The Bridge School

E-Safety Policy

2019

Contents

1. 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
- Virtual Learning Platforms
- Email and Instant Messaging
- Chat Rooms and Social Networking
- Forums, Wikis and Blogs
- 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.

We understand the responsibility to educate our students 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.

Both this policy and the Acceptable Use Agreement (for all staff, Management Committee members, visitors and students) 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 students and staff, but brought onto school premises utilising the school's network (such as laptops, mobile phones, camera phones, PDAs and portable media players, etc).

2. Roles and Responsibilities

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

The named eSafety co-ordinator in our school is **Nigel Hunt** who has been designated this role as a member of the senior leadership team. All members of the school community 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 Halton LA, CEOP (Child Exploitation and Online Protection) and Childnet.

Senior Management and Management Committee are updated by the Head or eSafety co-ordinator and all Management Committee members 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 Policy*** for staff, Management Committee members, visitors and students (appendices), is to protect the interests and safety of the whole school community. It is linked to the following mandatory school policies: The Bridge School Safeguarding and Child Protection Policy 2018/19 which includes reference to *"Keeping Children Safe in Education 2018"* and *"Guidance for safer working practice for those working with children and young people in education settings 2015"*, Health and Safety, home–school agreements, and Behaviour (including the anti-bullying) Policy and PHSE.

3. e-Safety skills development for staff

- Our staff receive regular information and training on eSafety issues in the form of regular staff training.
- Details of the ongoing staff training programme can be found in the School Development and Improvement Plan
- 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 (see attached flowchart.)
- All staff are encouraged to incorporate eSafety activities and awareness within their curriculum areas.

4. Managing the school e-Safety messages

- We endeavour to embed eSafety messages across the curriculum whenever the internet and/or related technologies are used.
- The e-safety policy will be introduced to the students at the start of each school year.
- E-safety posters will be prominently displayed.

5. e-Safety in the Curriculum

- Educating students on the dangers of technologies that maybe encountered outside school is done informally when opportunities arise and as part of the eSafety curriculum.
- Students are taught about copyright and respecting other people's information, images, etc through discussion, modelling and activities.
- Students are aware of the impact of online bullying and know how to seek help if they are affected by these issues. Students 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.

6. Password Security

- All users read and sign an Acceptable Use Agreement to demonstrate that they have understood the school's e-safety Policy.
- Users are provided with an individual network, email and Learning Platform log-in username.
- Students are not allowed to deliberately access on-line materials or files on the school network, of their peers, teachers or others.
- If you think your password may have been compromised or someone else has become aware of your password report this to the Headteacher
- Staff are aware of their individual responsibilities to protect the security and confidentiality of school networks, SIMS MIS system and/or Virtual Learning Platform, including ensuring that passwords are not shared and are changed periodically. Individual staff users must also make sure that workstations are not left unattended and are locked.
- Due consideration should be given when logging into the Virtual Learning Platform to the browser/cache options (shared or private computer)
- In our school, all ICT password policies are the responsibility of the Headteacher and all staff and students are expected to comply with the policies at all times.

7. Data Security

The accessing of school data is something that the school takes very seriously. The school follows Becta guidelines (published Autumn 2008).
Staff are aware of their responsibility when accessing school data. They must not;

- Allow others to view the data
- Edit the data unless specifically requested to do so by the Headteacher.

8. 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. All use of the **Halton Internet Web Filtering Systems** is logged and the logs are randomly monitored. Whenever any inappropriate use is detected it will be followed up by Halton Borough Council through its eSafety responsibilities.

- Students 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 students.
- 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.

9. Infrastructure

Halton Local Authority has a monitoring solution where web-based activity is monitored and recorded.

- School internet access is controlled through the LA's web filtering service.
- The school is aware of 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 students are aware that school based email and internet activity can be monitored and explored further if required.
- The school does not allow students access to internet logs.
- The school uses management control tools for controlling and monitoring workstations.
- If staff or students discover an unsuitable site, the screen must be switched off/ closed and the incident reported immediately to the e-safety co-ordinator.
- It is the responsibility of the school, by delegation to the network manager, to ensure that Anti-virus protection is installed and kept up-to-date on all school machines.
- Students and staff are not permitted to download programs or files on school based technologies without seeking prior permission from the Headteacher.

The reference to Halton Local Authority and its web filtering systems is based on the school purchasing the relevant Council's web filtering SLA: The Bridge School currently (present to April 2017) has this arrangement in place.

10. Managing other Web 2 technologies

Web 2/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 there are issues regarding the appropriateness of some content, contact, culture and commercialism. To this end, we encourage our students to think carefully 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 students within school. It is also noted that the age of the children would suggest that they are too young to sign up to social networking sites but may have access to them. Therefore all the advice and teaching is given in context of being SMART on line.
- All students are advised to be cautious about the information given by others on sites, for example users not being who they say they are.
- Students 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.
- Students 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 students are advised to set and maintain profiles on such sites to maximum privacy and deny access to unknown individuals.
- Students are encouraged to be wary about publishing specific and detailed private thoughts online.
- Our students 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 students using the LA Learning Platform or other systems approved by the Headteacher.
- Staff may not use social media to contact students at any time

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

Social network sites (such as 'Whatsapp' and Facebook) and Apps are not to be used by staff to discuss students at any time.

12. Personal Mobile devices (including phones)

- The school allows 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 student or parent/ carer using their personal device.
- Students are not allowed to bring personal mobile devices/phones to school unless with the prior approval of the school.
- The school is not responsible for the loss, damage or theft of any personal mobile device.
- The sending of inappropriate text messages or emails 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. Failure to comply with this rule may lead to a complete ban of mobile devices for that student.
- It will be requested that recordings that are made without permission, and that are deemed inappropriate, will be deleted. Police advice may be sought when this request is not adhered to.
- Users bringing personal devices into school must ensure there is no inappropriate or illegal content on the device.
- Staff should not contact students outside normal school hours.

13. 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.

14. Managing email

The use of email within most schools is an essential means of communication for both staff and students. 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 student based, within school or international. We recognise that students need to understand how to style an email in relation to their age and good 'netiquette'.

- 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 students, 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.
- Staff sending emails to external organisations, parents or students are advised to cc. the Headteacher, line manager or designated account.
- Students may only use school approved accounts on the school system and only under direct teacher supervision for educational purposes.
- Children use a class/group email address.
- The forwarding of chain letters this includes jokes and funnie statements. is not permitted in school.
- 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 and not revealing any personal details about themselves or others in e-mail communication, or arrange to meet anyone without specific permission, virus checking attachments.
- Students must immediately tell a teacher/trusted adult if they receive an offensive e-mail.
- Staff must inform (the eSafety co-ordinator/ line manager) if they receive an offensive e-mail.
- Students are introduced to email as part of the ICT Scheme of Work.

15. Safe Use of Images – Taking of Images and Film

Digital images are easy to capture, reproduce and publish and, therefore, misused. 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 students) and staff, the school permits the appropriate taking of images by staff and students with school equipment.
- Staff are not permitted to use personal digital equipment, such as mobile phones and cameras, to record images of students, 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.
- Students 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 students device.

16. 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.

17. Publishing student'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 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 school's communal areas
- in display material that may be used in external areas, ie 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. Consent may be required, in some cases, to be given by both parents in order for it to be deemed valid.

Students' names will not be published alongside their image and vice versa. E-mail and postal addresses of students will not be published. Students' 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.

18. Storage of Images

- Images/ films of children are stored on the school's network
- Students 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 students within the confines of the school network/ Learning Platform.
- ***Individual subject teachers and designated Key Workers,*** who may have stored images related to their subject work and mentoring, have the responsibility of deleting the images when they are no longer required, or the student has left the school.

19. CCTV and Webcams

- ***CCTV is used in The Bridge School. It is used in order to monitor student behaviour, the movement and presence of people within the school site and building, and for training and evaluation purposes for Bridge School staff only.***
- ***Images and footage from CCTV will not be communicated to any person outside of the school apart from if a crime has been committed and the Police request footage for the purposes of prosecution.***
- ***Staff will make parents/carers and students aware of this policy during the student Induction process.***
- We do not use publicly accessible webcams in school.
- Webcams in school will only ever used for specific learning purposes, e.g. 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)
    - Consent is sought from parents/carers and staff on joining the school, in the same way as for all images.

20. 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 students are supervised by a member of staff when video conferencing
- All students are supervised by a member of staff when video conferencing with end-points beyond the school.
- The school will keep 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.

21. Misuse and Infringements

Complaints

Complaints relating to eSafety should be made to the eSafety co-ordinator or Headteacher. Incidents should be logged on the school complaints records.

Inappropriate material

- All users are aware of the procedures for reporting accidental access to inappropriate materials. The breach must be immediately reported to the eSafety co-ordinator.
- 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 Headteacher/LA, immediate suspension, possibly leading to dismissal and involvement of police for very serious offences.
- Users are made aware of sanctions relating to the misuse or misconduct by formal interview and follow up letter from the Headteacher.
- Cyber bullying of staff will be recorded and monitored in the same manner as cyberbullying of students.

22. Prevent Strategy

Radicalisation and the Use of Social Media to encourage extremism

The internet and the use of social media in particular has become a major way to communicate with others, especially young people, which has provided access for like-minded people to create an online community and confirm extreme beliefs such as extreme ideological views or the use of violence to solve problems. This has led to social media becoming a platform for:

- intensifying and accelerating the radicalisation of young people;
- confirming extreme beliefs;
- accessing to likeminded people where they are not able to do this off-line, creating an online community;
- normalising abnormal views and behaviours, such as extreme ideological views or the use of violence to solve problems and address grievances.

The Bridge School has a number of measures in place to help prevent the use of Social Media for this purpose:

- Web site filtering is in place to help prevent access to terrorist and extremist material and social networking sites such as Facebook, Instagram or Twitter by Pupils
- Pupils and Staff are educated in safe use of Social Media and the risks posed by on-line activity, including from extremist and terrorist groups.

Further details on how social media is used to promote extremism and radicalisation can be found in guidance from the Department for Education '*How Social Media Is Used To Encourage Travel To Syria And Iraq: Briefing Note For Schools.'*

Reporting of E-Safety issues and concerns including concerns regarding Radicalisation

The Bridge School has clear reporting mechanisms in place, available for all users to report issues and concerns. For staff, any concerns regarding e-safety should be made to the e-safety officer who will review the issue and take the appropriate action. For pupils, they are taught to raise any concerns to their class teacher who will then pass this on to the e-safety officer. Complaints of a child protection nature must be dealt with in accordance with our child protection procedure.
Our Designated Safeguarding Lead provides advice and support to other members of staff on protecting children from the risk of on-line radicalisation. The Bridge School ensures staff understand what radicalisation and extremism mean and why people may be vulnerable to being drawn into terrorism. We ensure staff have the knowledge and confidence to identify children at risk of being drawn into terrorism, and to challenge extremist ideas which can be used to legitimise terrorism. Staff safeguard and promote the welfare of children and know where and how to refer children and young people for further help as appropriate by making referrals as necessary to Channel.

Assessing Risks: We will take all reasonable precautions to prevent access to inappropriate material. However, due to the international scale and linked nature of internet content, it is not possible to guarantee that unsuitable material will never appear on a computer connected to the school network. The school cannot accept liability for any material accessed, or any consequences of Internet access.

Emerging technologies, such as mobile phones with internet access (smartphones) are not governed by the school's infrastructure and bypass any and all security and filtering measures that are or could be deployed.

- We will audit ICT use to establish if the e-Safety policy is sufficiently robust and that the implementation of the e-safety policy is appropriate and effective.
- Methods to identify, assess and minimise risks will be reviewed regularly.
- Emerging technologies will be examined by the Head for educational benefit and a risk assessment will be carried out before use in school is allowed.
- Any person not directly employed by the school

23. Equal Opportunities

Students with additional needs

The school endeavours to create a consistent message with parents for all students and this in turn should aid establishment and future development of the schools' eSafety rules. However, staffs are aware that some students may require additional teaching including reminders, prompts and further explanation to reinforce their existing knowledge and understanding of eSafety issues.

Where a student 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.

Parental Involvement

- Parents/carers and students are actively encouraged to contribute to adjustments or reviews of the school eSafety policy by discussion through information events and annual questionnaires.
- 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).
- 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

24. Writing and Reviewing this Policy

Review Procedure

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

This policy will be reviewed annually 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.

Add the policy on taking photos at school events but make it clear they are not to be shared on the public domain eg internet

Acceptable use Agreement: Staff, Management Committee Members and Visitors Staff, Management Committee and Visitor Acceptable use Agreement / Code of Conduct

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.

- 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 or Management Committee.
- 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 students 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 students.
- I will only use the approved, secure email system(s) for any school business.
- I will ensure that all data regarding students and staff, financial information and any information classified as confidential (including all data held on SIMS) is kept secure and is used appropriately, whether in school, taken off the school premises or accessed remotely. Student / teacher / any school confidential data can only be taken out of school or accessed remotely away from school when authorised by the Head.
- I will not save any documents to a non-school PC or print to a non-school printer.
- I will not install any hardware of software without permission of the Headteacher.
- I will not browse, download, upload or distribute any material that could be considered offensive, illegal or discriminatory.
- Images of students and/ or staff will only be taken, stored and used for professional purposes inline 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 Headteacher.
- 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 the Headteacher.
- 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 e-Safety policy and help students 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

Signature ……..…… Date …….

Full Name ……(printed) Job title…….

e-Safety Rules

These e-Safety Rules help to protect students and the school by describing acceptable and unacceptable computer use.

- ✓ **I will only use ICT in school for school purposes.**
- ✓ **I will only use my class email address when emailing.**
- ✓ **I will only open email attachments from people I know, or who staff have approved.**
- ✓ **I will only open/delete my own files.**
- ✓ **I will make sure that all ICT contact with other pupils and adults is responsible, polite and sensible.**
- ✓ **I will not deliberately look for, save or send anything that could be racist, sexist, and homophobic or could be used for bullying purposes. If I accidentally find anything like this I will tell staff 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 unless this is part of a school project approved by my teacher and a responsible adult comes with me.**
- ✓ **I will be responsible for my behaviour when using ICT because I know that these rules are to keep me safe.**
- ✓ **I know that my use of ICT can be checked and that my parent/ carer contacted if a member of school staff is concerned about my eSafety.**

The school may exercise its right to monitor the use of the school's computer systems, including access to web-sites, the interception of e-mail and the deletion of inappropriate materials where it believes unauthorised use of the school's computer system may be taking place, or the system may be being used for criminal purposes or for storing unauthorised or unlawful text, imagery or sound.

ICT including the internet, learning platforms, email and mobile technologies have become an important part of learning in our school. We expect all pupils to be safe and responsible when using any ICT. It is essential that pupils are aware of eSafety and know how to stay safe when using any ICT.

Pupils are expected to read and discuss this agreement with their parent or carer and then to sign and follow the terms of the agreement. Any concerns or explanation can be discussed with their class teacher or The Bridge School's eSafety coordinator.

Student Signature:_____

Parent Signature: _____

Date: _____

25. School Incident Log

'School name' **eSafety Incident Log**

Details of ALL eSafety incidents to be recorded by the eSafety Coordinator. This incident log will be monitored termly by the Headteacher, Member of SLT or Chair of Governors. Any incidents involving Cyberbullying should be recorded on the 'Integrated Bullying and racist Incident Record Form 2'

Date & time	Name of pupil or staff member	Male or Female	Room and computer/ device number	Details of incident (including evidence)	Actions and reasons

26. Current Legislation (date)

Acts relating to monitoring of email

Users of this list should note that legislation is open to change and should always verify that the references and versions given or linked are up to date before relying on them.

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.