Felsted

E-SAFETY AND COMPUTER USAGE POLICY

COVERING BOTH SCHOOLS INCLUDING EYFS AND BOARDING

Governors' Committee normally reviewing:	Governance Committee
Date last formally approved:	Autumn Term 2018
Date policy became effective:	Autumn 2016 – as a policy for both schools

Period of Review:	Annually
Next Review Date :	Autumn Term 2019
Previous Reviews:	Previously approved as separate policies for Prep School and Senior School

Person responsible for implementation and monitoring :	Head of ICT Services Designated Safeguarding Leads E-Safety Officers
Other relevant policies :	• Safeguarding (Child Protection and Staff Behaviour) Policy • Social Media Policy • Preventing Radicalisation Policy • Discipline and Exclusions Policy • Data Protection Policy • Taking, Storing and Using Images Policy • Anti-Bullying Policy (Senior School) • Pastoral Care Plan including Anti-Bullying and the Behaviour and Discipline Policy (Prep School)

The following Policy encompasses the Aims and Ethos of the Preparatory School and the Senior School

Mr Simon James
Head, Preparatory School

Mr Chris Townsend
Head, Senior School

Aims and Ethos

SAFEGUARDING STATEMENT
Felsted is committed to maintaining a safe and secure environment for all pupils and a 'culture of vigilance' to safeguard and protect all in its care, and to all aspects of its 'Safeguarding (Child Protection and Staff Behaviour) Policy'.

EQUAL OPPORTUNITIES STATEMENT
The aims of the School and the principles of excellent pastoral care will be applied to all children irrespective of their race, sex, disability, religion or belief, sexual orientation, gender reassignment or pregnancy or maternity; equally these characteristics will be recognised and respected, and the School will aim to provide a positive culture of tolerance, equality and mutual respect.

E-SAFETY AND COMPUTER USAGE POLICY

1. INTRODUCTION

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

This policy applies to all members of the School community, including staff, pupils, parents, and visitors. It is the responsibility of relevant staff to make sure pupils understand the Pupils' Computer Usage Policy (Appendix 1 or Appendix 2).

2. RATIONALE

ICT and computing 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 equip 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
- Cloud computing, such as Google Drive, iCloud Drive and One Drive
- Blogs and Wikis
- Podcasting
- Video Broadcasting
- Music Downloading
- Gaming
- Chromebooks and Laptops
- 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 within the law 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. Everybody in the School has a shared responsibility to secure any personal data and sensitive information used in their day to day professional duties and even staff not directly involved in data handling are made aware of the risks and threats and how to minimise them.

Both this policy and the computer usage agreements (for all staff and pupils), copies attached, are inclusive of both fixed and mobile internet; technologies provided by the

School (such as PCs, chromebooks, laptops, tablets, webcams, whiteboards, voting systems, digital video equipment, etc); and technologies owned by pupils and staff, but brought onto school premises (such as chromebooks, laptops, mobile phones, tablets, camera phones and portable media players, etc).

3. MONITORING

The School has appropriate filters and monitoring in place as part of our obligation to comply with Keeping Children Safe in Education (September 2018) and the Prevent Duty.

The School requires all users of the wireless network to log in using their school supplied credentials. Users who access the network on a personal device must first register the device on the network. The School monitors online activity and is able to identify individuals as part of this process. A reporting system is in place for Designated Safeguarding Leads (DSLs) and the Senior Leadership Team (SLT) to monitor online activity and easily identify any areas of concern.

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 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, including serious conduct or welfare concerns, extremism and the protection of others. 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 2018, 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 2018, 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.

The School recognises that pupils and staff can access 3G and 4G technology on the School premises. All pupils are taught how to keep themselves safe online (see Section 9 of this policy) and the School works with parents on promoting e-safety awareness. The School's procedures for pupil access to mobile phones and staff use of mobile devices is provided in Section 14.2 of this policy.

4. BREACHES OF POLICY

4.1 Response to a Data breach by staff

In the event of **any** data breach, this must be reported immediately to the relevant Head (Teaching staff) or the Bursar (Operational staff) and the Compliance Manager (compliance@felsted.org).

A personal data breach is a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data. This will include almost any loss of, or compromise to, personal data held by the School regardless of whether the personal data falls into a third party's hands.

The School must generally report a data breach to the Information Commissioner's Office (ICO) without undue delay and within 72 hours if it presents a risk to individuals. In addition, the School must notify individuals affected if that risk is high. In any event, the School must keep a record of any personal data breaches, regardless of whether there is a need to notify the ICO.

4.2 Response to a Breach of Policy

A deliberate breach of this policy will be dealt with as a disciplinary matter using the School's usual procedures. In addition, a deliberate breach may result in the School restricting access to School IT systems.

4.3 *Incident Reporting*

Any breach that may be a breach of personal data must be reported immediately, following the procedure in 4.1 and within the Data Protection Guidance for Staff.

Any attempted or successful security breaches; loss of equipment; unauthorised use or suspected misuse of ICT; or unauthorized attempts to access personal data must be immediately reported to the School's Head of ICT Services and the eSafety Officer in the first instance. 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 Services.

All eSafety incidents involving either staff or pupils should be recorded on the eSafety incident log by the Director of Digital Learning & Technology (Prep) or Deputy Head (Welfare) (Senior). A copy is attached to this policy.

4.4 Complaints

Complaints and/or issues relating to eSafety should be made to:
Prep School:
Designated Safeguarding Lead
Senior School:
Deputy Head (Welfare)
Incidents should be logged and the School procedure for investigating an eSafety incident should be followed.

4.4 Inappropriate Material

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

Deliberate access to inappropriate materials must be reported to the DSL and the esafety Officer and logged. Depending on the seriousness of the offence there will follow; investigation by the Deputy Head/Head, immediate suspension, possibly leading to dismissal and involvement of police for very serious offences (see flowchart).

Where the allegation(s) concern the Head, the staff member should report the matter to the Chairman of Governors.

5. 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 School's 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.

6. ROLES AND RESPONSIBILITIES

As eSafety is an important aspect of strategic leadership within the School, the Heads and governors have ultimate responsibility and delegate to the Heads and Deputy Heads to confirm and report back that the policy and practices are embedded and monitored. The named eSafety Officers are **Jacqueline Atkins (Designated Safeguarding Lead - Prep School)** and **Tina Oakley-Agar (Senior School)**. All members of the School community have been made aware of who holds these posts. It is the role of the eSafety Officer to keep abreast of current issues and guidance through organisations such as the DfE, CEOP (Child Exploitation and Online Protection), NSPCC and Childnet.

This policy, supported by the School's computer usage agreements for staff, 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.

7. 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 the regular installation of software updates and virus definitions.

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.

8. DATA SECURITY

8.1 Guidelines, Responsibility and Management of Data

The accessing and appropriate use of school data is something that the School takes very seriously. Staff have been issued with, and are required to follow, the E-Safety and Computer Usage Policy, the Data Protection Policy and the Data Protection Staff Guidance. It is the responsibility of individual staff to ensure the security of any personal, sensitive, confidential and classified information. Any individual member of staff who produces any electronic documents that contain personal data are responsible for ensuring secure storage and/or disposal.

Personal data sent or received via email must be downloaded only via agreed channels to the designated storage area, for example MIS. *Sensitive* data must not be stored in any Cloud Based Service. Staff must not hold sensitive or personal data on any device or memory stick that may be transferred out of the school grounds, including personal devices. Should there be an imperative to take personal data outside of the School IT environment, this must be agreed with a Leadership Team (Prep) or Senior Leadership Team (Senior)

member beforehand and either the data or the storage device upon which it resides must be encrypted using a strong encryption algorithm.

When accessing the MIS externally from the school or a school device, staff are required to complete a second authentication phase.

PCs, laptops, chromebooks and/or tablets must be locked or switched off when away from desks/workstations.

Electronic files must be securely deleted and staff should manage their download files either by deleting the files once they have been viewed and are no longer needed or visiting their download folder once a month and deleting files no longer required.

The School password procedures, including the format of the password and frequency of changing passwords, must be followed by all staff.

All staff should log off or lock a computer that they are using before leaving it unattended.

8.2 Personal devices

No personal data should be stored on or downloaded to personal devices. This includes not viewing email attachments if the attachment must be downloaded in order to be viewed.

The School recognises that in certain circumstances some staff may need to use their personal device including phone, tablet, laptop or PC, for work purposes. In this instance staff must only do so if they have the following in place:

- The device has security settings in place with a password, passcode or fingerprint ID setting.
- No personal data is saved to the device, a portable memory facility or cloud storage (other than the School Google account).
- Staff sign out of Google, MIS and any other school system that has been logged in to.
- The temporary download folder on any device used is checked for any documents that may have been downloaded when viewing and are deleted immediately.
- If a personal device is used to access the School email or network systems, the ICT Manager must be notified immediately if this device is lost or stolen so that passwords to school accounts can be changed without delay.

If, in exceptional circumstances, staff need to hold school personal data on a personal device this must only be with permission from the Head and it must be encrypted. Staff are also reminded that they must not use their personal email accounts or personal mobile phones to make contact with students of the School expect in circumstances where prior permission has been given by the Head, as per Section 14.2 of this policy, the School's Safeguarding (Child Protection and Staff Behaviour) Policy and Social Media Policy.

9. STUDENT AND STAFF EDUCATION AND TRAINING

9.1 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 and computer science lessons, as well as during tutorial sessions. This is delivered by the eSafety Officers across the School as well as in ICT/Computer Science teachers in the Senior school.

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.

E-Safety tips are included on the Senior School MIS and are updated on a weekly basis.

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 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, NSPCC or CEOP report abuse button.

In PSHE, pupils cover the topic of staying safe online, including understanding the risks of talking to strangers online and recognising the danger signals when using chat rooms. Cyber-bullying is also explored in depth.

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

9.2 eSafety Skills Development for Staff

New staff receive information on the school's ESafety and Computer Usage Policy and the Data Protection Staff Guidance 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.

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

Our staff receive regular information and training on eSafety issues and data protection in the form of INSET or operational staff training sessions from the eSafety Officer, Designated Safeguarding Lead, ICT Manager, Compliance Manager or a nominated person. Data protection training is also provided via online training.

10. SYSTEMS AND ACCESS

10.1 Guiding Principles and Regulations

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 logins, account IDs and passwords and not allow them to be used by anyone else.

Enforced password changes take place on an annual basis for all members of staff.

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 (special category), 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, libellous, 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).

Where necessary, staff should 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. This is particularly relevant when downloading images for use in school from search engines such as Google, Bing, Yahoo, etc.

10.2 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'.

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. Staff must not use personal email addresses for school work and should refrain from using their school email account for personal business.

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.

MIS must be used to generate any emails being sent to more than one pupil or parent. Email addresses should be generated via *Lists and Labels*, using the '*Email these parents/pupils'* option. When sending **any** emails to personal email addresses, for example the email address of a parent, the email address **must** be entered into the **'Bcc' (**blind carbon copy) email address line. Parent or any other personal email addresses must never be entered into the 'To' or 'Cc' of the address line.

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

Members of staff should make every effort to ensure that emails are genuine before opening attachments or clicking on links within emails. If they are in any doubt then members of staff should, where practical, contact the sender to confirm that the email is genuine, and under no circumstances open attachments or click links if the sender is not known to then and if they are not expecting to receive email from the sender.

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 DDLT (Prep) or Deputy Head (Welfare) (Senior) 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.

Pupils in the Sixth Form wishing to access email via an app on their tablet or smartphone may make a request to do so to the ICT Department. The ICT Department shall ensure that the pupil's password is of sufficient strength before allowing such access and may enforce a regular password change to maintain the security of the email system.

10.3 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.

The following should be followed:

- 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. Staff are advised to be particularly cautious with the increased use of social media and retain a positive tone at all times, ensuring that the reputation of the School, its staff and governors are promoted and protected and that stakeholders understand their ambassadorial role with regards to Felsted.
- 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 or blogs.
- The School uses management control tools for controlling and monitoring workstations.

It is the responsibility of the School, by delegation to the ICT 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 Head of ICT Services 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 Services/DDLT.

If there are any issues related to viruses or anti-virus software, the DDLT/Head of ICT Services should be informed immediately.

10.4 Managing Web 2.0 Technologies (see Social Media Policy)

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 allows time-controlled use of these sites on the school network.

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.

11. PROTECTING PERSONAL, SENSITIVE, CONFIDENTIAL AND CLASSIFIED INFORMATION

All users should:

- Ensure that any School information accessed from your own PC or other media equipment is kept secure.
- Ensure that you log off or lock the screen 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.
- Not share any pupil, parents or staff personal data with third parties unless there is a lawful reason to do so and/or a third party agreement is in place.
- 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.
- 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 the screen display out of direct view of any third parties when you are accessing personal, sensitive, confidential or classified information.
- Ensure that hard copies of data are securely stored and disposed of after use.

- Paper records containing personal data must be kept under lock and key. Records which contain sensitive or confidential information should be stored in a designated secure location with additional security. Sensitive/personal data held in paper form must be shredded via the external company process when no longer required. Any individual member of staff who produces any hard copy documents (including photocopying) that contain personal data are responsible for ensuring secure storage and/or disposal.
- Electronic files must be securely deleted by the secure methods provided within the Data Protection Staff Guidance.
- Select the most appropriate storage medium and location for personal information and especially personal information of a sensitive nature. Sensitive (special category) data must not be stored in any Cloud Based Service.
- Refrain from emailing personal information to their own personal email account and from sharing cloud based documents with their own personal cloud storage accounts.
- Ensure that personal data is not taken outside of the School IT environment unless under circumstances approved by a LT/SLT member and with approved encryption by the ICT Manager.

12. REMOTE ACCESS

Remote access to the School network is generally available via WinSCP. In exceptional circumstances, remote access to a specific machine can be granted after consultation with the Head of ICT.

Individuals are responsible for all activity via a remote access facility and must only use equipment with an appropriate level of security for remote access. Remote access to the School's Management Information System (MIS) is granted to members of staff subject to their setting up a "secret phrase".

Staff should:

- 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, as per section 8.1 and section 11 of this policy.

13. SAFE USE OF IMAGES

Digital images are easy to capture, reproduce and publish and, therefore, misuse. The Taking, Storing and Using Images Policy must be followed for the storing and use of images of pupils, staff or visitors.

14. ICT EQUIPMENT WITHIN SCHOOL

14.1 PCs and Other School Equipment

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.

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 either stored on the School's network, or within a school provided clouds based service, 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 our 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.

14.2 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, gaming devices, tablets, mobile and smartphones are familiar to children outside 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.

Permission must be sought before any image or sound recordings are made on these devices of any member of the School community.

The School is not responsible for the loss, damage or theft of any personal mobile device.

Users bringing personal devices into school must ensure that there is no inappropriate or illegal content on the device.

14.2.2 Pupils

Prep School

With permission from the appropriate Head of Phase or the Houseparent, Year 7 and Year 8 pupils who travel on the School minibuses 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.

Boarders use the Hamilton House WiFi code to Skype or Facetime under supervision. Phones are kept secure in their private safes and boarding pupils are taught to use their phones responsibly.

Senior School

All pupils are permitted to bring a mobile phone to school but Years 9 and 10 must hand in their phones before lessons to a member of the House staff where they will be kept in a secure location. Pupils are permitted access to their devices at the end of the School day but must hand them in again before prep time and bedtime each evening. Year 11-13 students are permitted possession of their mobile phones at all times but must use their phones responsibly and never during lesson time.

All pupils are allowed to bring a Chromebook, iPad or other larger device to lessons but they must be used in an educational context only. For year 9s and 10s, these devices must be handed in at bedtime.

14.2.2 Staff

Stewart House (including EYFS)
Staff, volunteers and visitors are not permitted to use a personal mobile or other personal device to make telephone calls, take photographs or videos **at any time.**

This includes the following areas:

- Stewart House
- Swimming pool
- Changing room
- School grounds
- Forest School area
- Whilst on School trips

A telephone is available at the Stewart House office for emergency calls and school devices are available to use whilst on the School site or for trips off site.

Staff must keep personal devices out of reach and out of sight. If staff see an adult with a device whilst children are present this must be reported to **Mrs J Atkins** (*Head of Stewart House*) prepdsl@felsted.org

Prep School
The Prep 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, except in limited circumstances such as school trips or away matches that have been given prior approval by the Head.

Use of personal devices must not interfere with staff duties; personal mobile telephones and cameras should not be used when members of staff are teaching or involved in an activity with the pupils and their use should be limited to break times or such other times that staff are not carrying out teaching, supervisory or similar duties.

Staff are not permitted to use a personal mobile to take photographs or videos of pupils. Some school provided digital cameras or devices are available from the Director of Digital Learning (DDLT) and must only be used with prior approval for a particular purpose, such as to display a pupil's artwork, where it is necessary to record pupil progress or as part of the Schools Taking, Storing and Using Images Policy. Photos cannot be used or passed on outside the School without parental consent or a data sharing agreement in place.

The use of school provided (or in exceptional circumstances with the prior approval of the Head, personal) mobile phones by staff to contact children can only be for the better preferment of their professional duties. The group leader on all trips and visits involving an overnight stay should take a School mobile phone with him/her and may ask the pupils for their mobile numbers before allowing them out in small, unsupervised groups. The School mobile should be used for any contact with pupils that may be necessary. The group leader will delete any record of pupils' mobile phone numbers at the end of the trip or visit and should ensure that pupils delete any staff numbers that they may have acquired during the trip.

The School Boarding phones hold the numbers of the boarders and their families.

Senior School
The School allows staff to bring in personal mobile phones and devices for their own use. Use of personal devices must not interfere with staff duties; personal mobile telephones and cameras should not be used when members of staff are teaching or involved in an activity with the pupils and their use should be limited to break times or such other times that staff are not carrying out teaching, supervisory or similar duties.

Under no circumstances does the School allow a member of staff to contact a pupil or parent/carer using their personal device except in limited circumstances such as school trips

or away matches that have been given prior approval by the Head. Prior approval may also be given by the Head of the Senior School for staff to communicate professionally with pupils on School premises for safety reasons.

Where pupil mobile numbers are taken for the purpose of school trips and away days, the member of staff in charge of the excursion will ensure that any record of pupils' mobile phone numbers are securely deleted at the end of the trip or visit and will ensure that pupils also delete any staff numbers that they may have acquired during the trip.

Staff are not permitted to use a personal mobile to take photographs or videos whilst around pupils. Some school provided cameras or devices are available and must only be used with prior approval for a particular purpose or as part of the Schools Taking, Storing and Using Images Policy. Photos cannot be used or passed on outside the School without pupils consent or a data sharing agreement in place.

Both Schools
Staff are not permitted to accept personal calls during teaching times.

Staff are strictly prohibited from bringing any inappropriate or offensive material, such as indecent images and/or pornography, to the School site, in to the School IT environment or at any other time they are on duty (such as school trips). Staff must not use school property or the School network to access any such material or use their personal devices. If staff discover any material that is potentially illegal or inappropriate, they must immediately contact the DSL in accordance with the School's Safeguarding (Child Protection and Staff Behaviour) Policy.

In all other circumstances other than school trips and away matches, if staff need to speak to a pupil by telephone, they should use one of the School's telephones and email using the School system.

Staff should be aware that it is not appropriate to use social media to communicate with pupils. Staff must never be friends or linked with current pupils on any form of social media. If staff wish to connect with pupils who have recently left the School, they should speak to the Head and seek their prior approval. Please see the E-Safety and Computer Usage Policy and the Social Media Policy for staff obligations in relation to electronic communication with pupils.

15. TERMINATION OF ACCESS

15.1 Staff
Upon leaving the employment of Felsted School, members of staff shall have their Windows Domain, Google Suite and Management Information System (MIS) access withdrawn immediately. Access to email, via webmail only, shall be retained, in the case of a member of Common Room, for one term after termination of employment. For other members of staff, access shall be terminated immediately. This period of access may be extended or reduced at the discretion of the Head of the School under which the member of staff was employed. In instances where the account is role-based rather than a personal one then the account shall remain active, but the password shall be changed immediately, either by their line manager or by the Head of ICT Services, after the employee leaves.

15.2 Pupils
Pupils leaving the School at the end of the Sixth form shall retain their Management Information System (MIS) access until the start of the following academic year so as to allow them to retrieve their public examination results. These pupils shall also retain access to email, via webmail only, for a period of one year after leaving the School.

Pupils leaving the School at the end of Year 11 shall retain access to the MIS until the start of the following academic year so as to allow them to retrieve their public examination results.

Access to Windows Domain Accounts shall be terminated at the point at which a student leaves the School, and access to email shall be terminated for all students upon leaving the School except as described above.

16. CURRENT LEGISLATION

16.1 Acts Relating to Monitoring of Staff eMail

Data Protection Act 2018
http://www.legislation.gov.uk/ukpga/2018/12/contents/enacted

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

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

Human Rights Act 1998
http://www.hmso.gov.uk/acts/acts1998/19980042.htm

16.2 Other Acts Relating to eSafety and personal data

- Racial and Religious Hatred Act 2006
- Sexual Offences Act 2003
- Communications Act 2003 (section 127)
- The Computer Misuse Act 1990 (sections 1 – 3)
- Malicious Communications Act 1988 (section 1)
- Copyright, Design and Patents Act 1988
- Public Order Act 1986 (sections 17 – 29)
- Protection of Children Act 1978 (Section 1)
- Obscene Publications Act 1959 and 1964
- Protection from Harassment Act 1997
- Cloud Computing Services (2006)
  https://www.gov.uk/government/publications/cloud-computing-how-schools-can-move-services-to-the-cloud

APPENDIX 1: PUPILS' COMPUTER USAGE POLICY – PREP SCHOOL

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 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 login through another person's account or accessing another person's files.
- ✓ Understand that using other people's work and claiming that it is my own is a serious offence.
- ✓ 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 your Head of Phase 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 Director of Digital Learning, Designated Safeguarding Lead, Deputy Head or relevant Head of Phase consider 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 Pastoral Care Plan, including Behaviour and Discipline Policy and Anti-bullying Policy as well as the School Safeguarding (Child Protection) Policy.

I agree to the Terms and Conditions of the Pupils' Computer Usage Policy

Signed: …… Print Name: …… Date: ……

APPENDIX 2: PUPILS' COMPUTER USAGE POLICY – SENIOR SCHOOL

How I use technology at Felsted 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

I DO NOT:

- Use language on the internet or in emails that I would not use in front of a teacher
- Use other people's passwords; this includes attempting to log in through another person's account or accessing another person's files
- Access inappropriate material such as pornography, gambling websites or anything promoting violence or extremist views

I UNDERSTAND THAT:

- Using other people's work and claiming that it is my own is a serious offence
- Any persistent abuse of the School computer systems will result in my access being suspended or permanently removed
- 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

- 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 the Deputy Head (Welfare) or your HM 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 Headmaster, Designated Safeguarding Lead, Deputy Heads or relevant responsible Senior Leaders consider 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. Any form of Cyber-bullying is regarded as an exceptionally serious offence.

I agree to the Terms and Conditions of the Pupils' Computer Usage Policy

Signed: …… Print Name: …… Date: ……

APPENDIX 3: STAFF CODE OF CONDUCT FOR ICT – BOTH SCHOOLS

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 and Computer Usage Policy for further information and clarification.

1. I understand that it is a serious 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, tablets, 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 Headmaster
- 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 (with the permission of a member of LT/SLT and encryption approved by the ICT department) or accessed remotely
- I will not share any pupil, parents or staff personal data with third parties unless there is a lawful reason to do so and/or a third party agreement is in place
- I will respect copyright and intellectual property rights.

2. I understand that it is my duty to promote e-Safety with children in my care, to report any matters of concern, and to use electronic communications of any kind in a professional and responsible manner.

- 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
- I will report any incidents of concern regarding children's safety to the Director of Digital Learning & Technology/-Safety Officer, the Designated Safeguarding Lead or relevant Housemaster/Housemistress
- I will ensure that electronic communications with pupils, including email, are compatible with my professional role and comply with the School Safeguarding (Child Protection and Staff Behaviour) Policy.

3. I understand that my use of school information systems, Internet and email may be monitored and recorded to ensure policy compliance.

- I will ensure that I comply with the School's E-safety and Computer Usage Policy and other relevant policies including the Data Protection Policy, Social Media Policy, Record Keeping Policy and the Safeguarding (Child Protection and Staff Behaviour) Policy.

  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 agree to the Terms and Conditions of the Staff Computer Usage Agreement and Code of Conduct for ICT

Signed: …… Print Name: …… Date: ……

SAFEGUARDING STATEMENT
Felsted is committed to maintaining a safe and secure environment for all pupils and a 'culture of vigilance' to safeguard and protect all in its care, and to all aspects of its 'Safeguarding (Child Protection and Staff Behaviour) Policy'.

EQUAL OPPORTUNITIES STATEMENT
The aims of the School and the principles of excellent pastoral care will be applied to all children irrespective of their race, sex, disability, religion or belief, sexual orientation, gender reassignment or pregnancy or maternity; equally these characteristics will be recognised and respected, and the School will aim to provide a positive culture of tolerance, equality and mutual respect.

E-SAFETY AND COMPUTER USAGE POLICY

APPENDIX 4: EXAMPLE OF E-SAFETY INCIDENT LOG

Details of ALL eSafety incidents to be recorded by the eSafety Officer.

This incident log will be monitored termly by the Head, Deputy Head (Welfare) Assistant Head (ICT) or Chair of Governors. Any incidents involving Cyber bullying should be recorded in the Bullying Log.

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

APPENDIX 5: FLOWCHART FOR RESPONDING TO ESAFETY INCIDENTS