

E-Safety and Computer Usage Policy

Date formally approved by the Governors :
Date policy became effective : January 2010
Review Date: January 2011
Person responsible for implementation and monitoring : E-Safety Officer, Head of ICT, Child Protection Officers, Head
Other relevant policies: Procedure on Discipline and Exclusions, Policy for the Safety and Security of Pupils, Policy to Safeguard and to promote the Welfare of Children, Child Protection Policy, Data Protection Policy

Aims of the School – Garde ta Foy

Felsted Preparatory School (as part of Felsted) aims to educate children in a warm and caring environment, where the highest possible standards are set. The School aims to encourage boys and girls to achieve their individual best by gaining appropriate skills and awareness in order to be prepared for the next stage of their education. To achieve these aims, pupils ought:

- To understand and enjoy the academic and intellectual challenges that they face as well as the social, spiritual, physical, creative, moral, emotional and cultural dimensions of life at Felsted Preparatory School and beyond.
- To develop the capacity to know and appreciate their own strengths and weaknesses, and to encourage and nurture the development of personal faith, while also being considerate, tolerant and respectful of the strengths and weaknesses of others, which is consistent with the School's Christian ethos and foundation.
- To develop an understanding and sympathetic appreciation of those of different backgrounds and cultures.
- To set themselves high personal standards and values in all that they do.
- To participate in and enjoy the wide range of activities on offer.

Felsted Preparatory School – encouraging all children to achieve their individual best.

This policy supports the aims of the School in educating Young Felstedians to explore their horizons in line with the e-world safely and setting up a safety net around them.

Policy contents

[Rationale](#)

[Monitoring](#)

[Incidents](#)

[Inclusion](#)

[Roles and Responsibilities](#)

[Viruses](#)

[Data Security](#)

[Pupil and Staff training](#)

[Systems and Access](#)

[Email use](#)

[Internet Use](#)

[Web 2.0 Technologies](#)

[Protecting Information](#)

[Remote Access](#)

[Safe Use of Images](#)

[ICT Equipment within School](#)

[Current Legislation](#)

[Procedure for investigating an incident](#)

[Acceptable Use Policies](#)

[Incident Log Form](#)

[Monitoring and Evaluation](#)

Rationale

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

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

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

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

At Felsted, we understand the responsibility to educate our pupils 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.

Schools hold personal data on learners, staff and other people to help them conduct their 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. This can make it more difficult for the School to use technology to benefit learners.

Everybody in the School 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 (for all staff and pupils), copies attached) 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 pupils and staff, but brought onto school premises (such as laptops, mobile phones, camera phones, PDAs and portable media players, etc).

Monitoring

Authorised ICT staff may inspect any ICT 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 their department. Any ICT authorised staff member will be happy to comply with this request.

ICT authorised staff may monitor, intercept, access, inspect, record and disclose telephone calls, e-mails, instant messaging, internet/intranet use and any other electronic communications (data, voice or image) involving its 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 ICT; 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.

ICT authorised staff may, without prior notice, access the e-mail or voice-mail 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 ICT 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 ICT hardware, software or services from the offending individual.

Any policy breach is grounds for disciplinary action in accordance with the School Disciplinary Procedure.

Policy breaches may also lead to criminal or civil proceedings.

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 eSafety Officer. Additionally, all security breaches, lost/stolen equipment or data, virus notifications, misuse or unauthorised use of ICT and all other policy non-compliance must be reported to the Head of ICT.

All eSafety incidents involving either staff or pupils should be recorded on the eSafety incident log by the eSafety Officer. A copy is attached to this policy.

Complaints

Complaints and/or issues relating to eSafety should be made to the eSafety Officer or Head. Incidents should be logged and the School procedure for investigating an eSafety incident should be followed.

Inappropriate Material

All users are aware of the procedures for reporting accidental access to inappropriate materials. The breach must be immediately reported to the eSafety Officer.

Deliberate access to inappropriate materials by any user will lead to the incident being logged by the eSafety Officer, depending on the seriousness of the offence; investigation by the Head/eSafety Officer, immediate suspension, possibly leading to dismissal and involvement of police for very serious offences (see flowchart).

Inclusion

The school endeavours to create a consistent message with parents for all pupils and this in turn should aid establishment and future development of the schools' eSafety rules.

However, staff are aware that some pupils may require additional teaching including reminders, prompts and further explanation to reinforce their existing knowledge and understanding of 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.

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 Officer in this school is Matthew Clarke. All members of the school community have been made aware of who holds this post. It is the role of the eSafety Officer to keep abreast of current issues and guidance through organisations such as Becta, CEOP (Child Exploitation and Online Protection) and Childnet.

This policy, supported by the school's acceptable use agreements for staff, governors, visitors and pupils, is to protect the interests and safety of the whole school community. It is linked to the school policies listed in the introduction to this policy.

Computer Viruses

Never interfere with any anti-virus software installed on school ICT equipment that you use.

If your machine is not routinely connected to the school network, you must make provision for regular virus updates.

If you suspect there may be a virus on any school ICT equipment, stop using the equipment and contact the ICT department. They will advise you what actions to take and be responsible for advising others that need to know.

Data Security

The accessing and appropriate use of school data is something that the school takes very seriously.

The school follows Becta guidelines Becta Schools - Leadership and management - Security - Data handling security guidance for schools (published Spring 2009) (http://schools.becta.org.uk/index.php?section=lv&catcode=ss_lv_saf_se_03&rid=14734)

The School gives relevant staff access to its Management Information System, with a unique ID and password. It is the responsibility of everyone to keep passwords secure.

Staff have been issued with the relevant guidance documents and the Policy for ICT Acceptable Use.

Staff should avoid leaving any portable or mobile ICT equipment or removable storage media in unattended vehicles. Where this is not possible, keep it locked out of sight.

It is the responsibility of individual staff to ensure the security of any personal, sensitive, confidential and classified 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. Anyone expecting a confidential/sensitive fax, should have warned the sender to notify before it is sent.

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 pupils 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 internet skills in ICT/ PSHE lessons.

Educating pupils on the dangers of technologies that may be encountered outside school is done informally when opportunities arise and as part of the eSafety curriculum.

Pupils are aware of the relevant legislation when using the internet such as data protection and intellectual property which may limit what they want to do but also serves to protect them.

Pupils are taught about copyright and respecting other people's information, images, etc through discussion, modeling and activities.

Pupils are aware of the impact of Cyberbullying and know how to seek help if they are affected by any form of online bullying. Pupils are also aware of where to seek advice or help if they experience problems when using the internet and related technologies; i.e. parent/ carer, teacher/ trusted staff member, or an organisation such as Childline or CEOP report abuse button.

Pupils are taught to critically evaluate materials and learn good searching skills through cross curricular teacher models, discussions and via the ICT curriculum.

eSafety Skills Development for Staff

New staff receive information on the school's acceptable use policy as part of their induction.

All staff have been made aware of individual responsibilities relating to the safeguarding of children within the context of eSafety and knows what to do in the event of misuse of technology by any member of the school community (see enclosed flowchart).

All staff are encouraged to incorporate eSafety activities and awareness within their curriculum areas.

Our staff receive regular information and training on eSafety issues in the form of INSET from the eSafety Officer.

Systems and Access

All staff are responsible for any activity on school systems carried out under access/account rights assigned to them, whether accessed via school ICT equipment or their own PC.

No member of staff should allow any unauthorised person to use school ICT facilities and services that have been provided to them.

Staff should use only their personal logons, account IDs and passwords and not allow them to be used by anyone else.

Screen displays should be kept out of direct view of any third parties when accessing personal, sensitive, confidential or classified information.

Staff should ensure they log off before moving away from a computer during the normal working day to protect any personal, sensitive, confidential or otherwise classified data and to prevent unauthorised access.

Staff should not introduce or propagate viruses knowingly.

It is imperative that staff do not access, load, store, post or send from school ICT any material that is, or may be considered to be, illegal, offensive, libelous, pornographic, obscene, defamatory, intimidating, misleading or disruptive to the school or may bring the school into disrepute. This includes, but is not limited to, jokes, chain letters, files, emails, clips or images that are not part of the school's business activities; sexual comments or images, nudity, racial slurs, gender specific comments, or anything that would offend someone on the basis of their age, sexual orientation, religious or political beliefs, national origin, or disability (in accordance with the Sex Discrimination Act, the Race Relations Act and the Disability Discrimination Act).

Any information held on School systems, hardware or used in relation to School business may be subject to The Freedom of Information Act.

Where necessary, obtain permission from the owner or owning authority and pay any relevant fees before using, copying or distributing any material that is protected under the Copyright, Designs and Patents Act 1998.

E-mail

The use of e-mail within most schools is an essential means of communication for both staff and pupils. In the context of school, e-mail should not be considered private. Educationally, e-mail can offer significant benefits including; direct written contact between schools on different projects, be they staff based or pupil based, within school or international. We recognise that pupils need to understand how to style an e-mail in relation to their age and good network etiquette; 'netiquette'. In order to achieve ICT level 4 or above, pupils must have experienced sending and receiving e-mails.

The school gives all staff their own e-mail account to use for all school business as a work based tool This is to minimise the risk of receiving unsolicited or malicious e-mails 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 e-mail histories can be traced. The school email account should be the account that is used for all school business.

Under no circumstances should staff contact pupils, parents or conduct any school business using personal e-mail addresses.

All e-mails should be written and checked carefully before sending, in the same way as a letter written on school headed paper.

E-mails created or received as part of your School job will be subject to disclosure in response to a request for information under the Freedom of Information Act 2000.

All pupil e-mail users are expected to adhere to the generally accepted rules of netiquette particularly in relation to the use of appropriate language and not revealing any personal details about themselves or others in e-mail communication, or arrange to meet anyone without specific permission, virus checking attachments.

Staff must inform the e-Safety Officer if they receive an offensive e-mail.

Pupils are introduced to e-mail as part of the ICT Scheme of Work.

However you access your school e-mail (whether directly, through webmail when away from the office or on non-school hardware) all the school e-mail policies apply.

Internet Usage

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 internet at Felsted is logged and the logs are randomly but regularly monitored.

Whenever any inappropriate use is detected it will be followed up.

Raw image searches are discouraged when working with pupils

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.

You must not post personal, sensitive, confidential or classified information or disseminate such information in any way that may compromise its intended restricted audience.

Don't reveal names of colleagues, pupils or parents, or any other confidential information acquired through your job on any social networking site or blog.

On-line gambling is not allowed.

Staff and pupils are aware that school based email and internet activity can be monitored and explored further if required.

The school does not allow pupils access to internet logs.

The school uses management control tools for controlling and monitoring workstations.

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.

Pupils 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.

Pupils and staff are not permitted to download programs on school based technologies without seeking prior permission from the Head of ICT.

If there are any issues related to viruses or anti-virus software, the network manager should be informed via the Head of ICT or ICT Technician immediately.

Managing Web 2.0 Technologies

Web 2.0, 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 pupils 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 endeavors to deny access to social networking sites to pupils within school.

All pupils are advised to be cautious about the information given by others on sites, for example users not being who they say they are.

Pupils are taught to avoid placing images of themselves (or details within images that could give background details) on such sites and to consider the appropriateness of any images they post due to the difficulty of removing an image once online.

Pupils are always reminded to avoid giving out personal details on such sites which may identify them or where they are (full name, address, mobile/home phone numbers, school details, IM/ email address, specific hobbies/ interests).

Our pupils are advised to set and maintain profiles on such sites to maximum privacy and deny access to unknown individuals.

Pupils are encouraged to be wary about publishing specific and detailed private thoughts online.

Protecting Personal, Sensitive, Confidential and Classified Information

Ensure that any School information accessed from your own PC or removable media equipment is kept secure.

Ensure you log off before moving away from your computer during your normal working day to prevent unauthorised access.

Ensure the accuracy of any personal, sensitive, confidential and classified information you disclose or share with others.

Ensure that personal, sensitive, confidential or classified information is not disclosed to any unauthorised person.

Ensure the security of any personal, sensitive, confidential and classified information contained in documents you fax, copy, scan or print. This is particularly important when shared copiers (multi-function print, fax, scan and copiers) are used and when access is from a non-school environment.

You must not post on the internet personal, sensitive, confidential, or classified information, or disseminate such information in any way that may compromise its intended restricted audience.

Keep your screen display out of direct view of any third parties when you are accessing personal, sensitive, confidential or classified information.

Ensure hard copies of data are securely stored and disposed of after use.

Remote Access

You are responsible for all activity via your remote access facility.

Only use equipment with an appropriate level of security for remote access.

Avoid writing down or otherwise recording any network access information. Any such information that is written down must be kept in a secure place and disguised so that no other person will be able to identify what it is.

Protect School information and data at all times, including any printed material produced while using the remote access facility. Take particular care when access is from a non-School environment.

Safe Use of Images

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.

With the written consent of parents (on behalf of pupils) and staff, the school permits the appropriate taking of images by staff and pupils with school equipment.

ICT Equipment within School

As a user of ICT, you are responsible for any activity undertaken on the school's ICT equipment provided to you.

Do not attempt unauthorised access or make unauthorised modifications to computer equipment, programs, files or data. This is an offence under the Computer Misuse Act 1990.

It is imperative that you save your data on a frequent basis to the school's network drive. You are responsible for the backup and restoration of any of your data that is not held on the school's network drive.

It is your responsibility to ensure that any information accessed from your own PC or removable media equipment is kept secure, and that no personal, sensitive, confidential or classified information is disclosed to any unauthorised person.

All activities carried out on School systems and hardware will be monitored in accordance with the general policy.

Staff must ensure that all school data is stored on school's network, and not kept solely on a laptop.

Equipment must be kept physically secure in accordance with this policy to be covered for insurance purposes. When travelling by car, best practice is to place the laptop in the boot of your car before starting your journey.

Ensure portable and mobile ICT equipment is made available as necessary for anti-virus updates and software installations, patches or upgrades.

The installation of any applications or software packages must be authorised by the ICT support team, fully licensed and only carried out by your ICT support.

In areas where there are likely to be members of the general public, portable or mobile ICT equipment must not be left unattended and, wherever possible, must be kept out of sight.

Portable equipment must be transported in its protective case if supplied.

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.

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 pupil or parent/ carer using their personal device.

With permission from the appropriate Head of Year or the Housemaster, pupils are allowed to bring personal mobile devices/phones to school but must hand them in to the relevant office at the start of each day. This technology may be used for educational purposes, as mutually agreed with the Head of ICT. 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.

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.hms0.gov.uk/acts/acts1998/19980029.htm>

The Telecommunications (Lawful Business Practice)
(Interception of Communications) Regulations 2000
<http://www.hmsso.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.hmsso.gov.uk/acts/acts2000/20000023.htm>

Human Rights Act 1998
<http://www.hmsso.gov.uk/acts/acts1998/19980042.htm>

Other Acts Relating to eSafety

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
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:

- i. access to computer files or software without permission (for example using another person's password to access files)
- ii. unauthorised access, as above, in order to commit a further criminal act (such as fraud)
- iii. 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 their 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.

Acts Relating to the Protection of Personal Data

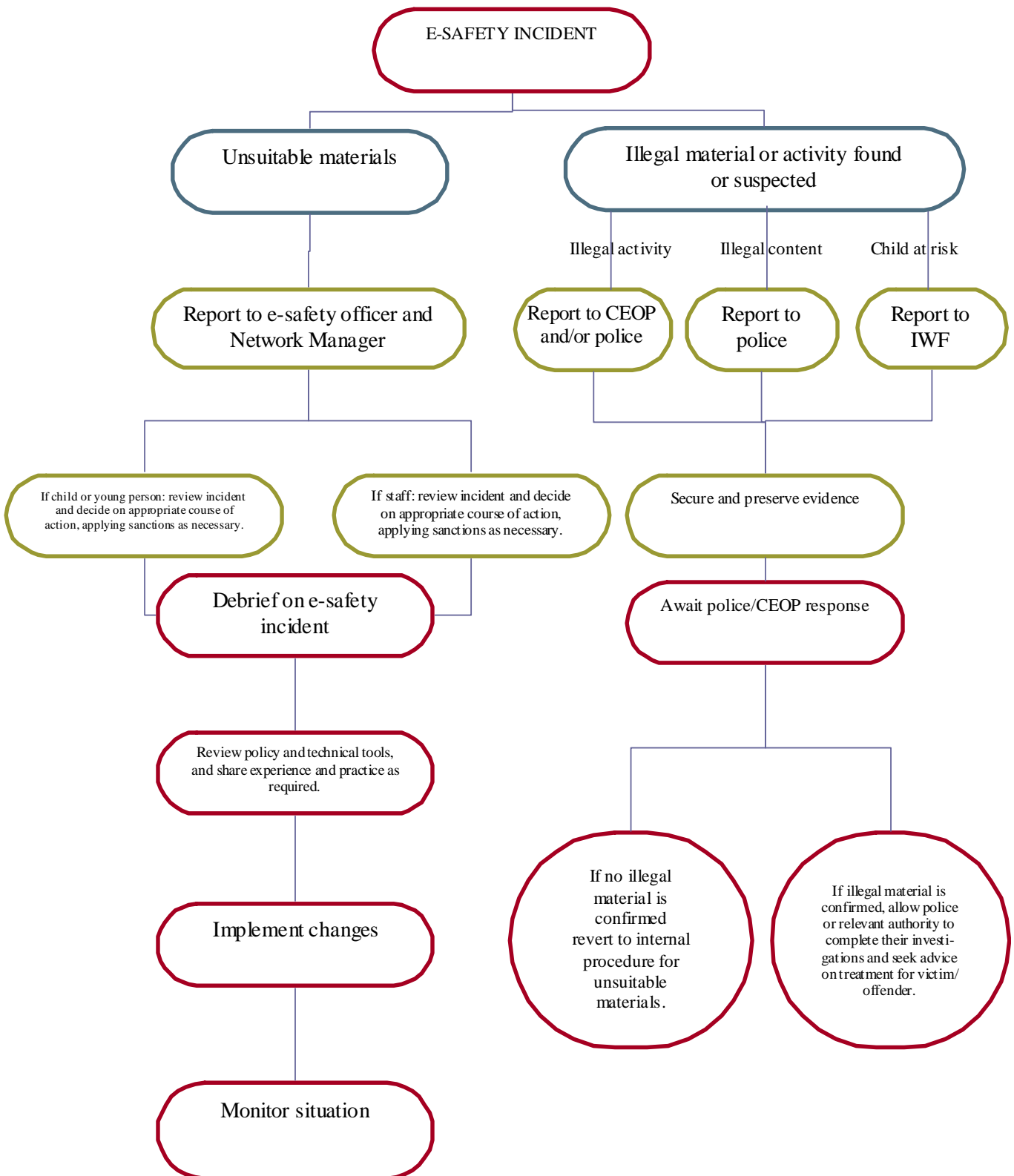
Data Protection Act 1998

http://www.opsi.gov.uk/acts/acts1998/ukpga_19980029_en_1

The Freedom of Information Act 200

http://www.ico.gov.uk/for_organisations/freedom_of_information_guide.a.spx

Flowchart for responding to e-safety incidents.
 (Adapted from BECTA model in AUPs in Context – Feb 2009)



Pupils' Computer Usage Policy

How I use technology at Felsted Preparatory School

I DO:

- ✓ Use the computers to help me research topics for my work.
- ✓ Use the computers to make pieces of work look well presented.
- ✓ Use the computers to communicate with members of staff if I need to be excused from lessons.
- ✓ Use the computers to communicate with members of my family if I don't see them very often i.e. if I am boarding or if my parents go away during term time.
- ✓ Ask a member of staff if I am unsure whether I should be doing something or not or if I need help.
- ✓ Tell a member of staff immediately if I feel uncomfortable or threatened by anything that I see on the internet or receive in an e-mail.
- ✓ Only send e-mails that are polite and friendly.
- ✓ Keep my personal information and passwords safe and will not give them out to anyone.
- ✓ Know how to look after myself and my friends by using the internet in a safe and responsible way.
- ✓ Understand that any I should not use language on the internet or in emails that I would not use in front of a teacher.
- ✓ Understand that I should not use other people's passwords; this includes attempting to log in through another person's account or accessing another person's files (including the pre-prep account).
- ✓ Understand that using other people's work and claiming that it is my own is a crime.

- ✓ Understand that any persistent abuse of the School computer systems will result in my access being suspended or permanently removed.
- ✓ Understand that cyber-bullying is when a person or a group of people threaten, tease, embarrass or abuse someone else by using ICT, particularly mobile phones, the internet and related technologies such as social networks.
- ✓ Know that cyber-bullying will be dealt with as seriously as any real world bullying incident.

Staying safe

If **at any time** you feel unsafe using a computer then find a responsible adult straight away and make sure that Mr Clarke or your Form Tutor are made aware of what is happening.

School Directory

Every pupil in the school is given an area on the Felsted Schools server system to store their work and other important files. *This area is not to be used for storing movies, videos, personal music files or computer games.*

What you can expect to happen if you do not follow these rules

If the Head, Child Protection Officers, Deputy Heads or relevant Head of Year feel that there has been a breach of these rules then the ICT department will investigate the matter fully and accounts will be suspended or deleted if necessary. Appropriate action will also be taken in line with the School's disciplinary policy.

Staff Code of Conduct for ICT

To ensure that members of staff are fully aware of their professional responsibilities when using information systems and when communicating with pupils, they are asked to sign this code of conduct. Members of staff should consult the school's e-safety policy for further information and clarification.

- I understand that it is a criminal offence to use a school ICT system for a purpose not permitted by its owner.
- I appreciate that ICT includes a wide range of systems, including mobile phones, PDAs, digital cameras, email, social networking and that ICT use may also include personal ICT devices when used for school business.
- I understand that school information systems may not be used for private purposes without specific permission from the Head.
- I understand that my use of school information systems, Internet and email may be monitored and recorded to ensure policy compliance.
- I will respect system security and I will not disclose any password or security information to anyone other than an authorised system manager.
- I will not install any software or hardware without permission.
- I will ensure that personal data is stored securely and is used appropriately, whether in school, taken off the school premises or accessed remotely.
- I will respect copyright and intellectual property rights.
- I will report any incidents of concern regarding children's safety to the e-Safety Officer, the Child Protection Office or relevant Head of Year.
- I will ensure that electronic communications with pupils including email, IM and social networking are compatible with my professional role and that messages cannot be misunderstood or misinterpreted.
- I will promote e-safety with children in my care and will help them to develop a responsible attitude to system use, communications and publishing.

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

I have read, understood and accept the Staff Code of Conduct for ICT.

Signed: Printed: Date:

Accepted for school: Printed:

Felsted Preparatory School
eSafety Incident Log

Details of ALL eSafety incidents to be recorded by the eSafety Officer. This incident log will be monitored termly by the Head, Head of ICT or Chair of Governors. Any incidents involving Cyber bullying should be recorded separately by the relevant Head of Year.

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

Monitoring and Evaluation

This policy is monitored when procedures described above are implemented. They are adjusted as necessary following experience. The policy is evaluated in accordance with the School's evaluation cycle and the Header at the top of this policy.