will be introduced to the pupils at the start of each school year and form part of the ongoing computing and PSHCE curriculum areas.

E-Safety skills development for staff

Staff will receive regular information and training on E-Safety issues as new developments occur. All staff will be expected to incorporate E-Safety activities and awareness within their curriculum areas.

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 E-Safety and know what to do in the event of misuse of technology by any member of the school community (see attached flowchart.)

E-Safety in the Curriculum

The school has a framework for teaching internet skills in ICT, using Purple Mash.

Educating pupils on the dangers of technologies that maybe encountered outside school is done informally when opportunities arise and as part of the E-Safety curriculum in an age appropriate manner.

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, modelling and activities.

Pupils are made 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 staff member, 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

Staff are provided with an individual network log-in username. They are expected to use a personal password and to keep it private.

Users who believe that their password may have been compromised or someone else has become aware of their password should report this to the headteacher or ICT technician.

Pupils have individual logins for many sites including Google Classroom, Lexia, TT Rockstars and Purple Mash. Pupils are not allowed to use the accounts of others or make any attempt to 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, MIS systems and/or Learning Platform, including ensuring that passwords to these areas are not shared and are changed when prompted to do so by the system.

Individual staff users must also make sure that workstations are not left unattended without being locked.

Pupils and staff must ensure that they log off the school network at the end of each lesson, or at the end of each day.

Passwords should not be saved in the cache when logging on to any computer which is shared.

Data Security

It is a legal requirement of the Data Protection Act 1998 to protect and secure personal data. Becta defines personal data as "any combination of data items that identifies an individual and gives specific information about them, their families or circumstances. This includes names, contact details, gender, dates of birth, behaviour and assessment records." Staff should follow the procedures outlined in BECTA Data Security Do's and Don'ts (appendices).

Staff should use data drives that are encrypted so that any data can be kept secure, if it is transported. Best practice should be that data is not taken out of school in any format. We request that data is stored on the school provided One Drive system and that this is password protected.

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.

Pupils will have supervised access 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.

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 and any further research.

Surf Protect is our filtering system and endeavours to identify any unsuitable material and stop it being viewed. At the end of each day, the headteacher and DSL receive a report that shows any sites that have been blocked during the course of the day. We have the ability to see the time of the site block and the key word that was blocked if it was part of a particular search. This will then be followed up with classes. If staff or pupils discover an unsuitable site that is not blocked by Surf Protect, the screen must be switched off/closed and the incident reported immediately to the Head Teacher and Partnership Education.

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

Caldecote CE Academy is aware of its responsibility when monitoring staff communication under current legislation and takes into account: Data Protection Act 2018, The Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000, Regulation of Investigatory Powers Act 2000, Human Rights Act 1998.

School internet access is controlled through the web filtering service 'Surf Protect' by Exa.
Staff and pupils are aware that school-based email and internet activity can be monitored and explored further if required.

The school does not allow pupils access to internet logs.

It is the responsibility of the school, to ensure that Anti-virus protection is installed and kept up to date on all school machines; staff with school laptops will check that updates are being regularly performed. The school works closely with Partnership Education, the DSAMAT appointed contractor, to ensure that this is timely.

Pupils and Staff using personal removable media are responsible for measures to protect against viruses carried on such media. It is not the school's responsibility, to install or maintain virus protection on personal systems. Pupils are not permitted to bring in and use portable storage devices.

If there are any issues related to viruses or anti-virus software, Partnership Education and DSAMAT should be informed immediately by raising an emergency ticket and contacting COO.

Managing other Advanced Internet technologies

Social networking sites, if used responsibly, both outside and within an educational context, can provide easy to use, creative and free facilities. However, it is important to recognise that the age appropriate rating for social networking, is 13 years. We ensure that our children and families are aware of the age rating. We ensure that children and families are informed about the way that information can be added and removed by all users, including themselves, from these sites.

At present, the school endeavours 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 through any electronic media.

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, 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.

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 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 does not allow pupils to bring in personal mobile phones however the school does allow staff to bring in personal mobile phones and devices for their own use. Under no circumstances does the school allow a member of staff to contact a pupil or parent/carer using their personal device – The only exception to this rule is the contacting of parents where necessary during a school trip, in an emergency and only under the direction of the SEC (School Emergency Contact)

The school is not responsible for the loss, damage or theft of any personal mobile device.

The sending of inappropriate text messages between any members 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.

Users bringing personal devices into school must ensure there is no inappropriate or illegal content on the device.

Where the school provides mobile technologies such as phones, laptops and tablets for offsite visits and trips, only these devices should be used.

Managing email

The use of email 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, within school or wider afield. We recognise that pupils need to understand how to style an email in relation to their age and good network etiquette (netiquette) and this forms part of our Purple Mash curriculum.

The school gives all permanent 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.

Email sent to an external organisation should be written carefully before sending, in the same way as a letter written on school headed paper.

If staff are sending emails to parents or pupils, they are advised to cc. the Head teacher, DSL or office.

All email 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 email communication, or arrange to meet anyone without specific permission, and virus checking attachments.

Pupils must immediately tell a teacher/trusted adult if they receive an offensive email.

Staff must inform (Head Teacher/line manager) if they receive an offensive email.

Pupils are introduced to email as a part of their induction in the use of the school's ICT systems in Lower Key Stage 2.

Safe Use of Images

Taking of Images and Film Digital images are easy to capture, reproduce and publish and, therefore, misuse. It is therefore not always appropriate to take or store images of any member of the school community or public, without first seeking consent and considering any potential harm that might arise.

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.

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/guardians will be asked to give permission to use their child's work/photos in the following ways:

- on the school web site
- on social media (X or Facebook for example)
- on the school newsletter (Using Microsoft Sway)
- in the school prospectus and other printed publications that the school may produce for promotional purposes
- in display material that may be used in the school's communal areas
  in display material that may be used in external areas, i.e. exhibition promoting the school
- general media appearances, e.g. 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 this school unless there is a change in the child's circumstances where consent could be an issue, e.g. 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. Email and postal addresses of pupils will not be published. Pupils' full names will not be published. The Head teacher must authorise all web site content.

Storage of Images

Images/films of children are stored on the school's network.

Pupils and staff are not permitted to use personal portable media for storage of images (e.g. USB sticks, laptops) without the express permission of the Head teacher.

Rights of access to this material are restricted to the staff and pupils within the confines of the school network.

Webcams

Webcams in school are only ever used for specific learning purposes.

Pupils will be supervised when using webcams.

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)

Misuse and Infringements

Complaints

Complaints relating to E-Safety should be made to the Head teacher. Incidents should be logged and the Flowcharts for Managing an E-Safety Incident (appendices) should be followed.

Inappropriate material
All users are aware of the procedures for reporting accidental access to inappropriate materials. The breach must be immediately reported to the DSAMAT COO.

Deliberate access to inappropriate materials by any user will lead to the incident being logged by the ICT Technician, and, depending on the seriousness of the offence, investigation by the Headteacher, DSAMAT, immediate suspension, possibly leading to dismissal and involvement of police for very serious offences.

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

There will be an on-going opportunity for staff to discuss with the SENDCo any issue of E-Safety 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.

Our e-Safety Policy has been written by the school, building on the Hertfordshire Grid for Learning exemplar policy (with acknowledgement to LGfL, SWGfL and Bristol City Council) and Becta guidance.

Appendix 1

BECTA Good practice in information handling:

Data security dos and don'ts. We have written this guide for anyone working in a school, college or university who collects, manages, transfers or uses data about learners, staff or other individuals during the course of their work. Its aim is to raise your awareness of where potential breaches of security could occur. Following these 'dos and don'ts' will help you to prevent data from being lost or used in a way which may cause individuals harm or distress and/or prevent the loss of reputation your organisation may suffer if you lose personal data about individuals.

This document is one of a series of good practice guides to help schools, colleges and universities protect personal and sensitive data. Building on good practice from industry and central government these guides describe procedures and possible technical and operational solutions that can help organisations reduce the risks of data security incidents and comply with current legislation.

Produced by Becta on behalf of the Department for Children, Schools and Families, these guides have been reviewed and updated with feedback from a number of cross-sector organisations including DCSF, DIUS, JISC Legal, The Information Authority and JANET(UK), as well as from schools, local authorities, RBCs and suppliers. For further information on these guides, please see

http://www.becta.org.uk/schools/datasecurity http://www.becta.org.uk/feandskills/datasecurity.

Your roles and responsibilities

As a member of your organisation you have a shared responsibility to secure any sensitive or personal data you use in your day-to-day professional duties.

1.1 Important 'dos'

- make sure you and your colleagues are adequately trained
- follow guidance
- become more security aware
- raise any security concerns
- encourage your colleagues to follow good practice and guidance
- report incidents

1.2 Why protect information?

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

1.3 What information do you need to protect?

You should secure any personal data you hold about individuals and any data that is deemed sensitive or valuable to your organisation. Your organisation should have someone who is responsible for working out exactly what information needs to be secured. This person is your Information Asset Owner. They should understand what information you need to handle, how the information changes over time, who else is able to use it and why. Several people may share this role if you work in a large organisation.

1.4 Using protective markings

It is good practice to protectively mark personal data. This will help people handling it understand the need to keep it secure and to destroy it when it is no longer needed. This is especially important if personal data information is combined into a report and printed. Your Information Asset Owner should help you work out how you need to mark the information you view as part of your job. There are different levels of marking depending on how just how sensitive the information is.

1.5 Steps you can take to help prevent security problems

There are plenty of things that you should do (or not do) that will greatly reduce the risks of sensitive information going missing or being obtained illegally. Many of these 'dos and don'ts' will apply to how you handle your own personal information. Using these practices will help you to protect your own privacy. We have separated these points into different areas to make it easier for you to refer back to.

1.6 Working online

Do:

make sure that you follow your organisation's policies on keeping your computers up to date with the latest security updates. Make sure that you keep any computers that you own up to date. Computers need regular updates to their operating systems, web browsers and security software (anti-virus and antispyware). Get advice from your IT team if you need help.

only visit websites that are allowed by your organisation. Remember your organisation may monitor and record (log) the websites you visit.

turn on relevant security warnings in your web browser (for example, the automatic phishing filter available in Internet Explorer and attack and forgery site warnings in Mozilla Firefox.)

make sure that you only install software that your IT team has checked and approved • be wary of links to websites in emails, especially if the email is unsolicited

only download files or programs from sources you trust. If in doubt, talk to your IT team.

check that your organisation has an acceptable-use policy (AUP)1 for the internet and ensure that you follow it.

1.7 Email and messaging

Do:

- read your organisation's email policy
- report any spam or phishingemails to your IT team that are not blocked or filtered
- report phishing emails to the organisation they are supposedly from

1 See Becta's publication AUPs in Context: Establishing Safe and Responsible Online Behaviours [http://publications.becta.org.uk/display.cfm?resID=39286]

2 See Becta's information on developing e-safety policies [http://schools.becta.org.uk/index.php?section=is&catcode=ss_to_es_pp_pol_03]

3 Phishing is an attempt to obtain your personal information (for example, account details) by sending you an email that appears to be from a trusted source (for example, your bank) [http://www.google.co.uk/search?q=define%3A+phishing]

use your organisation's contacts or address book. This helps to stop email being sent to the wrong address

1.7.2

Don't

• click on links in unsolicited emails. Be especially wary of emails requesting or asking you to confirm any personal information, such as passwords, bank details and so on
• turn off any email security measures that your IT team has put in place or recommended
• email sensitive information unless you know it is encrypted . Talk to your IT team for advice
• try to bypass your organisation's security measures to access your email off-site (for example, forwarding email to a personal account)
• reply to chain emails

1.8 Passwords

1.8.1 Do

• follow your organisation's password policy
• use a strong password (strong passwords are usually eight characters or more and contain upper- and lower-case letters, as well as numbers)
• make your password easy to remember, but hard to guess
• choose a password that is quick to type
• use a mnemonic (such as a rhyme, acronym or phrase) to help you remember your password. Change your password(s) if you think someone may have found out what they are

1.8.2 Don't

• share your passwords with anyone else
• write your passwords down
• use your work passwords for your own personal online accounts
• save passwords in web browsers if offered to do so
• use your username as a password
• use names as passwords
email your password or share it in an instant message.

1.9 Laptops

4 Encryption is a way of scrambling information. It helps stop anyone using the information if they do not have an electronic key or password to unscramble it

1.9.1 Do

• shut down your laptop using the 'Shut Down' or 'Turn Off' option
• try to prevent people from watching you enter passwords or view sensitive information
• turn off and store your laptop securely (if travelling, use your hotel's safe)
• use a physical laptop lock if available to prevent theft

• lock your desktop when leaving your laptop unattended
• make sure your laptop is protected with encryption software

1.9.2 Don't

• store remote access tokens with your laptop
• leave your laptop unattended unless you trust the physical security in place
use public wireless hotspots – they are not secure
• leave your laptop in your car. If this is unavoidable, temporarily lock it out of sight in the boot.
• let unauthorised people use your laptop
• use hibernate or standby

1.10 Sending and sharing

1.10.1 Do

• be aware of who you are allowed to share information with. Check with your Information Asset Owner if you are not sure
• ask third parties how they will protect sensitive information once it has been passed to them
• encrypt all removable media (USB pen drives, CDs, portable drives) taken outside your organisation or sent by post or courier

1.10.2 Don't

• send sensitive information (even if encrypted) on removable media (USB pen drives, CDs, portable drives) if secure remote access is available
• send sensitive information by email unless it is encrypted
• place protective labels on outside envelopes. Use an inner envelope if necessary. This means that people can't see from the outside that the envelope contains sensitive information
assume that third-party organisations know how your information should be protected

1.11 Working on-site

1.11.1 Do
• lock sensitive information away when left unattended
• use a lock for your laptop to help prevent opportunistic theft

1.11.2 Don't

- let strangers or unauthorised people into staff areas
- position screens where they can be read from outside the room

1.12 Working off-site

1.12.1 Do

- only take offsite information you are authorised to and only when it is necessary. Ensure that it is protected offsite in the ways referred to above
- wherever possible access data remotely instead of taking it off-site
- be aware of your location and take appropriate action to reduce the risk of theft
- make sure you sign out completely from any services you have used

try to reduce the risk of people looking at what you are working with

1.12.2 Don't

- leave your laptop behind if you travel abroad (some countries restrict or prohibit encryption technologies)

Further help and support

Your organisation has a legal obligation to protect personal information. Your senior management should be aware of their legal obligations under the Data Protection Act 1998. For more information, visit the website of the Information Commissioner's Office [http://www.ico.gov.uk].

More detailed guidance for organisations can be found on the Becta website [http://www.becta.org.uk/plansustainablesuccess and http://www.becta.org.uk/schools/esafety].

Test your online safety skills at the Get Safe Online website [http://www.getsafeonline.org].

Appendix 2

Caldecote CE Academy E-Safety Incident Log

Details of ALL E-Safety incidents are to be recorded by the Headteacher. This incident log will be monitored termly by the Headteacher and any incidents reported to Governors. Any incidents involving cyber bullying should be recorded using the behaviour monitoring system.

Date: Time: When the occurrence took place:	Name of pupil or staff member: Logged by:
Description of the occurrence: (what happened Inc. classification of any information compromised)	
Immediate corrective action: (what was done to minimise the impact of the incident) Further Action: (tasks to be undertaken to prevent occurrence)	
Advice taken:	
If yes logged from whom and actions Legal implications:	
Closed Date:	
Date by which the incident was closed by the Head / SIRO	
Signed by all parties involved in incident to clarify actions taken	

Appendix 3

E-Safety Rules


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.
Find out more at Childnet's website ...
www.kidsmart.org.uk
Childnet International © 2002-2007 Registered Charity no. 1080173 www.childnet.com
Childnet International
Kid Smart

Appendix 4

Current Legislation Acts relating to monitoring of staff email:

Data Protection Act 2018. 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 E-Safety 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 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 (email) 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 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.