IT USERS and E-SAFETY POLICY

Last Reviewed:	June 2025	**Next Review:**	June2026
Approved by:	FGB	**Date:**	June 2025

CONTENTS	
REFERENCE NUMBER AREA	PAGE
Contents	2 - 3
1. Rationale	4
2. Aims	4-5
3. Definitions	5
4. Practice	5
4.1 ACCEPTABLE USE OF PORTABLE TECHNOLOGY POLICY	5
4.2 ACCEPTABLE USE POLICY	5
5. PERSONAL RESPONSIBILITY	6
6. ACCEPTABLE USE	6
7. PRIVILEGES	6
8. NETWORK ETIQUETTE & PRIVACY	6
9. SERVICES	7
10. SECURITY	7
11. VANDALISM	7
12. HEALTH AND SAFETY	7
13. RETURN OF EQUIPMENT	8
14. Roles and Responsibilities	8
15. e-Safety skills development for staff	8
16. Managing the school e-Safety messages	8
17. e-Safety in the Curriculum	8
18. Password Security	9
19. Data Security	9
20. Managing the Internet	9
21. Infrastructure	10
22. Managing other Websites technologies	10
23. Mobile technologies	11
24. Personal Mobile devices (including phones)	11
25. School provided Mobile devices (including phones)	11
26. Managing email	11
27. Taking of Images and Film	12
28. Consent of adults who work at the school	12
29. Publishing student's images and work	12
30. Storage of Images	12
31. Webcams and CCTV	13
32. Video Conferencing	13

33. Misuse and Infringements	**14**
34. Complaints	**14**
35. Inappropriate material	**14**
36. Equal Opportunities	**14**
37. Students with additional needs	**14**
38. Parental Involvement	**14**
39. Writing and Reviewing this Policy	**15**
40. Staff and student involvement in policy creation	**15**
41. Review Procedure	**15**
42. Appendix A **Acceptable Use Agreement: Staff, Governors and Visitors Code of Conduct**	**16**
43. Appendix B **Student Acceptable Use Agreement / e-Safety Rules**	**17-18**
44. Appendix C **Flowchart for responding to internet safety incidents in school**	**19**
45. Appendix D **Flowcharts for Managing an e-Safety Incident**	**20**
46. Appendix E **Incident Log**	**21**
47. SMILE poster	**22**
48. Appendix F **Legislation**	**23-25**

1. Rationale

As part of the ongoing development programme for Information Technology at Falconer School, we now offer all Teachers access to personal mobile technology, providing a wealth of information to assist with reducing workload and enhancing teaching and learning. With home use of school technology comes the responsibility of the user to only access materials that are considered appropriate, inoffensive and legal. To ensure this Falconer School reserves the right to scan portable devices without notice and check for inappropriate or offensive material. Please read this document and ensure that you understand the various sections fully.

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
- 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.

2. Aims

As e-Safety is an important aspect of strategic leadership within the school the Head teacher and Governing Body have ultimate responsibility to ensure that the policy and practices are embedded and monitored.

Senior Leaders and Governors are updated by the Head teacher 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, is to protect the interests and safety of the whole school community. It is linked to the following mandatory school policies: anti-bullying, behaviour, child protection, complaints, code of conduct for employees and health and safety.

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

Both this policy and the Acceptable Use Agreement (for all staff, governors, visitors and students) are inclusive of both fixed and mobile internet; technologies provided by the school (such as PCs, laptops, personal digital assistants

(PDAs), 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.).

3. Definitions

ICT (information and communications technology): This is an umbrella term that includes any communication device or application, encompassing: cameras, mobile phones, smart watches, computer and network hardware and software, satellite systems etc., and the services and applications associated with them e.g. video-conferences, e-learning, databases and electronic records. **ICT** includes technology that can be used to store, transmit or manipulate data, such as MP3 players, Personal Digital Assistants (PDAs) and USB media, including any device that can connect to the internet.

ICT facilities: Includes all facilities, systems and services including but not limited to network infrastructure, desktop computers, laptops, tablets, phones, music players or hardware, software, websites, web applications or services, and any device system or service which may become available in the future which is provided as part of the ICT service

Users: Anyone authorised by the Trust or its academies to use the ICT facilities, including governors, staff, agency workers, volunteers, contractors and visitors Cyber-security: the practice of defending computers, servers, mobile devices, electronic systems, networks, and data from malicious attacks.

Personal use: Any use or activity not directly related to the users' employment, study or purpose.

Authorised personnel: Employees authorised by the Trust to perform systems administration and/or monitoring of the ICT facilities

Materials: Files and data created using the ICT facilities including but not limited to documents, photos, audio, video, printed output, web pages, social networking sites and blogs

4. Practice

4.1 ACCEPTABLE USE OF PORTABLE TECHNOLOGY POLICY

Members of staff at Falconer School may be issued with a number of important items or loaned equipment for which they will be responsible. These may include: laptop and associated materials (cables and laptop lock, carrying case etc.) Staff may also borrow iPads, digital cameras, voice recorders and external storage devices. To qualify, staff must read sign and return the agreement attached to this Policy.

4.2 ACCEPTABLE USE POLICY

Misuse may come in many forms, but it is commonly viewed as any message(s) sent or received that indicate or suggest pornography, unethical or illegal requests, racism, sexism, inappropriate language, any use which may be likely to cause offence and other issues described below. Listed below are the provisions of this agreement. If any member of staff violates these provisions, access to their laptop and other devices will be denied and the staff member will be subject to an investigation and possible disciplinary action. The e-mail network account of the member of staff will be locked during this investigation.

TERMS & CONDITIONS OF THIS AGREEMENT

5. PERSONAL RESPONSIBILITY

The items remain the property of Falconer School and are for use ONLY by the named member of staff. Staff should not use items for any purpose which would contravene reasonable expectations for the conduct of an employee of the school.

6. ACCEPTABLE USE

The use of electronic services and technology must be in support of education and research in accordance with the educational goals and objectives of Falconer School. Staff are personally responsible for this provision at all times when using the electronic information service and technology. Use of other networks or computing resources must comply with the rules appropriate to that network. Transmission or use of any material in violation of any United Kingdom or other national laws is prohibited. This includes, but is not limited to, copyrighted material, threatening or obscene material or material protected by trade laws. Personal uses for matters unrelated to teaching and learning within the laws of the United Kingdom outside of school hours are permitted.

7. PRIVILEGES

The use of the Internet and other electronic technology is a privilege and inappropriate use will result in that privilege being withdrawn.

8. NETWORK ETIQUETTE & PRIVACY

Staff are expected to abide by the generally accepted rules of network etiquette. These rules include, but are not limited to the following:

- BE POLITE. Never send or encourage others to send abusive messages
- BE PROFESSIONAL. Use language and terminology which would normally be uses in the classroom
- USE APPROPRIATE LANGUAGE. Staff are a representative of the school at all times and what is said can be viewed by others. Staff should never swear, use vulgarities or any other inappropriate language. Illegal activities of any kind are strictly forbidden
- PRIVACY. Staff should not reveal any personal information to anyone, especially the home address or personal telephone of themselves or any details of students
- PASSWORD. Staff should not reveal their password to anyone. If at anytime a member of staff thinks someone has obtained their password, they should contact a member of the NS department immediately and change the password
- ELECTRONIC MAIL. No emails should be private between staff and students. Staff must never have one to one email exchanges with students from a personal email account. Each subject has a faculty email address for the purpose of communication with students and parents
- PROOF READ – staff should always proof read the message to ensure that it is error free and easy to understand before sending
- Messages relating to, or in support of, illegal activities may be reported to the authorities immediately
- The school's Website should be the main conduit used by staff for most educational exchanges with students
- The use of **Twitter, Facebook or other social networking sites** may be used for educational purposes but they must never be used for social contact with students
- Staff should always use their own username and password to logon into the school system and never use the administrator login details

9. SERVICES

Falconer School makes no warranties of any kind whether expressed or implied, for the network service it is providing. Falconer School will not be responsible for any damages suffered whilst on this system. These damages include loss of data as a result of delays, non-deliveries, mis-deliveries or service interruptions caused by the system or elements of the system, or your errors or omissions. Use of any information obtained via the network or other information systems is at your own risk. Falconer School specifically denies any responsibility for the accuracy of information obtained via its Internet services.

10. SECURITY

Staff are expected to ensure that the laptop and other accessories will be kept securely at all times and recognise that if it is lost, damaged or stolen due to a lapse in their security they may be liable for replacing or repairing the device.

To ensure security, portable devices and technology should be stored in the boot of cars when in transit or when leaving the device in the car when parked. At home, the device should be stored away from direct sunlight and view of passersby. To ensure security at School, the device should always be under the direct control and supervision of the staff member and when not in use should be securely stored.
Staff are responsible for reading and adhering to all Health and Safety and Care literature provided with the portable device.
Security on any computer system is a high priority because there are so many users. If a security problem is identified, staff must notify a member of the SLT staff at once. Staff must ensure to keep their password to themselves and change it on a regular basis. The logon and password is designed to be entered on each log on occasion to ensure that if the device is lost or stolen, it cannot be accessed easily.

Staff should ensure that when posting events, documents or emails onto the Internet or School Intranet that student names are kept to a minimum. Never publish a student's full name or personal details to ensure their privacy and safety. Student photos should only be used if parental consent has been given to the school – this can be checked with the Data Manager.
Full student names should never be included with a photo. The laptop computer is insured under the school insurance policy but all reasonable precautions should be taken to ensure the security of the machine and the (sometimes sensitive and confidential) data held on it (see GDPR policy).

11. VANDALISM

Vandalism is defined as any malicious attempt to harm or destroy any equipment or data of another user or of any other networks that are connected to the system. This includes, but is not limited to, the uploading or creation of computer viruses, the willful damage of computer hardware, whether connected to the network or not, the deletion of data from its place of storage. If staff recognise another member of the school participating in this activity they should contact the Head of ICT.

12. HEALTH and SAFETY

Health and Safety guidelines will be distributed alongside the policy and the portable device. Falconer School will take no responsibility for the implications resulting from not adhering to the suggested posture and handing of equipment in relation to, but not limited to repetitive strain injury (RSI) or eye-strain. If you are experiencing discomfort when using the technology for a long period of time, please speak to Kate Ward, HR Officer to request a workstation assessment.

13. RETURN OF EQUIPMENT

Staff must take reasonable steps to ensure that the items can be returned to the school in a fit state for a subsequent user. Staff will be required to return all items on or before their last day of employment at the school.

14. Roles and Responsibilities

As e-Safety is an important aspect of strategic leadership within the school, the Head and governors have ultimate responsibility to ensure that the policy and practices are embedded and monitored. The named e-Safety co-ordinator in our school is the Head teacher ***(DSL)*** 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 e-Safety 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 Leaders and Governors are updated by the Head/ e-Safety 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 students (appendices), 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/student discipline (including the anti-bullying) policy and PHSE

15. e-Safety skills development for staff

- Our staff receive regular information and training on e-Safety through staff meetings
- New staff receive information on the school's acceptable use policy as part of their induction
- All staff have been made aware of individual responsibilities relating to the safeguarding of children within the context of e-Safety and know what to do in the event of misuse of technology by any member of the school community (see attached flowchart)
- All staff are encouraged to incorporate e-Safety activities and awareness within their curriculum areas where appropriate

16. Managing the school e-Safety messages

- We endeavour to embed e-Safety messages across the curriculum whenever the internet and/or related technologies are used
- E-safety posters will be prominently displayed

17. e-Safety in the Curriculum

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

- The school has a framework for teaching internet skills in ICT
- Educating students on the dangers of technologies that maybe encountered outside school is done informally when opportunities arise and as part of the e-Safety 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

18. Password Security

Password security is essential for staff, particularly as they are able to access and use student 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 them with others, particularly their friends. Staff and students are regularly reminded of the need for password security.

- All users read and sign an Acceptable Use Agreement to demonstrate that they have understood the school's e-safety Policy
- Users are provided with an individual network, email and Learning Platform log-in username. 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 you think your password may have been compromised or someone else has become aware of your password report this to Head of ICT
- Staff are aware of their individual responsibilities to protect the security and confidentiality of school networks, MIS systems and/or Learning Platform, including ensuring that passwords 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 passwords are the responsibility of Head of ICT and all staff and students are expected to comply with the policies at all times

19. 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 HT
- Data can only be accessed and used on school computers or laptops. Staff are aware they must not use their personal devices for accessing any school/student data

20. Managing the Internet

The internet is an open communication medium, available to all, at all times. Anyone can view information, send messages, discuss ideas and publish material which makes it both an invaluable resource for education, business and social interaction, as well as a potential risk to young and vulnerable people. All use of the **Hertfordshire Grid for Learning** (HGfL) 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
- Raw image searches are discouraged when working with students

- If Internet research is set for homework, specific sites will be suggested that have previously been checked by the teacher. It is advised that parents recheck these sites and supervise this work. Parents will be advised to supervise any further research
- All users must observe software copyright at all times. It is illegal to copy or distribute school software or illegal software from other sources
- All users must observe copyright of materials from electronic resources

21. Infrastructure

- Falconer utilises an external provider service where web-based activity is monitored and recorded
- School internet access is controlled through the schools broadband service. For further information relating to filtering please go to **http://www.thegrid.org.uk/eservices/safety/filtered.shtml**
- Falconer School is aware of its responsibility when monitoring staff communication under current legislation and takes into account; Data Protection Act 1998, The Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000, Regulation of Investigatory Powers Act 2000, Human Rights Act 1998
- Staff and students are aware that school based email and internet activity can be monitored and explored further if required
- The school does not allow students access to internet logs.
- The school uses management control tools for controlling and monitoring workstations
- If staff or students discover an unsuitable site, the screen must be switched off/ closed and the incident reported immediately to the e-safety co-ordinator
- It is the responsibility of the school, by delegation to the network manager, to ensure that Anti-virus protection is installed and kept up-to-date on all school machines
- Students and Staff 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 to install or maintain virus protection on personal systems. If students wish to bring in a removable media, it must be given to the ***(***technician/teacher***)*** for a safety check first
- Students and staff are not permitted to download programs or files on school based technologies without seeking prior permission from the ICT subject leader
- If there are any issues related to viruses or anti-virus software, the network manager should be informed

22. Managing other Websites technologies

Websites, 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

23. Mobile technologies

Many emerging technologies offer new opportunities for teaching and learning including a move towards personalised learning and 1:1 device ownership for children and young people. Many existing mobile technologies such as portable media players, PDAs, gaming devices, mobile and Smart phones are familiar to children outside of school too. They often provide a collaborative, well-known device with possible internet access and thus open up risk and misuse associated with communication and internet use. Emerging technologies will be examined for educational benefit and the risk assessed before use in school is allowed. Our school chooses to manage the use of these devices in the following ways so that users exploit them appropriately.

24. Personal Mobile devices (including phones)

- The school allows staff to bring in personal mobile phones and devices for their own use. Under no circumstances does the school allow a member of staff to contact a student or parent/ carer using their personal device
- Students are discouraged from bringing in personal mobile devices/phones to school. Mobile phones will be handed to staff on arrival
- This technology may be used, however 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 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

25. School provided Mobile devices (including phones)

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

26. Managing email

The use of email within most schools is an essential means of communication for both staff and students. In the context of school, email should not be considered private. Educationally, email can offer significant benefits including; direct written contact between schools on different projects, be they staff based or student based, within school or international. We recognise that students need to understand how to style an email in relation to their age and good 'netiquette'.

- The school gives all staff their own email account to use for all school business. This is to minimise the risk of receiving unsolicited or malicious emails and avoids the risk of personal profile information being revealed
- It is the responsibility of each account holder to keep the password secure. For the safety and security of users and recipients, all mail is filtered and logged; if necessary email histories can be traced. This should be the account that is used for all school business

- Under no circumstances should staff contact students, parents or conduct any school business using personal email addresses
- The school requires a standard disclaimer to be attached to all email correspondence, stating that, 'the views expressed are not necessarily those of the school or the LA'. The responsibility for adding this disclaimer lies with the account holder
- E-mail sent to an external organisation should be written carefully before sending, in the same way as a letter written on school headed paper
- Staff sending emails to external organisations, parents or students are advised to cc. the Head teacher, line manager or designated account
- Students may only use school approved accounts on the school system and only under direct teacher supervision for educational purposes
- All students have their own individual school issued accounts
- 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 e-Safety co-ordinator/ line manager) if they receive an offensive e-mail
- Students are introduced to email as part of the ICT lessons

Safe Use of Images

27. Taking of Images and Film

Digital images are easy to capture, reproduce and publish and, therefore, misused. We must remember that it is not always appropriate to take or store images of any member of the school community or public, without first seeking consent and considering the appropriateness.

- With the written consent of parents (on behalf of students) and staff, the school permits the appropriate taking of images by staff and students with school equipment
- Staff are not permitted to use personal digital equipment, such as mobile phones and cameras, to record images of students, this includes when on field trips. However, with the express permission of the Head teacher, images can be taken provided they are transferred immediately and solely to the school's network and deleted from the staff device
- Students are not permitted to use personal digital equipment, including mobile phones and cameras, to record images of the others, this includes when on field trips. However, with the express permission of the Head teacher, images can be taken provided they are transferred immediately and solely to the school's network and deleted from the student's device
- A list of any pupils who the school cannot take images of under any circumstances as well as those that cannot be shared externally to the school.

28. 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

29. Publishing student's images and work

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

- on the school web site
- on the school's Learning Platform

- in the school prospectus and other printed publications that the school may produce for promotional purposes
- recorded/ transmitted on a video or webcam
- in display material that may be used in the school's communal areas
- in display material that may be used in external areas, i.e. exhibition promoting the school
- general media appearances, e.g. local/ national media/ press releases sent to the press highlighting an activity (sent using traditional methods or electronically)

This consent form is considered valid for the entire period that the child attends this school unless there is a change in the child's circumstances where consent could be an issue, e.g. divorce of parents, custody issues, etc.
Parents/ carers may withdraw permission, in writing, at any time. Consent has to be given by both parents in order for it to be deemed valid.

Students' names will not be published alongside their image and vice versa. E-mail and postal addresses of students will not be published. Students' full names will not be published.
Before posting student work on the Internet, a check needs to be made to ensure that permission has been given for work to be displayed.
Only the Web Manager has authority to upload to the site.

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

30. Storage of Images

- Images/ films of children are stored on the school's network in the 'Teacher Shared' folder which is restricted to students
- Students and staff are not permitted to use personal portable media for storage of images (e.g., USB sticks) without the express permission of the Head teacher
- Rights of access to this material are restricted to the teaching staff and students within the confines of the school network/ Learning Platform
- The curriculum teachers have the responsibility of deleting the images when they are no longer required, or the student has left the school

31. Webcams and CCTV

- The school uses CCTV for security and safety. The only people with access to this are the Head teacher and the office staff. Notification of CCTV use is displayed at the front of the school

32. Video Conferencing

- Permission is sought from parents and carers if their children are involved in video conferences
- Permission is sought from parents and carers if their children are involved in video conferences with end-points outside of the school
- All students are supervised by a member of staff when video conferencing
- All students are supervised by a member of staff when video conferencing with end-points beyond the school
- The school keeps a record of video conferences, including date, time and participants
- Approval from the Head teacher 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

33. Misuse and Infringements

34. Complaints

Complaints relating to e-Safety should be made to the Head teacher. Incidents will be logged and the **Hertfordshire Flowcharts for Managing an e-Safety Incident** will be followed.

35. Inappropriate material

- All users are aware of the procedures for reporting accidental access to inappropriate materials. The breach must be immediately reported to the e-Safety co-ordinator
- Deliberate access to inappropriate materials by any user will lead to the incident being logged by the e-Safety co-ordinator, depending on the seriousness of the offence; investigation by the Headteacher/ LA, immediate suspension, possibly leading to dismissal and involvement of police for very serious offences (see flowchart.)
- Users are made aware of sanctions relating to the misuse or misconduct by signing the e-policy agreement and having had e-safety induction

36. Equal Opportunities

37. 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' e-Safety 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 e-Safety issues.

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

38. Parental Involvement

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

- Parents/ carers are asked to read through and sign acceptable use agreements on behalf of their child on admission to school
- Parents/ carers are required to make a decision as to whether they consent to images of their child being taken/ used in the public domain (e.g., on school website)
- The school disseminates information to parents relating to e-Safety where appropriate in the form of;
    - Information and celebration evenings
    - Posters
    - Website/ Learning Platform postings
    - Newsletter items

39. Writing and Reviewing this Policy

40. Staff and student involvement in policy creation

- Staff and students have been involved in making/ reviewing the e-Safety policy through the school council and staff meetings

41. Review Procedure

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

This policy will be reviewed every 3 years by the appropriate members of the Governing Body 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.

42. Appendix A

Acceptable Use Agreement: Staff, Governors and Visitors
Code of Conduct

ICT and the related technologies such as email, the internet and mobile devices are an expected part of our daily working life in school. This policy is designed to ensure that all staff are aware of their professional responsibilities when using any form of ICT. All staff are expected to sign this policy and adhere at all times to its contents. Any concerns or clarification should be discussed with the Head teacher, school e-Safety 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 and personal email address, to students.
- 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
- I will not install any hardware or software without the permission of the Headteacher. I will not browse, download, upload or distribute any material that could be considered offensive, illegal or discriminatory
- Images of students and/ or staff will only be taken, stored and used for professional purposes 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 respect copyright and intellectual property rights
- I will ensure that my online activity, both in school and outside school, will not bring my professional role into disrepute
- I will support and promote the school's e-Safety policy and help students to be safe and responsible in their use of ICT and related technologies
- Students/staff are not permitted to use personal portable media for storage of images e.g. (USB Sticks) without express permission of the Headteacher
- Teachers should keep their folders tidy and updated in the 'Teacher Shared' folder e.g. (remove images that re no longer required)

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 ……..

(Please print)

Job title ……

43. Appendix B

Student Acceptable Use Agreement / e-Safety Rules

- I will only use ICT 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/ Learning Platform with my own user name and password
- I will follow the school's ICT security system and not reveal my passwords to anyone and change them regularly
- I will make sure that all ICT communications with students, teachers or others is responsible and sensible
- 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
- Images of students and/ or staff will only be taken, stored and used for school purposes in line with school policy and not be distributed outside the school network without the permission of the Headteacher
- 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 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 e.g. use of proxy servers
- 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 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

Falconer School

Dear Parents and Carers

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

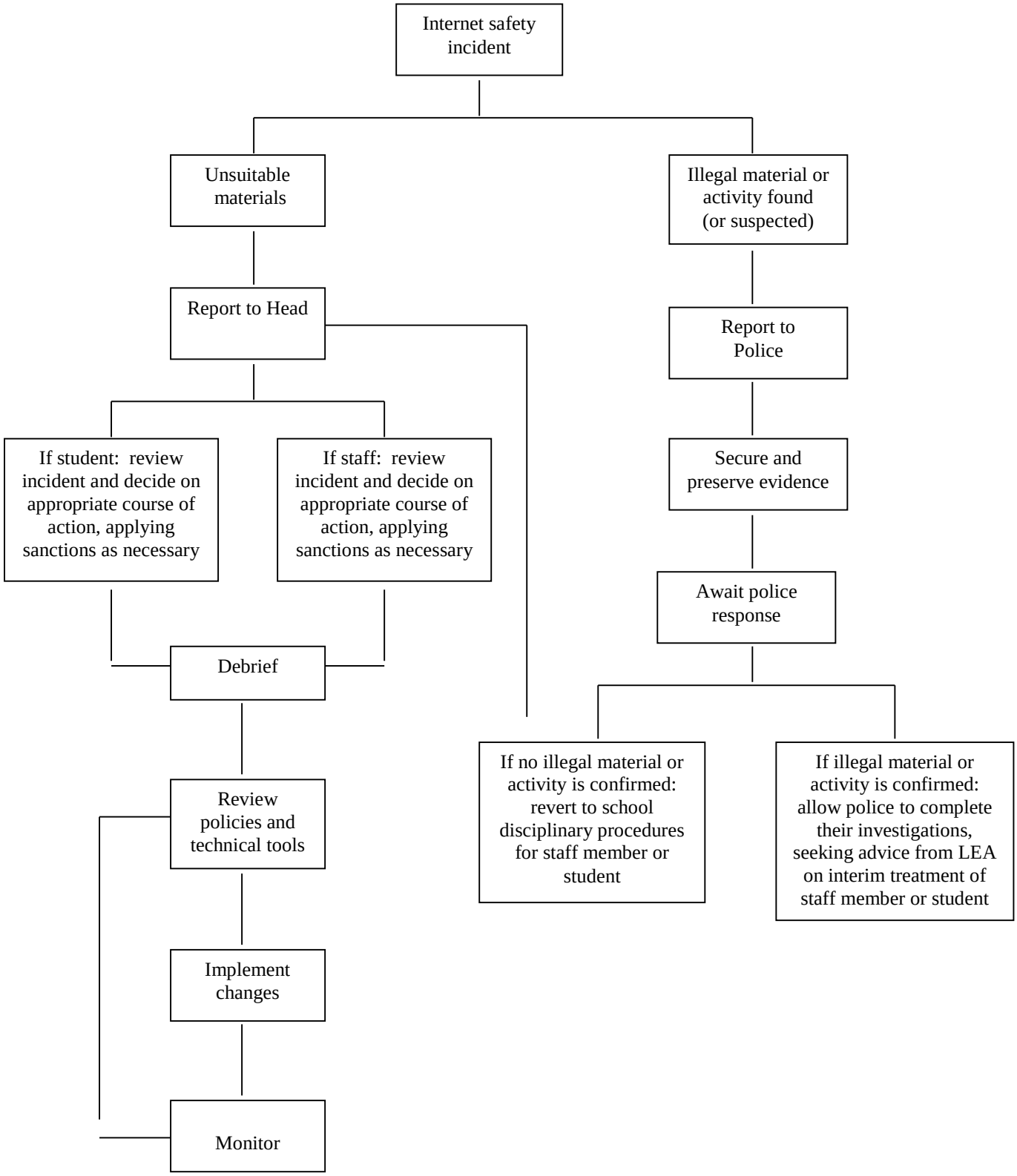
Students are expected to read and discuss this agreement with their parent or carer and then to sign and follow the terms of the agreement. Any concerns or explanation can be discussed with their class teacher or the Headteacher, school e-Safety coordinator.

Please return the bottom section of this form to school for filing.

✂ - - -

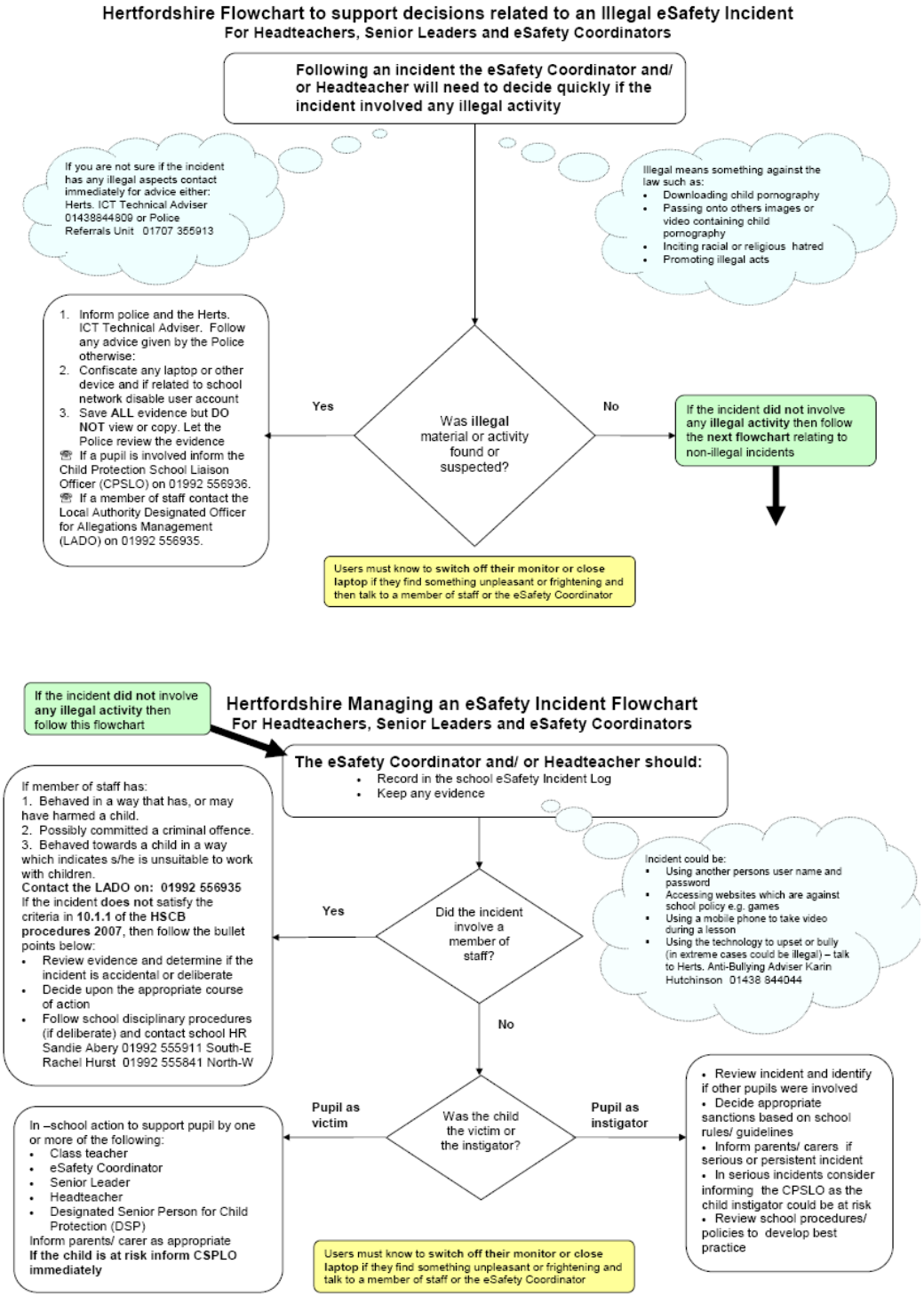
44. Appendix C

Flowchart for responding to internet safety incidents in school



45. Appendix D

Flowcharts for Managing an e-Safety Incident



46. Appendix E

Incident Log

Date & Time	Name of Student or Staff Member	Male or Female	Room & Computer/Device number	Details of incident	Actions & Reasons

47. Appendix F

Smile and Stay Safe Poster

E-Safety Rules to be displayed



SMILE 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 may 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.

48. Appendix G

Current Legislation

Acts relating to monitoring of staff email

Data Protection Act 2018

The Act requires anyone who handles personal information to comply with important data protection principles when treating personal data relating to any living individual. The Act grants individuals rights of access to their personal data, compensation and prevention of processing.

https://www.gov.uk/data-protection

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

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

Regulation of Investigatory Powers Act 2000

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

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

Human Rights Act 1998

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

Other Acts relating to e-Safety

Racial and Religious Hatred Act 2006

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

Sexual Offences Act 2003 (updated March 2023)

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.

Communications Act 2003 (section 127)

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

The Computer Misuse Act 1990 (sections 1 – 3)

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

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

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

Malicious Communications Act 1988 (section 1)

This legislation makes it a criminal offence to send an electronic message (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 (additions 1977)

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.