Tring School

E-Safety Policy

Policy Date: March 2016

Issue No: 2

Approved by: Governing Body April 2016 *(Students, Learning & Community Committee)*

Date: April 2016

Review due: April 2018

Recommended Good Practice: *HFL eSafety and Data Security Jan 2016*

Tring School

School Policy for eSafety and Data Security

Based on the Hertfordshire model for eSafety and Data Security

Contents

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).

INTRODUCTION

IT 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 lifelong learning and employment.

Information and Communications Technology (ICT) 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
- Email and Instant Messaging
- Chat Rooms and Social Networking
- Blogs and Wikis
- Podcasting
- Video Broadcasting and sharing
- Downloading
- Twitter and facebook
- Gaming
- Mobile/ Smart phones with text, video and web functionality
- Other mobile devices with web functionality such as tablets and gaming machines
- On-demand TV and video, movies and radio/smart TVs

While 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 and that some have minimum age requirements (13 years in most cases).

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

Tring School hold personal data on learners, staff and others to help us conduct our day-to-day activities. Some of this information is sensitive and could be used by another person or criminal organisation to cause harm or distress to an individual. The loss of sensitive information can result in media coverage, and potentially damage the reputation of the school.

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

Both this policy and the Acceptable Use Agreement are inclusive of: both fixed and mobile internet; technologies provided by the school (such as PCs, laptops, tablets, webcams, whiteboards, voting systems, digital video equipment, etc); and technologies owned by students and staff, but brought onto school premises (such as laptops, mobile phones, gaming devices and tablets, etc).

ROLES AND RESPONSIBILITIES

As eSafety 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. The named eSafety co-ordinator in our school is **Mr Barlow** 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 HCC, Herts for Learning Ltd, CEOP (Child Exploitation and Online Protection) and Childnet.

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

This policy, supported by the school's Acceptable Use Agreements for staff, Governors, visitors and pupils, is used to protect the interests and safety of the whole school community. It is linked to the following mandatory school policies: Child Protection; Health and Safety; Behaviour; Anti-bullying; and PHSE; and by Home–school Agreements.

ESAFETY SKILLS DEVELOPMENT FOR STAFF

- Our staff receive information on eSafety issues in the form of training opportunities, in-house communications and via our website.
- New staff receive information on the school's eSafety 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).
- Our staff, Governors and visitors (if appropriate) all agree to an Acceptable Use Policy (AUP).
- All staff are encouraged to incorporate eSafety activities and awareness within their curriculum areas as appropriate.

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 will be part of our Lifeskills and assembly programme.
- E-safety posters will be prominently displayed around the school's ICT facilities.
- E-safety has its own distinct section on the school's website.
- The school will provide e-safety evenings for the community on a bi-yearly basis.

ESAFETY IN THE CURRICULUM

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

- The school has a framework for teaching eSafety as part of the Lifeskills programme.
- The school has a framework for teaching internet skills in ICT lessons in year 7.
- The school provides opportunities within a range of curriculum areas to teach about eSafety.
- Educating students on the dangers of technologies that may be encountered outside school is done informally when opportunities arise and as part of the eSafety curriculum.
- Students 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.
- 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.
- Students are taught to critically evaluate materials and learn good searching skills through cross curricular teaching.

MONITORING

Authorised IT staff may inspect any IT equipment owned or leased by the school at any time without prior notice. If you are in doubt as to whether the individual requesting such access is authorised to do so, please ask for their identification badge and contact Mrs Gower or Mr Barlow. Any IT authorised staff member will be happy to comply with this request.

IT authorised staff may monitor, intercept, access, inspect, record and disclose telephone calls, emails, instant messaging, internet/intranet use and any other electronic communications (data, voice, video or image) involving the school's employees or contractors, without consent, to the extent permitted by law. This may be: to confirm or obtain school business related information; to confirm or investigate compliance with school policies, standards and procedures; to ensure the effective operation of school IT; for quality control or training purposes; to comply with a Subject Access Request under the Data Protection Act 1998; or to prevent or detect crime.

IT authorised staff may, without prior notice, access the email or voicemail account where applicable, of someone who is absent in order to deal with any business-related issues retained on that account.

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

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

BREACHES

A breach or suspected breach of policy by a school employee, contractor or pupil may result in the temporary or permanent withdrawal of school IT hardware, software or services from the offending individual.

For staff any policy breach is grounds for disciplinary action in accordance with the school Disciplinary Procedure or, for Support Staff, in their Probationary Period as stated.

Policy breaches may also lead to criminal or civil proceedings.

The Information Commissioner’s powers to issue monetary penalties came into force on 6 April 2010, allowing the Information Commissioner‘s office to serve notices requiring organisations to pay up to £500,000 for serious breaches of the Data Protection Act.

The data protection powers of the Information Commissioner’s Office are to:

· Conduct assessments to check organisations are complying with the Act;

· Serve information notices requiring organisations to provide the Information Commissioner’s Office with specified information within a certain time period;

· Serve enforcement notices and ‘stop now’ orders where there has been a breach of the Act, requiring organisations to take (or refrain from taking) specified steps in order to ensure they comply with the law;

· Prosecute those who commit criminal offences under the Act;

· Conduct audits to assess whether organisations’ processing of personal data follows good practice,

· Report to Parliament on data protection issues of concern

For pupils, reference will be made to the school’s Behaviour Policy.

INCIDENT REPORTING

Any security breaches or attempts, loss of equipment and any unauthorised use or suspected misuse of ICT must be immediately reported to the school’s relevant responsible person. Additionally, all security breaches, lost/stolen equipment or data (including remote access Secure ID tokens and PINs), virus notifications, unsolicited emails, misuse or unauthorised use of ICT and all other policy non-compliance must be reported to the relevant responsible person. The relevant responsible individuals in the school are as follows: Mrs D Gower.

Please refer to the relevant section on Incident Reporting, eSafety Incident Log & Infringements.

COMPUTER VIRUSES

- All files downloaded from the Internet, received via email or on removable media such as a memory stick must be checked for any viruses using school provided anti-virus software before being used.
- Never interfere with any anti-virus software installed on school ICT equipment.
- If your machine is not routinely connected to the school network, you must make provision for regular virus updates through your IT team.
- If you suspect there may be a virus on any school ICT equipment, stop using the equipment and contact your ICT support provider immediately. The ICT support provider will advise you on what actions to take and be responsible for advising others that need to know.

PASSWORD SECURITY

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

- All users read and agree to an Acceptable Use Agreement to demonstrate that they have understood the school's e-Safety Policy.
- Our staff agree to our AUP.
- Users are provided with an individual network log-in username. From Year 7 they are also expected to use a personal password and keep it private.
- Students are not allowed to deliberately access on-line materials or files on the school network, of their peers, teachers or others.
- If students think another person knows their password then they know how to reset it or they can ask their teacher or a member of the IT staff.
- Staff are aware of their individual responsibilities to protect the security and confidentiality of school networks, MIS systems and VLE, 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.
- In our school, all ICT password policies are the responsibility of the Network Manager and all staff and students are expected to comply with the policies at all times.

DATA SECURITY

Data Protection: key responsibilities for School Heads and Governors

The accessing and appropriate use of school data is taken very seriously. HCC guidance documents can be found at:

http://www.thegrid.org.uk/info/dataprotection/index.shtml#data

- Staff are aware of their responsibility when accessing school data. Level of access is determined by the person's job.
- The school gives relevant staff access to its Management Information System, with a unique username and password.
- It is the responsibility of everyone to keep passwords secure.
- It is the responsibility of individual staff to ensure the security of any personal or sensitive information contained in documents faxed, copied, scanned or printed. This is particularly important when shared copiers (multi-function print, fax, scan and copiers) are used.
- Staff should always keep all school-related data secure. This includes all personal, sensitive, confidential or classified data.

- Anyone sending a confidential or sensitive fax should notify the recipient before it is sent
- To comply with the DPA all pupil data is stored and accessed within the schools network. To access the network a complex password is required.
- Any data taken off the school premises must be encrypted if stored on a removable device.
- All remote access to data is via Sims Learning Gateway or VPN.

MANAGING THE INTERNET

The internet is an open communication medium, available to all. 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 school network by pupils is logged and the logs are randomly but regularly monitored. Whenever any inappropriate use is detected it will be followed up.

- The school students will have supervised access to internet resources (where reasonable) through the school's fixed and mobile internet technology.
- Staff will preview any recommended online services, software, sites and apps before use.
- 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.

- School internet access is controlled through our web filtering service (provided by Hertfordshire) and Securus (a bespoke package designed to monitor the school's internet traffic and flag up misuse or concerns)
- Tring 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.
- 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 discover an unsuitable site, the screen must be switched off and the incident reported immediately to the e-Safety Co-ordinator.
- If students discover an unsuitable site, the screen must be switched off and the incident reported immediately to the teacher.
- 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 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's responsibility, nor the network manager's, to install or maintain virus protection on personal systems
- Students are not permitted to download programs on school-based technologies.
- If there are any issues related to viruses or anti-virus software, the network manager should be informed via the call logging system for staff or via teachers for students.

MANAGING OTHER ONLINE TECHNOLOGIES

Online technologies, including social networking sites, if used responsibly, both outside and within an educational context, can provide easy-to-use, creative, collaborative and free facilities. However, it is important to recognise that there are issues regarding the appropriateness of some content, contact, culture and commercialism. To this end, we encourage our 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.
- 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 should not use the internet or web-based communication channels to send personal messages to children/young people.
- Staff should be aware of information that they are putting into the public domain (Facebook, Snapchat, Twitter, YouTube, etc). Staff should not allow children or young people to be listed as their ‘friends’ and should not allow themselves to be listed as ‘friend’ on students’ sites.

MOBILE TECHNOLOGIES

Many emerging technologies offer new opportunities for teaching and learning, including a move towards personalised learning and 1:1 device ownership for students. Many existing mobile technologies such as tablets, gaming devices and mobile 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

- The school allows staff to bring in personal mobile phones and devices for their own use.
- This technology may be used, however, for educational purposes, as mutually agreed with the teacher. Sixth Form students can bring in their own devices for educational purposes.
- Pupils are allowed to bring personal mobile devices/phones to school but must not use them for personal purposes within lesson time. At all times the device must be switched onto silent.
- This technology may be used for educational purposes, as mutually agreed with the Headteacher. The device user, in this instance, must always ask the prior permission of the bill payer.
- The school is not responsible for the loss, damage or theft of any personal mobile device.
- The sending of inappropriate electronic messages between any members 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

- The sending of inappropriate electronic 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.
- 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 school gives all staff and students 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 their 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 or parents, or conduct any school business, using any personal communication methods, e.g. email address, social networking, Twitter, video sites etc.
- Email 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 sensitive emails to external organisations, parents or students are advised to cc or bcc their line manager/HOH etc. if they think the issue might be contentious.
- Students may only use school approved accounts on the school system and only under direct teacher supervision for educational purposes.
- The forwarding of chain letters is not permitted in school.
- All email users are expected to adhere to the generally accepted rules of network etiquette, particularly in relation to the use of appropriate language, and not reveal any personal details about themselves or others in email communication, or arrange to meet anyone without specific permission; they should virus check attachments.
- Students must immediately tell a teacher/trusted adult if they receive an offensive email.
- 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 in Year 7.

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. HCC guidance can be found here: https://ico.org.uk/media/for-organisations/documents/1542/cctv-code-of-practice.pdf

- Parents or carers must opt out if they do not want appropriate images of their child to be used within the school or on the website or for promotional material.
- Students must not take or distribute any inappropriate images/audio/video of members of the school community.

CONSENT OF ADULTS WHO WORK AT THE SCHOOL

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

PUBLISHING PUPIL'S IMAGES AND WORK

On a child's entry to the school, all parents/guardians will be asked to opt out if they do not wish their child's work/photos used in the following ways:

- on the school website
- on the school's VLE
- 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, e.g. 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 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 withdrawn, e.g. divorce of parents, custody issues, etc.

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

Email and postal addresses of students will not be published.

For further information relating to issues associated with school websites and the safe use of images in Hertfordshire schools, see http://www.thegrid.org.uk/schoolweb/safety/index.shtml

http://www.thegrid.org.uk/info/csf/policies/index.shtml#images

STORAGE OF IMAGES

- Images/films of children are stored on the school's network and the website.
- Rights of access to this material are restricted to the teaching staff and students within the confines of the school network/VLE.
- The designated person has the responsibility of deleting the images when they are no longer required.

WEBCAMS AND CCTV

For details about the school's use of CCTV, please see the Safeguarding Policy, which is available via the school's website or on request.

VIDEO CONFERENCING

- Parents can opt out of allowing their children to participate in video conferencing.
- 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 keeps a record of video conferences, including date, time and participants.
- Approval from the Headteacher or eSafety Co-ordinator 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 third-party organisations may not be 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.

SOCIAL MEDIA, INCLUDING FACEBOOK AND TWITTER

Facebook, Twitter and other forms of social media are increasingly becoming an important part of our daily lives.

- Our school uses Facebook and Twitter to communicate with parents and carers. Mrs Stubbs & Mrs Gower are responsible for all postings on these technologies and monitors responses from others.
- Staff are discouraged from accessing their personal social media accounts using school equipment.

- Staff are able to set up Social Learning Platform accounts, using their school email address, in order to be able to teach pupils the safe and responsible use of social media.
- Pupils are not permitted to access their social media accounts while at school.
- Pupils in Years XX are permitted to access their personal social media account using their own device (i.e. mobile phone) outside of lessons.
- Staff, Governors, pupils, parents and carers are regularly provided with information on how to use social media responsibly and what to do if they are aware of inappropriate use by others.
- Staff, Governors, pupils, parents and carers are aware that the information, comments, images and video they post online can be viewed by others, copied and stay online for ever.
- Staff, Governors, pupils, parents and carers are aware that their online behaviour should at all times be compatible with UK law.

MISUSE AND INFRINGEMENTS

COMPLAINTS

Complaints relating to eSafety should be made to the eSafety Co-ordinator or Headteacher. Incidents should be logged on SIMS and the Hertfordshire Flowcharts for Managing an eSafety Incident should be followed (see Appendix).

INAPPROPRIATE MATERIAL

- All users are aware of the procedures for reporting accidental access to inappropriate materials. The breach must be recorded on SIMS as an ICT incident. 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 member of staff on SIMS, and, depending on the seriousness of the offence, investigation by the Headteacher/LA and/or immediate suspension, possibly leading to dismissal and involvement of police for very serious offences (see flowchart).

- Users are made aware of sanctions relating to the misuse or misconduct by having an AUA which they agree to every time they log in.

- The school's discipline procedures will be used for all ICT offences.

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 school's eSafety rules.

However, staff 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 and young people.

PARENTAL INVOLVEMENT

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

- Parents/carers and students are actively encouraged to contribute to adjustments or reviews of the school eSafety Policy by placing the policy and AUA on the school website and asking for feedback.
- Parents/carers are required to make a decision as to whether they wish to remove their 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:
    - Website postings
    - Newsletter items
    - Items circulated via Keep Kids Safe

WRITING AND REVIEWING THIS POLICY

STAFF AND STUDENT INVOLVEMENT IN POLICY CREATION

- Staff and students will be involved in the reviewing of the eSafety Policy through the School Council and circulation to all staff for comments and feedback, at the appropriate time.

REVIEW PROCEDURE

- There will be an ongoing opportunity for staff to discuss with the eSafety Co-ordinator any issue of eSafety that concerns them.
- This policy will be reviewed every 24 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.
- This policy has been read, amended and approved by the staff, Headteacher and Governors on 27 April 2016.

ACCEPTABLE USE POLICY: STAFF, GOVERNORS AND VISITORS

Tring School - ICT Acceptable Use Policy / Code of Conduct

ICT (including data) 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 **Nigel Barlow, School eSafety Coordinator**.

- ➢ I will only use the school's email/internet and any related technologies for professional purposes or for uses deemed 'reasonable' by the Head 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, personal Twitter account, or any other social media link, to pupils.
- ➢ I will only use the approved, secure email system(s) for any school business.
- ➢ I will ensure that personal data (such as data held on SIMS) 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 or Governing Body.
- ➢ Personal or sensitive data taken off site must be encrypted, e.g. on a password-secured laptop or memory stick.
- ➢ I will not install any hardware or software without permission of Debbie Gower, Network Manager.
- ➢ 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 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 my Line Manager or Headteacher.
- ➢ I will support the school approach to online safety and not deliberately upload or add any images, video, sounds or text that could upset or offend any member of the school community.
- ➢ 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 and Data Security Policy and help pupils to be safe and responsible in their use of ICT and related technologies.
- ➢ I understand this forms part of the terms and conditions set out in my contract of employment.

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

Additional Guidance:

1) Do not, under any circumstances, reveal your own or any other member of staff's personal email address to students.

2) Do not, under any circumstances, use your own or any other member of staff's, personal email address to communicate with students directly. Email communication with students should be made via your Tring School email address.

3) Do not under any circumstance communicate with students using social networking sites. Do not reveal your use of (or any other member of staff's use of) social networking/gaming or dating sites to students. Be very careful when using public networking sites as students have been known to pose as adults to engage teachers in communication.

4) If you believe you have discovered an incident of, or become a victim of, cyberbullying:

    a. Do not delete or tamper with any evidence. Save it.

    b. Report the incident immediately to the eSafety Coordinator.

5) Consider very carefully before taking images of students. If you take images of students for professional purposes using a personal camera, save the images onto the school network and then delete them from your personal storage. No images of students should be stored on your personal media (computer, phone, camera etc).

6) Managing a blog or wiki as part of the curriculum should be done using Google for Education. Any questions regarding this, see Mr C Lickfold.

7) Filtering (the blocking of some websites) is done to steer students away from sites where they could be vulnerable. Filtering is NOT 100% effective and is no substitute for staff vigilance. You have a responsibility to monitor and dissuade students from accessing non-educational sites during the school day. You must report any students accessing non-educational sites to the ICT Support Team for disciplinary action to be taken.

8) You have a responsibility to ensure that media brought into or sent into school is virus-checked before uploading to the school network. If you are unsure about this, please contact the ICT Support Team.

9) You are responsible for ensuring you comply with the licensing arrangements for any programs installed on the school computers.

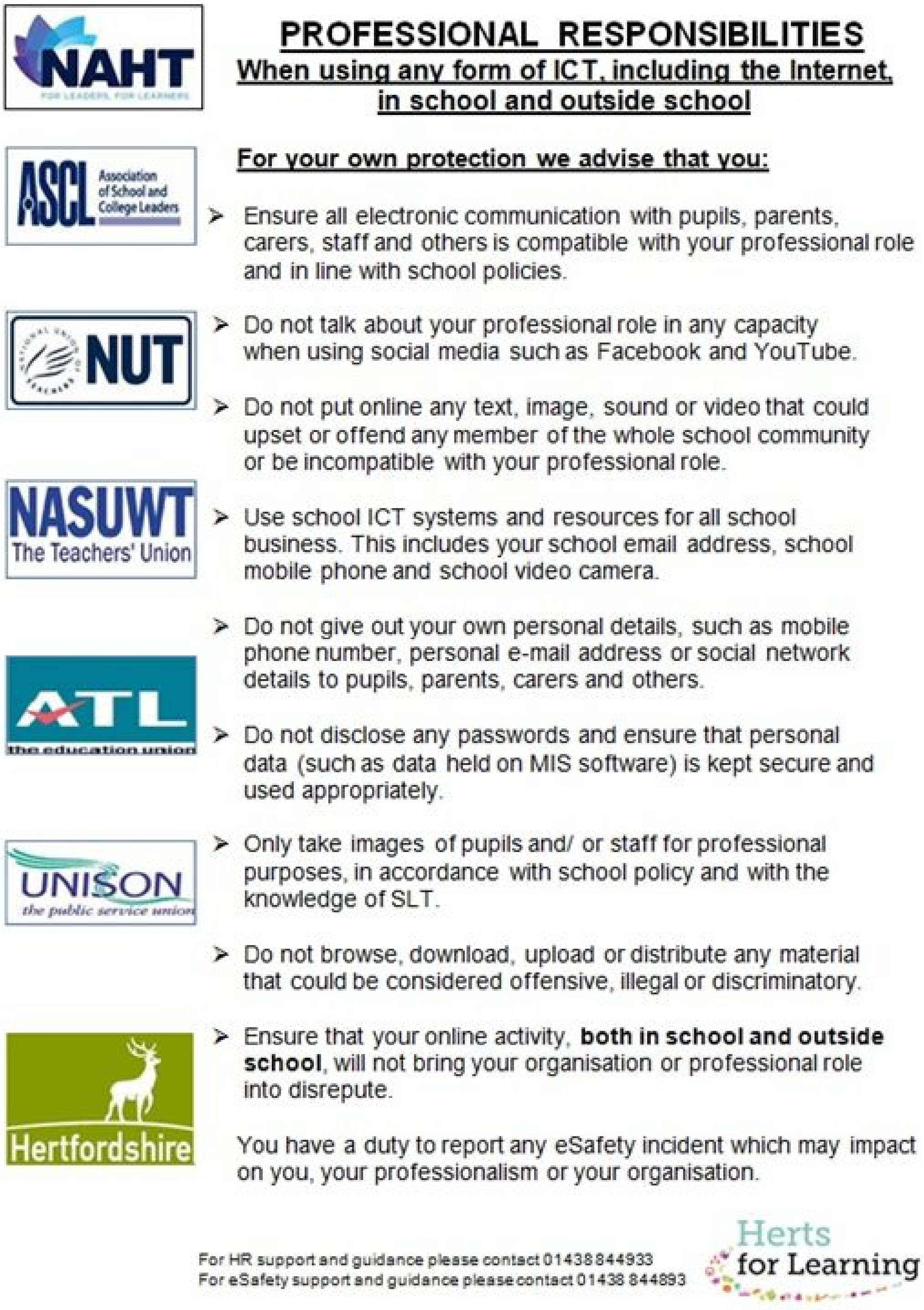
10) Do not allow students or other adults to use your user id(s).

11) Monitor and ensure that when students log on, they use their own user ids.

12) You will be held responsible for actions carried out using your personal user ids.

Staff Professional Responsibilities:

13) The HSCB eSafety subgroup group have produced a clear summary of professional responsibilities related to the use of ICT which has been endorsed by unions. To download visit http://www.thegrid.org.uk/eservices/safety/policies.shtml



PROFESSIONAL RESPONSIBILITIES

When using any form of ICT, including the Internet, in school and outside school

For your own protection we advise that you:

- Ensure all electronic communication with pupils, parents, carers, staff and others is compatible with your professional role and in line with school policies.
- Do not talk about your professional role in any capacity when using social media such as Facebook and YouTube.
- Do not put online any text, image, sound or video that could upset or offend any member of the whole school community or be incompatible with your professional role.
- Use school ICT systems and resources for all school business. This includes your school email address, school mobile phone and school video camera.
- Do not give out your own personal details, such as mobile phone number, personal e-mail address or social network details to pupils, parents, carers and others.
- Do not disclose any passwords and ensure that personal data (such as data held on MIS software) is kept secure and used appropriately.
- Only take images of pupils and/ or staff for professional purposes, in accordance with school policy and with the knowledge of SLT.
- Do not browse, download, upload or distribute any material that could be considered offensive, illegal or discriminatory.
- Ensure that your online activity, **both in school and outside school**, will not bring your organisation or professional role into disrepute.

You have a duty to report any eSafety incident which may impact on you, your professionalism or your organisation.

For HR support and guidance please contact 01438 844933
For eSafety support and guidance please contact 01438 844893

ACCEPTABLE USE POLICY: STUDENTS

Tring School – Pupil ICT Acceptable Use Agreement

ICT and the related technologies such as the internet form an important part of learning in our school. We expect all pupils to be responsible for their behaviour when using ICT and the internet. It is essential that pupils are aware of eSafety and know how to stay safe when using any ICT.

Tring School students are expected to agree and follow the eSafety Rules. Any concerns or explanation can be discussed with Mr Barlow, Tring School eSafety Co-ordinator, or Mrs Gower, Network Manager. If you, your parent or carer would like a copy of this policy it can be downloaded from the Tring School website.

ICT and the related technologies such as email, the internet and mobile phones are an expected part of our daily working life in school. You are expected to agree to the AUP Policy and adhere at all times to its contents.

You must not use the Tring School network to download or share copyright content without permission of the copyright owner. To do so may result in legal sanctions, network termination or both.

You have been provided access to Tring School computer facilities and to the school-wide communication network and you must assume responsibility for their appropriate use. Tring School expects you to be careful, responsible, honest and polite in the use of computers, communications and the Tring School network. Those of you who use the internet to communicate with individuals or
other institutions are expected to abide by the rules laid down in law and those set out in Tring Schools AUPs and policies.

By logging on to any of the school's IT systems/facilities you are automatically agreeing to the terms and conditions of the school's Acceptable Use Policy.

- I will only use IT systems in school including the internet, email, digital video, mobile technologies etc for school purposes.
- I will not download or install software on school technologies.
- I will only log on to the school network, other systems and resources with my own user name and password.
- I will follow the schools ICT security system and not reveal my passwords to anyone.
- I will only use my school email to send and receive emails to and from students and staff within school. I will not use my personal email account in school with the exception of UCAS applications.
- I will make sure that all ICT communications with pupils, teachers or others is responsible and sensible.
- I know it is essential that I keep my email account password private. I know I will be held responsible for any emails sent from my account.
- I will not deliberately browse, download or upload material that could be considered offensive or illegal. If I accidentally come across any such material I will report it immediately to my teacher.

- I will not give out any personal information such as name, phone number or address. I will not arrange to meet someone unless this is part of a school project approved by my teacher.
- I am aware that when I take images of pupils and/or staff, I must only store and use these for school purposes in line with school policy and must never distribute these outside the school network without the permission of all parties involved. This includes school breaks and all occasions when I am in school uniform or when otherwise representing the school.
- I will ensure that my online activity, both in school and outside school, will not cause my school, the staff, pupils or others distress or bring the school community into disrepute, including through uploads of images, video, sounds or texts.
- I will respect the privacy and ownership of others' work online at all times.
- I will support the school approach to online safety and not deliberately upload or add any images, video, sounds or text that could upset or offend any member of the school community.
- I understand that all my use of the internet and other related technologies can be monitored and logged and can be made available to my teachers.
- I will not attempt to bypass the internet filtering system.
- I understand that these rules are designed to keep me safe and that if they are not followed, school sanctions will be applied and my parent/carer may be contacted.
- I will not bring a Smart Watch to school because I am not permitted to wear one during the school day.
- I will not sign up to online services until I am old enough to do so.

Parent and pupil signatures

Dear Parent/Carer

ICT, including the internet, email, mobile technologies and online resources, has 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/carer and then to sign and follow the terms of the agreement. Any concerns or explanation can be discussed with Mr Barlow, eSafety Co-ordinator.

Please return the bottom section of this form which will be kept on record at the school.

We have discussed this policy and ....(pupil name) agrees to follow the eSafety Rules and to support the safe use of ICT at Tring School.

Parent/ Carer Signature ....

Pupil Signature ....

Form .... Date ....

Guidance:

1) Use of any recording devices (mobile phones, digital cameras, etc) during the school day is prohibited, unless sanctioned by a member of staff.

2) Do not, under any circumstances, reveal your school password(s) to any other person. If you think your user id and password is being used by someone else, change your password and contact the IT Technicians as soon as possible. You will be held responsible for actions carried out on the network using your personal user ids.

3) Any email communications between pupils and school staff should be made using the Tring School email system. username@tringschool.org.

4) If you believe you have discovered an incident of, or become a victim of, cyberbullying:

    a. Do not delete or tamper with any evidence. Save it.

    b. Report the incident immediately to the eSafety Coordinator or any member of staff.

5) Consider very carefully before uploading images or video of other students onto the internet. Check that they do not mind the images being posted and it is good practice not to make the images publicly available, i.e. restrict access to them to your immediate friends. Posting images on the internet against a person's consent can be considered as bullying.

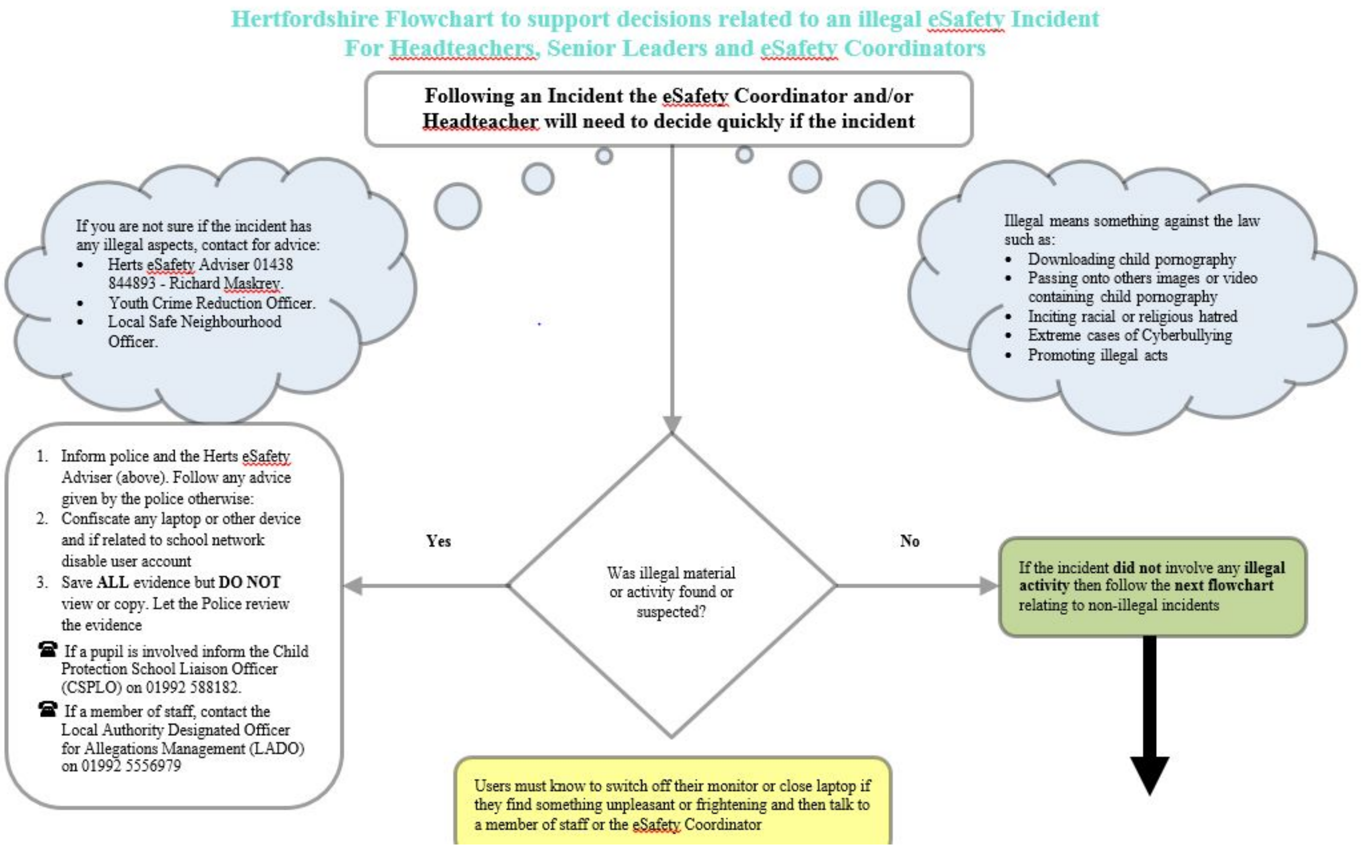
6) Filtering (the blocking of some websites) in school is done to steer students away from sites where they could be vulnerable. The use of gaming and social networking is not permitted using the school network. If you are caught accessing these sites you may face disciplinary action.

7) You have a responsibility to ensure that any files or media brought into or sent into school is virus-checked before uploading to the school network. If you are unsure about this, please contact an ICT Technician.

8) You will be allocated a small amount of space on the school network to store your work. It is your responsibility to delete old work and to manage this space. Google Drive should be used to store your work so it is easily available across devices.

Individuals should not attempt to exploit, test or probe for suspected security holes on Tring School computers or Networks but should report them to the Tring School IT Technical Team.

FLOWCHARTS FOR MANAGING AN E-SAFETY INCIDENT



Hertfordshire Flowchart to support decisions related to an illegal eSafety Incident
For Headteachers, Senior Leaders and eSafety Coordinators

Following an Incident the eSafety Coordinator and/or Headteacher will need to decide quickly if the incident

If you are not sure if the incident has any illegal aspects, contact for advice:

- Herts eSafety Adviser 01438 844893 - Richard Maskrey.
- Youth Crime Reduction Officer.
- Local Safe Neighbourhood Officer.

Illegal means something against the law such as:

- Downloading child pornography
- Passing onto others images or video containing child pornography
- Inciting racial or religious hatred
- Extreme cases of Cyberbullying
- Promoting illegal acts

Was illegal material or activity found or suspected?

Yes

1. Inform police and the Herts eSafety Adviser (above). Follow any advice given by the police otherwise:
2. Confiscate any laptop or other device and if related to school network disable user account
3. Save **ALL** evidence but **DO NOT** view or copy. Let the Police review the evidence

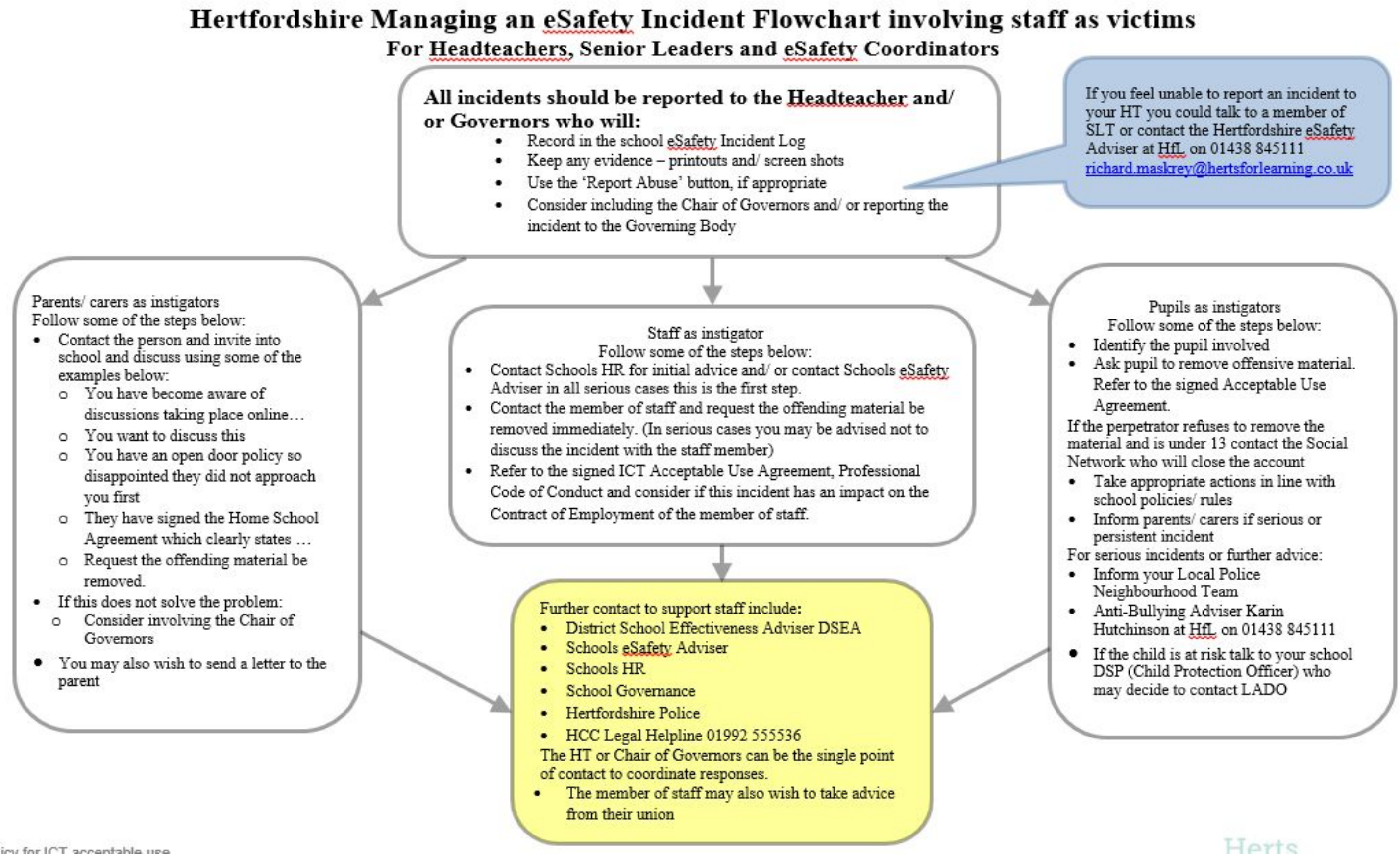
☎ If a pupil is involved inform the Child Protection School Liaison Officer (CSPLO) on 01992 588182.

☎ If a member of staff, contact the Local Authority Designated Officer for Allegations Management (LADO) on 01992 5556979

No

If the incident **did not** involve any **illegal activity** then follow the **next flowchart** relating to non-illegal incidents

Users must know to switch off their monitor or close laptop if they find something unpleasant or frightening and then talk to a member of staff or the eSafety Coordinator



Hertfordshire Managing an eSafety Incident Flowchart involving staff as victims
For Headteachers, Senior Leaders and eSafety Coordinators

All incidents should be reported to the Headteacher and/ or Governors who will:

- Record in the school eSafety Incident Log
- Keep any evidence – printouts and/ screen shots
- Use the 'Report Abuse' button, if appropriate
- Consider including the Chair of Governors and/ or reporting the incident to the Governing Body

If you feel unable to report an incident to your HT you could talk to a member of SLT or contact the Hertfordshire eSafety Adviser at HfL on 01438 845111 richard.maskrey@hertsforlearning.co.uk

Parents/ carers as instigators
Follow some of the steps below:

- Contact the person and invite into school and discuss using some of the examples below:
  - You have become aware of discussions taking place online…
  - You want to discuss this
  - You have an open door policy so disappointed they did not approach you first
  - They have signed the Home School Agreement which clearly states …
  - Request the offending material be removed.
- If this does not solve the problem:
  - Consider involving the Chair of Governors
- You may also wish to send a letter to the parent

Staff as instigator
Follow some of the steps below:

- Contact Schools HR for initial advice and/ or contact Schools eSafety Adviser in all serious cases this is the first step.
- Contact the member of staff and request the offending material be removed immediately. (In serious cases you may be advised not to discuss the incident with the staff member)
- Refer to the signed ICT Acceptable Use Agreement, Professional Code of Conduct and consider if this incident has an impact on the Contract of Employment of the member of staff.

Pupils as instigators
Follow some of the steps below:

- Identify the pupil involved
- Ask pupil to remove offensive material. Refer to the signed Acceptable Use Agreement.

If the perpetrator refuses to remove the material and is under 13 contact the Social Network who will close the account

- Take appropriate actions in line with school policies/ rules
- Inform parents/ carers if serious or persistent incident

For serious incidents or further advice:

- Inform your Local Police Neighbourhood Team
- Anti-Bullying Adviser Karin Hutchinson at HfL on 01438 845111
- If the child is at risk talk to your school DSP (Child Protection Officer) who may decide to contact LADO

Further contact to support staff include:

- District School Effectiveness Adviser DSEA
- Schools eSafety Adviser
- Schools HR
- School Governance
- Hertfordshire Police
- HCC Legal Helpline 01992 555536

The HT or Chair of Governors can be the single point of contact to coordinate responses.

- The member of staff may also wish to take advice from their union

Disposal of Redundant ICT Equipment Policy

- All redundant ICT equipment will be disposed of through an authorised agency. This should include a written receipt for the item including an acceptance of responsibility for the destruction of any personal data.
- All redundant ICT equipment that may have held personal data will have the storage media overwritten multiple times to ensure the data is irretrievably destroyed. Or, if the storage media has failed, it will be physically destroyed. We will only use authorised companies who will supply a written guarantee that this will happen.
- Disposal of any ICT equipment will conform to:

The Waste Electrical and Electronic Equipment Regulations 2006

The Waste Electrical and Electronic Equipment (Amendment) Regulations 2007

http://www.environment-agency.gov.uk/business/topics/waste/32084.aspx

http://www.opsi.gov.uk/si/si2006/uksi_20063289_en.pdf

http://www.opsi.gov.uk/si/si2007/pdf/uksi_20073454_en.pdf?lang=_e

Data Protection Act 1998

https://ico.org.uk/for-organisations/education/

Electricity at Work Regulations 1989

http://www.opsi.gov.uk/si/si1989/Uksi_19890635_en_1.htm

- The school will maintain a comprehensive inventory of all its ICT equipment including a record of disposal.
- The school’s disposal record will include:
  - Date item disposed of
  - Authorisation for disposal, including:
    - verification of software licensing
    - any personal data likely to be held on the storage medium?*
  - How it was disposed of, e.g. waste, gift, sale
  - Name of person and/or organisation who received the disposed item

* if personal data is likely to be held the storage medium will be overwritten multiple times to ensure the data is irretrievably destroyed.

- Any redundant ICT equipment being considered for sale/gift will have been subject to a recent electrical safety check and hold a valid PAT certificate.

Further information available at:

Waste Electrical and Electronic Equipment (WEEE) Regulations

Environment Agency website

Introduction

http://www.environment-agency.gov.uk/business/topics/waste/32084.aspx

The Waste Electrical and Electronic Equipment Regulations 2006

http://www.opsi.gov.uk/si/si2006/uksi_20063289_en.pdf

The Waste Electrical and Electronic Equipment (Amendment) Regulations 2007

http://www.opsi.gov.uk/si/si2007/pdf/uksi_20073454_en.pdf?lang=_e

Information Commissioner website

https://ico.org.uk/

Data Protection Act – data protection guide, including the 8 principles

https://ico.org.uk/for-organisations/education/

PC Disposal – SITSS Information

http://www.thegrid.org.uk/info/traded/sitss/services/computer_management/pc_disposal

CURRENT LEGISLATION

ACTS RELATING TO MONITORING OF STAFF EMAIL

Data Protection Act 1998

The Act requires anyone who handles personal information to comply with important data protection principles when treating personal data relating to any living individual. The Act grants individuals rights of access to their personal data, compensation and prevention of processing. http://www.hmso.gov.uk/acts/acts1998/19980029.htm

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

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

Regulation of Investigatory Powers Act 2000

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

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

Human Rights Act 1998

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

OTHER ACTS RELATING TO ESAFETY

Racial and Religious Hatred Act 2006

It a criminal offence to threaten people because of their faith, or to stir up religious hatred by displaying, publishing or distributing written material that 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 the document 'Children & Families: Safer from Sexual Crime' as part of their child protection packs.

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)
- gain 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 the 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.