Watford Grammar School for Boys

School Policy for eSafety

Based on the Hertfordshire model for eSafety

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) and Becta guidance.

INTRODUCTION

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

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

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

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

At Watford Grammar School for Boys, 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.

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, 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 (such as laptops, mobile phones, camera phones, PDAs and portable media players, 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 Carr 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 Herts LA, Becta, CEOP (Child Exploitation and Online Protection) and Childnet.

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

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

eSAFETY SKILLS DEVELOPMENT FOR STAFF

- Our staff receive information on eSafety issues in the form of emails and the VLE
- 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 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.
- The e-safety policy will be introduced to the students at the start of each school year.
- E-safety posters will be prominently displayed.

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 PSHE programme.
- The school has a framework for teaching internet skills in ICT lessons and this is available on the VLE
- The school provides opportunities within a range of curriculum areas to teach about eSafety.
- 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 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 teacher models, discussions and via the ICT curriculum, i.e. in the Year 7 Internet option and Year 8 HTML unit.

PASSWORD SECURITY

Password security is essential for staff, particularly as they are able to access and use pupil data. Staff are expected to have secure passwords which are not shared with anyone. The 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 an 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 support 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

The accessing and appropriate use 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. Level of access is determined by the persons Job.
- 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. Most data is stored in SIMs which is password protected, although some data is stored in external databases for use with the online reporting system and IEPs (Individual Learning Plans) are stored on a shared drive.
- Any data taken off the school premises must be encrypted if stored on a removable device. The encryption software used is TrueCrypt.
- All remote access to data is via HTTPs

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 maintains 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.
- All users must observe software copyright at all times. It is illegal to copy or distribute school software or illegal software from other sources.
- All users must observe copyright of materials from electronic resources.

INFRASTUCTURE

- School internet access is controlled through our web filtering service and PCE
- Watford Grammar School for Boys 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 WEB 2 TECHNOLOGIES

Web 2, 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, Myspace, 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 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.

PERSONAL MOBILE DEVICES (INCLUDING PHONES)

- The school allows staff to bring in personal mobile phones and devices for their own use.
- Staff must ensure that all personal digital devices that are used to access school data, such as email and SIMs have appropriate security enabled.
- Students are discouraged from bringing mobile phones and devices into school. If they do bring them then they must be switched onto silent at all times.
- This technology may be used, however for educational purposes, as mutually agreed with the teacher. 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 text messages between any member of the school community is not allowed.
- Permission must be sought before any image or sound recordings are made on these devices of any member of the school community.
- Users bringing personal devices into school must ensure there is no inappropriate or illegal content on the device.

SCHOOL PROVIDED MOBILE DEVICES (INCLUDING PHONES)

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

MANAGING EMAIL

The use of email within most schools is an essential means of communication for staff. 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 within school or international. In order to achieve ICT level 4 or above, students must have experienced sending and receiving emails.

- The school gives all staff their own email account to use for all school business. This is to minimise the risk of receiving unsolicited or malicious emails and avoids the risk of personal profile information being revealed.
- It is the responsibility of each account holder to keep the password secure. For the safety and security of users and recipients, all mail is filtered and logged; if necessary email histories can be traced. This should be the account that is used for all school business.
- Under no circumstances should staff contact students, parents or conduct any school business using any personal communication methods, e.g. email address, social networking, twitter, video sites etc.
- 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 sensitive emails to external organisations, parents or students are advised to cc or bcc their line manager/ HOY 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 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.

SAFE USE OF IMAGES

TAKING OF IMAGES AND FILM

Digital images are easy to capture, reproduce and publish and, therefore, misused.

- Parents or carers must opt out if they do not want appropriate images of their son to be used within the school or on the web site 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 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, i.e. exhibition promoting the school
- general media appearances, e.g. local/ national media/ press releases sent to the press highlighting an activity (sent using traditional methods or electronically)

This consent 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 an issue, eg divorce of parents, custody issues, etc.

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

E-mail 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 web site
- Rights of access to this material are restricted to the teaching staff and students within the confines of the school network/ Learning Platform.
- Effie Stevenson has the responsibility of deleting the images when they are no longer required.

WEBCAMS AND CCTV

For details of this section please see the related document "CCTV SYSTEM POLICY" on the school VLE.

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 Headmaster 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 3rd 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.

MISUSE AND INFRINGEMENTS

COMPLAINTS

Complaints relating to eSafety should be made to the eSafety co-ordinator or Headmaster. 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.
- Deliberate access to inappropriate materials by any user will lead to the incident being logged by the member of staff on SIMs, depending on the seriousness of the offence; investigation by the Headmaster/ LA, 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 login.
- The schools 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 schools' 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 pupil has poor social understanding, careful consideration is given to group interactions when raising awareness of eSafety. Internet activities are planned and well managed for these children and young people.

PARENTAL INVOLVEMENT

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/ Learning Platform postings
    - Newsletter items
    - Learning platform training

WRITING AND REVIEWING THIS POLICY

STAFF AND PUPIL INVOLVEMENT IN POLICY CREATION

- Staff and students have been involved in making/ reviewing the eSafety policy through the school council and circulation to all staff for comments and feedback.

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 every (12) months and consideration given to the implications for future whole school development planning.
- The policy will be amended if new technologies are adopted or Central Government change the orders or guidance in any way.
- This policy has been read, amended and approved by the staff, head teacher and governors on …….

ACCEPTABLE USE AGREEMENT: STAFF

Staff, 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 Richard Carr 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 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 students and staff are compatible with my professional role.
- I will not give out my own personal details, such as mobile phone number, social networking username, twitter account and personal email address, to students unless sanctioned by the Headmaster. Nor will I use any of the above for personal communication with students unless sanction by the Headmaster.
- 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 taken offsite should only be done using an encrypted portal device.
- I will not install any hardware of software without permission of the Network Manager or eSafety Co-ordinator
- 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.
- 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 Headmaster.
- I will respect copyright and intellectual property rights.
- I will not bring into school any illegal content, including pirated songs, movies, software, offensive material and will not try and share or distribute it further.
- I will ensure that my online activity, both in school and outside school, will not bring my professional role into disrepute. This will include for example, posts on social networking sites, video and photo publishing and sharing sites.
- 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 agreement

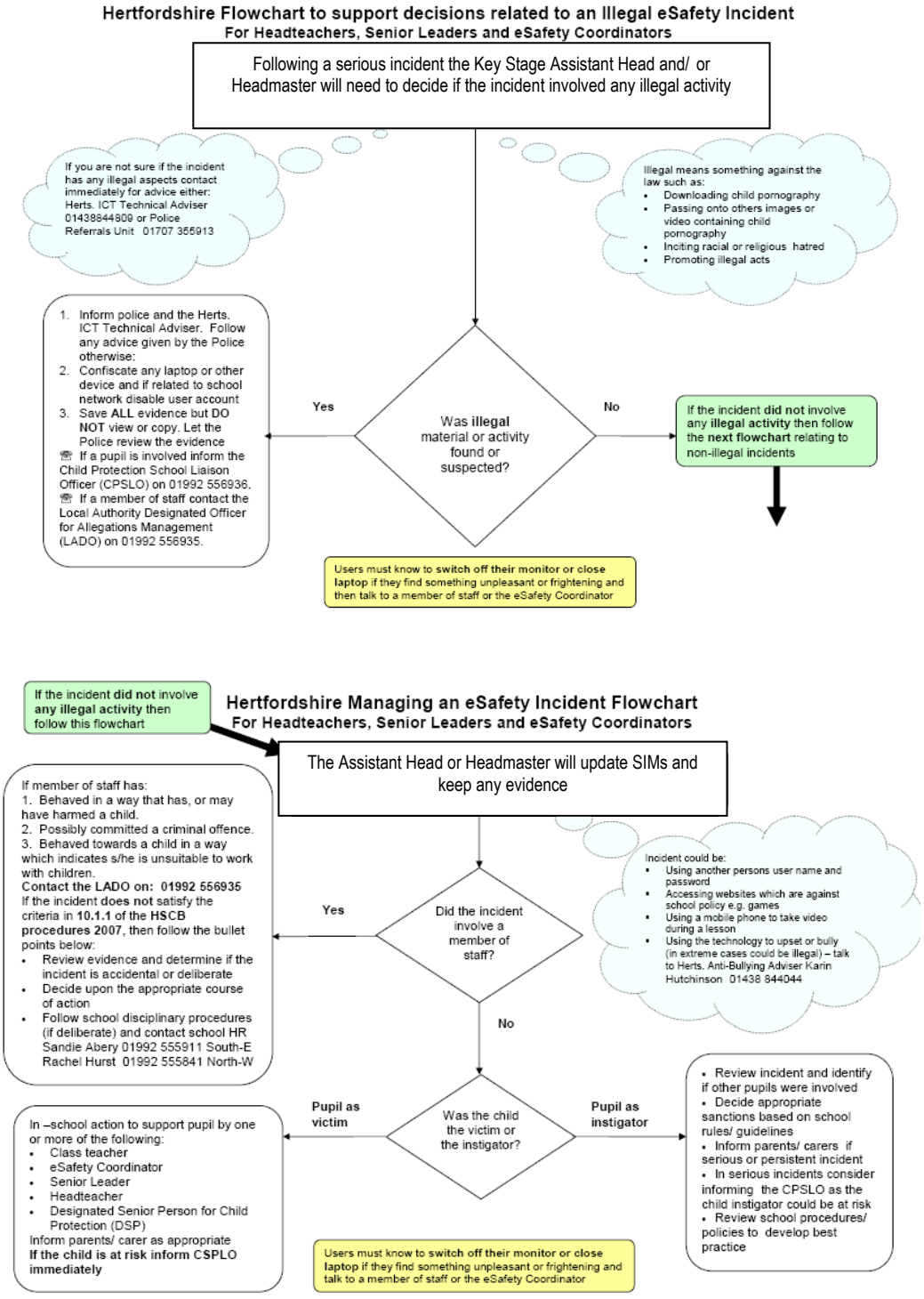
I agree to follow this code of conduct and to support the safe use of ICT throughout the school and understand that it is a condition of being employed at the school.

ACCEPTABLE USE AGREEMENT: STUDENTS

eSafety Rules

- I will only use ICT systems in school, including the internet, email, digital video, mobile technologies, etc. for school purposes.
- If I discover an unsuitable site, I will switch the screen off and immediately tell my teacher.
- I will not invite any member of the school staff to become “a friend” on social networking or similar types of sites.
- I will not download or install software on school technologies.
- I will only log on to the school network/ Learning Platform with my own user name and password.
- I will follow the schools ICT security system and not reveal my passwords to anyone and change them regularly.
- I will only use my school email address, when given.
- I will make sure that all digital communications with students, teachers or others is responsible, appropriate, inoffensive and sensible. This is both inside and outside of school and includes all electronic communication such as social networking, twitter, video broadcasting, texting etc. If I feel bullied online then I know that it is important to tell my parent/ carer or a teacher and do not suffer in silence. I also know that there are sites such as Childline/ CEOP where I can get further help.
- I will be responsible for my behaviour when using the Internet. This includes resources I access and the language I use.
- I will not deliberately browse, download, upload or forward 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 must seek permission from my teacher before I take, store and distribute images, audio or videos of students and/ or staff. These digital recordings must never be of an inappropriate or offensive nature. If asked to delete any digital recordings I will do so from all media (i.e. USB, home computer etc)
- I will ensure that my online activity, both in school and outside school, will not cause my school, the staff, students or others distress or bring it into disrepute.
- I will respect the privacy and ownership of others’ work on-line at all times.
- I will not attempt to bypass the internet filtering system.
- I understand that all my use of the Internet and other related technologies will be monitored and logged and can be made available to my teachers.
- 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 or even the police may be contacted.
- I will not bypass or attempt to bypass any of the security features provided at the school.
- I will not bring into school any illegal content, including pirated songs, movies, software, offensive material and will not try and share or distribute it further.
- I will change my password if I think someone else knows it.

FLOWCHARTS FOR MANAGING AN ESAFETY INCIDENT



SMILE AND STAY SAFE POSTER

MILE and stay safe

Staying safe means keeping your personal details private, such as full name, phone number, home address, photos or school. Never reply to ASL (age, sex, location)

Meeting up with someone you have met online can be dangerous. Only meet up if you have first told your parent or carer and they can be with you.

Information online can be untrue, biased or just inaccurate. Someone online my not be telling the truth about who they are - they may not be a 'friend'

Let a parent, carer, teacher or trusted adult know if you ever feel worried, uncomfortable or frightened about something online or someone you have met or who has contacted you online.

Emails, downloads, IM messages, photos and anything from someone you do not know or trust may contain a virus or unpleasant message. So do not open or reply.

CURRENT LEGISLATION

ACTS RELATING TO MONITORING OF STAFF EMAIL

Data Protection Act 1998

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

The Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000
http://www.hmso.gov.uk/si/si2000/20002699.htm

Regulation of Investigatory Powers Act 2000

Regulating the interception of communications and making it an offence to intercept or monitor communications without the consent of the parties involved in the communication. The RIP was enacted to comply with the Human Rights Act 1998. The Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000, however, permit a degree of monitoring and record keeping, for example, to ensure communications are relevant to school activity or to investigate or detect unauthorised use of the network. Nevertheless, any monitoring is subject to informed consent, which means steps must have been taken to ensure that everyone who may use the system is informed that communications may be monitored. Covert monitoring without informing users that surveillance is taking place risks breaching data protection and privacy legislation.
http://www.hmso.gov.uk/acts/acts2000/20000023.htm

Human Rights Act 1998

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

OTHER ACTS RELATING TO ESAFETY

Racial and Religious Hatred Act 2006

It a criminal offence to threaten people because of their faith, or to stir up religious hatred by displaying, publishing or distributing written material which is threatening. Other laws already protect people from threats based on their race, nationality or ethnic background.

Sexual Offences Act 2003

The new grooming offence is committed if you are over 18 and have communicated with a child under 16 at least twice (including by phone or using the Internet) it is an offence to meet them or travel to meet them anywhere in the world with the intention of committing a sexual offence. Causing a child under 16 to watch a sexual act is illegal, including looking at images such as videos, photos or webcams, for your own gratification. It is also an offence for a person in a position of trust to engage in sexual activity with any person under 18, with whom they are in a position of trust. Schools should already have a copy of "*Children & Families: Safer from Sexual Crime*" document as part of their child protection packs. For more information
www.teachernet.gov.uk

Communications Act 2003 (section 127)

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

The Computer Misuse Act 1990 (sections 1 – 3)

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

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

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

Malicious Communications Act 1988 (section 1)

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

Copyright, Design and Patents Act 1988

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

Public Order Act 1986 (sections 17 – 29)

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

Protection of Children Act 1978 (Section 1)

It is an offence to take, permit to be taken, make, possess, show, distribute or advertise indecent images of children in the United Kingdom. A child for these purposes is a anyone under the age of 18. Viewing an indecent image of a child on your computer means that you have made a digital image. An image of a child also covers pseudo-photographs (digitally collated or otherwise). A person convicted of such an offence may face up to 10 years in prison.

Obscene Publications Act 1959 and 1964

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

Protection from Harassment Act 1997

A person must not pursue a course of conduct, which amounts to harassment of another, and which he knows or ought to know amounts to harassment of the other.
A person whose course of conduct causes another to fear, on at least two occasions, that violence will be used against him is guilty of an offence if he knows or ought to know that his course of conduct will cause the other so to fear on each of those occasions.