Felsted

ONLINE SAFETY AND ICT ACCEPTABLE USE POLICY

COVERING BOTH SCHOOLS INCLUDING EYFS AND BOARDING

Governors' Committee normally reviewing:	Governance Committee
Date last formally approved:	Autumn Term 2022
Date policy became effective:	Autumn 2016 – as a policy for both schools

Period of Review:	Annually
Next Review Date:	Autumn Term 2023
Previous Reviews:	Previously E-Safety and Computer Usage Policy

Person responsible for implementation and monitoring:	Director of Digital Strategy Designated Safeguarding Leads
Other relevant policies : ● Safeguarding (Child Protection and Staff Behaviour) Policy ● Social Media Policy ● Preventing Radicalisation Policy ● Behaviour and Discipline Policy ● Data Protection Policy	● Taking, Storing and Using Images Policy ● Anti-Bullying Policy ●

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

ONLINE SAFETY AND ICT ACCEPTABLE USE POLICY

1. INTRODUCTION

This policy supports the aims of Felsted School ("the School") in educating the School community to explore horizons in line with the digital world safely and setting up a safety net for pupils and staff.

This policy applies to all members of the School community, including staff, pupils, parents, and visitors and includes use of the Schools' IT accounts, systems and devices while on and away (for example online learning and school trips) from the school site. It is the responsibility of relevant staff to make sure that pupils understand the Pupils' Computer/Device Usage Agreement (Appendix 1, Appendix 2 or Appendix 3). It is the responsibility of managers to ensure that all staff who access the School's IT environment understand and accept the Staff Code of Conduct for IT (Appendix 4). All staff (including volunteers) and any other users of our IT are expected to adhere to this policy.

The School has additional guidance in place for the delivery of online learning where classes are held remotely during any period of school closure, including:

- Online Learning: Policy and Procedures for Teaching Staff
- Online Learning: Guidance for Parents
- Remote Learning: Prep School
- Online Curriculum: Senior School

2. RATIONALE

Information Technology includes a wide range of resources including web-based, mobile, and blended learning. It is important to recognise the constant and fast paced evolution of IT within our society as a whole. Currently the internet technologies children and young people are using inside and/or outside of the classroom include:

- Websites
- Learning Platforms, Virtual Learning Environments, Artificial Intelligence
- E-mail and Instant Messaging
- Chat Rooms
- Social Networking
- Cloud computing, such as Google Drive, iCloud Drive and OneDrive
- Blogs and Wikis
- Podcasting
- Video Broadcasting
- Music Streaming and/or Downloading
- Film or TV streaming
- Gaming
- Mobile devices, such as Chromebooks, Laptops, iPADs, Tablets, etc.
- Mobile/Smart phones with text, video and/or web functionality
- Other mobile devices with web functionality, including Apple Watches.

Whilst exciting and beneficial, both in and out of the context of education, much IT, particularly web-based resources, are not consistently monitored. All users need to be aware of the range of risks associated with the use of these digital technologies. At Felsted School, we understand the responsibility to educate our pupils about the importance of online safety issues; helping them to raise their awareness and develop 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. Building these important skills and strategies, will help them to become model digital citizens in a complex HyFlex world ahead.

This policy and the Computer/Device Usage Agreements for all staff and pupils (see Appendix 1, 2, 3 and 4) apply to technologies and accounts provided by the School (such as Google Workspace for Education accounts (including Gmail and other Google Apps), access to the School's database and software systems (e.g. iSAMs, Century Tech, etc.), PCs, chromebooks, mobile devices, laptops, tablets, webcams, interactive whiteboards, voting systems, digital video equipment, etc); and to technologies owned by pupils and staff, brought onto school premises (such as chromebooks, laptops, mobile devices, tablets, portable media players and any other internet enabled device) or used from home when logged in to a School account, to complete School work.

3. ROLES AND RESPONSIBILITIES

As online safety is an important aspect of strategic leadership within the School, the 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 Online Safety Officers are the **Director of Digital Strategy, and the Designated Safeguarding Leads**. All members of the School community are made aware of who holds these posts. It is the role of the Online Safety Officers 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/Device Usage Agreements for staff and pupils, is to protect the interests and safety of the entire school community; it is linked to the school policies listed in the introduction to this policy.

4. MONITORING

The School has appropriate filters and monitoring in place as part of our obligation to comply with Keeping Children Safe in Education (September 2022) and the Prevent Duty.

The School is constantly reviewing industry trends to improve filtering and monitoring of internet use in accordance with Keeping Children Safe in Education and any other Department for Education and online safety statutory guidance.

The School requires all users of the wireless and local network to login using their school supplied credentials. 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 identify any areas of concern.

The School recognises that pupils and staff can access the internet over mobile phone operators 3G/4G/5G connections. Parents are advised to make use of the filtering and monitoring facilities provided by their mobile phone operator on these connections. All pupils are taught how to keep themselves safe online (see Section 5 of this policy) and the School works with parents on promoting online safety and e-safety awareness. The School's procedures for pupils and staff access to, and use of, mobile devices is provided in Section 5.8 and 6.3.2 of this policy.

5. PUPILS

5.1 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 online safety/e-safety guidelines and regulations.

However, staff are aware that some pupils may require additional support, including reminders, prompts and further explanation to reinforce their existing knowledge and understanding of online safety/e-safety issues.

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

5.2 Education

IT and online resources, including collaborative online spaces, are increasingly used across all areas of the curriculum. The School makes extensive use of the Google Workspace For Education collaborative applications, both in class and for prep work.

We believe it is essential for online safety/e-safety guidance to be given to the pupils on a regular and meaningful basis. Online safety/e-safety is embedded within our curriculum, with many PSHE lessons addressing key areas of digital citizenship and online safety, and we continually look for new opportunities to promote online safety/e-safety.

The School has a framework for teaching internet skills, including in ICT and Computer Science lessons.

Educating pupils on the potential dangers of technologies that may be encountered, including the emotional and social aspects of emerging technologies, is done informally when opportunities arise and as part of the curriculum.

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

Pupils are taught about digital citizenship, copyright, and the importance of respecting other people's information, images, and opinions, through collaborative discussion and activities.

Pupils are aware of the impact of cyberbullying/online bullying and know how to seek help if they are affected by any form of cyberbullying. 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.

Pupils are taught to critically evaluate digital resources and materials, and to build effective and efficient online searching skills through cross-curricular teacher models and discussions.

The School works closely with parents to help them support the online safety of pupils, including talks by external speakers, the DSL & DDS speaking at parents' evenings, information and guidance via School newsletters and working with parents on an individual basis where extra support is needed.

5.3 Email

The use of email within most schools is an essential means of communication for both staff and pupils. We recognise that pupils need to understand how to appropriately style an email in relation to their age, their audience, and with good network etiquette.

All pupil email users are expected to adhere to the generally accepted rules, particularly in relation to the use of appropriate language, not revealing any personal details about themselves or others in email communication (e.g. name, date of birth, address, telephone number, etc.), not arranging to meet anyone without specific permission, and checking for/ not opening virus attachments/links.

Pupils are introduced to email as part of the ICT Scheme of Work. However, pupils access school email, all the school email policies apply.

5.4 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 through the Felsted School Network is logged and is subject to the Schools' online monitoring and filtering.

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, including Google image searches.
- Users must not post personal, sensitive, confidential or classified information or disseminate such information in any way that may compromise its intended restricted audience.
- On-line gambling is not allowed.
- Access to websites that could be categorised as "adults only" is not permitted, even if the pupil is over the age of 18.
- Pupils are aware that school based email and internet activity can be monitored and explored further if required.
- The School uses management control tools for controlling and monitoring workstations.

It is the responsibility of the School, by delegation to the Head of IT and the Director of Digital Strategy, to ensure that anti-virus protection is installed and kept up-to-date on all school machines. It is not the School's responsibility to install or maintain virus protection on any personally-owned devices.

Removable media (personal or for school use) should not be used on school devices.

Pupils are not permitted to download programs on school based technologies without seeking prior permission from the IT Department.

Pupils must never interfere with any monitoring software installed on the School's IT equipment.

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

5.5 Social Media (see Social Media Policy)

Social media, 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 carefully reflect about the way that information can be added and removed by all users, including themselves, from these sites. Information which is captured by third parties, automatically or through 'cookies' consent, can be stored as part of their digital footprint, transferred externally and/or used within advertisement frameworks to build digital profiling.

At present, the School allows time-controlled use of sites on the School network, depending on the terms of service and age requirements for the relevant social media platform. Certain sites / platforms may be blocked for certain pupils to access via their school login, depending on a pupils age and the age restrictions of the site.

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 from their digital footprint. It is important to remember that anything and everything may always be captured when connecting online, including the sites visited.

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

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 and opinions online, especially where they may intentionally or unintentionally cause others harm.

Pupils are advised to carefully read the Terms and Conditions, including any age restrictions on the use of any website before signing up. Pupils are equally encouraged to check with a trusted adult, if unsure about the safety or any website, before registering to join any online community.

5.6 Inappropriate Material

Accidental access to inappropriate materials must be immediately reported to a DSL.

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

5.7 Viruses

Pupils must never interfere with any anti-virus software installed on School IT equipment.

If a machine is not routinely connected to the school network, pupils must make provision for the regular installation of software updates and virus definitions.

If pupils suspect there may be a virus on any school IT equipment, they must stop using the equipment immediately and contact the IT department. The IT department will advise what actions are to be taken, and are responsible for advising others who need to know.

5.8 Personal Devices

5.8.1 Chromebooks to be used in an educational context (including in lessons and prep time)

Chromebooks are our preferred device for pupils. The School makes extensive use of the Google Workspace for Education applications, both in and out of class and for prep work, and the tight integration between Chromebooks and these products, provides the students and teachers with a stable digital learning environment with seamless access to key school IT systems and digital resources**.**

Prep School

All students in Years 5, 6, 7 and 8 are required to have a Chromebook, including supported headphones, to use in School for their academic work across the School week.

Senior School

All students are encouraged to make use of a Chromebook for their academic work in and out of class. From January 2023, all Year 9-11 students will be required to have either a Chromebook, a Windows Laptop, a +11" Tablet/iPAD, or a MacBook, including supported headphones, in school for their academic work across the School week.
All students in Years 5, 6, 7 and 8 are required to have a Chromebook, including supported headphones, to use in School for their academic work across the School week.

5.8.2 Mobile Devices

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. Other pupils may bring their mobile device into School only with the agreement of the Head of Phase for a valid reason and may only access their phone if specifically directed to by a member of staff for a specific task.

Traditional and weekly boarders can bring personal devices for use in Hamilton House. Devices 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 device 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 mobile devices at the end of the School day but must hand them in again before prep time and bedtime each evening. Year 11 students may carry their phone during the day and evening but must hand it in at bedtime. Year 12-13 students are permitted possession of their mobile phones at all times but must use them responsibly and never during lesson time unless permitted by their teacher.

5.9 Monitoring

Trained authorised staff may inspect IT equipment or accounts owned, leased or managed by the School. The School's web filtering and monitoring web service is Smoothwall.

For personal devices, the School's Search Policy must be followed for any search.

If the School suspects that inappropriate images of children may be found on a device, they should first consult the guidance “Sharing nudes and semi-nudes: advice for education settings working with children and young people” to establish whether it is appropriate or not to view the images.

5.10 Issues or Concerns

Issues or concerns relating to online safety/e-safety should be made to the DSL.

Incidents will be logged and the School procedure for investigating online safety/e-safety incidents will be followed.

5.11 Termination of Access

Pupils in the Senior School Sixth Form preparing for university applications, etc., are encouraged to use an alternative email address for these communications (e.g. Gmail, Hotmail, etc.), as Year 13 pupils will lose access to their Felsted School email account and their iSAMs access at the Autumn half term (middle of October) after leaving the School.

Pupils leaving the School at the end of Year 11 will lose access to their iSAMS and Felsted School email account, at the end of August of the year in which they are leaving.

Pupils that leave the School at any other time will have all accounts deactivated as soon as they leave.

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.

6. STAFF

6.1 Monitoring

Deliberate and serious breach of the policy statements in this section may lead to the School taking disciplinary measures in accordance with the School’s Disciplinary Procedure.

All of the School’s ICT accounts (including email, Google accounts and iSAMS), ICT equipment, devices, phone, internet and email related resources are provided for business purposes. Therefore, the organisation maintains the right to monitor internet and network traffic, together with the email systems. The specific content of any transactions may be monitored, investigated and/or used in order to meet the School’s obligations regarding monitoring and filtering arrangements; if there is a suspicion of improper use; to confirm or obtain School business-related information; to confirm or investigate compliance with School policies, standards and procedures (including safeguarding); to ensure the effective operation of School IT; for quality control or training purposes; to comply with a Subject Access Request under the Data Protection Act 2018, or to prevent or detect crime.

IT authorised staff may, without prior notice, but after gaining permission from a member of SLT, 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.

Staff should always exercise caution when committing confidential information to email since the confidentiality of such material cannot be guaranteed. The School reserves the right to monitor electronic communications in accordance with applicable laws and policies. The right to monitor communications includes messages sent or received by system users (employees, volunteers and temporary employees) within and outside the system as well as deleted messages.

6.2 PCs and Other School Equipment

A user of IT is responsible for any activity undertaken on the School's IT equipment provided.

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/chromebook in the boot of a car before starting a journey.

The installation of any applications or software packages must be authorised and carried out by the IT Department.

Portable or mobile IT equipment must not be left unattended and any personal data and/or confidential information must be kept secure and out of sight.

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

6.3 Data Security

6.3.1 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 Online Safety and ICT Acceptable Use 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. All staff must have two factor authentications in place and sensitive category data can only be stored in any Cloud Based Service after assessment and consultation with the IT department. Staff must not hold any 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 the Director of Digital Strategy and a Leadership Team (Prep) or Senior Leadership Team (Senior) member beforehand and the data or the storage device upon which it resides must be encrypted using a strong encryption algorithm.

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 device that they are using before leaving it unattended.

6.3.2 Accessing school systems via 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, iSAMS 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 Head of IT 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.

6.4. Breaches

6.4.1 Response to a Data Breach

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.

6.4.2 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.

6.4.3 Incident Reporting

Any breach that may be a breach of personal data must be reported immediately, following the procedure in 6.4.1 and within the Data Protection Guidance for Staff.

Any attempted or successful security breaches, loss of equipment, unauthorised use or suspected misuse of IT, security breaches, lost/stolen equipment or data, virus notifications, misuse or unauthorised use of IT and any other policy non-compliance must be reported to the Head of IT.

All online safety/e-safety incidents involving either staff or pupils should be recorded on the online safety/e-safety incident log by the Designated Safeguarding Lead (Prep) or Designated Safeguarding Lead (Senior). A copy is attached to this policy.

6.4.4 Inappropriate Material

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

Deliberate access to inappropriate materials must be reported to the DSL 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.

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

6.4.5 Viruses

Anti-virus software installed on school IT equipment must not be interfered with.

If a user suspects there may be a virus on any school IT equipment, they must stop using the equipment and contact the IT Department. They will advise what actions to take and be responsible for advising others who need to know.

The IT Department may assess risk to the School's systems by undertaking controlled phishing tests.

6.5 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 IT equipment or their own device.

No member of staff should allow any unauthorised person to use school IT facilities and services that have been provided for 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 for all members of staff as required.

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 device 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 IT 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, sex-specific comments, or anything that would offend someone on the basis of their age, sex, sexual orientation, gender reassignment, marriage and civil partnership, pregnancy and maternity, race, religion or beliefs or disability (in accordance with the Equality Act 2010).

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 1988. This is particularly relevant when downloading images for use in school from search engines such as Google, Bing, Yahoo, etc.

6.6 Staff Training

New staff receive information on the school's Online Safety and ICT Acceptable Use Policy, Social Media 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 online safety and know what to do in the event of misuse of technology by any member of the school community.

All teaching staff are encouraged to incorporate online safety/e-safety activities and awareness within their curriculum areas.

Our staff receive regular information and training on online safety/ e-safety issues and data protection in the form of INSET or operational staff training sessions from the Online Safety Officer, Designated Safeguarding Lead, Director of Digital Strategy, Head of IT, Compliance Manager or a nominated person. Data protection training is also provided via online training.

6.7 E-mail

The School gives all staff their own email account to use for all school business as a work based tool. Staff must not use personal email addresses for school work and should refrain from using their school email account for personal business.

When using email staff must ensure that they:

- comply with current legislation;
- use email in an acceptable way;
- do not create unnecessary business risk to the School by their misuse of the internet.

In addition, staff are asked to follow the following points on email use:

- When publishing or transmitting information externally, be aware that they are representing the School and could be seen as speaking on the School's behalf. Make it clear when opinions are personal. If in doubt, staff should consult their line manager;
- Keep electronic files of electronic correspondence, only retaining what is needed.
- If sending personal, sensitive and/or confidential information via email, then the following protocols should be used. If there is any doubt as to the information being sent or the appropriate level of protection required, staff should check with the Head of IT:
    - Personal, sensitive and/or confidential information should be sent securely and any attachment should be encrypted. Staff should follow the Data Protection Staff Guidance for further advice on this;
    - Any password or key must be sent separately and preferably communicated by another means e.g. telephone or alternative email address;
    - Before sending the email, staff should verify the recipient by checking the address, and if appropriate, telephoning the recipient to check and inform them that the email will be sent;
- Treat others with respect and in a way in which staff would expect to be treated;
- Do not forward email warnings about viruses. If in doubt, contact the IT Department for advice.

Do not open an email without a reasonably good expectation of what it contains, and do not download files unless they are from a trusted source. It is the responsibility of each account holder to keep the password secure. For the safety and security of users and recipients, all email is filtered and logged; if necessary email histories can be traced.

iSams must be used to generate any emails being sent to more than one pupil or parent. 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. If emails are being blind copied to more than one parent, no other pupil names or any other personal data should be included in the email. If pupil personal data would be shared with a third party, for example another parent, then separate emails must be sent.

All e-mails should be written and checked carefully before sending, including checking attachments.

Staff must inform the DSL (Prep) or DSL (Senior) if they receive an offensive email.

6.8 Use of the Internet

Use of the Internet by staff is permitted and encouraged where such use supports the goals and objectives of the School.

However, when using the Internet, staff must ensure that they:

- comply with current legislation;
- use the internet in an acceptable way;
- do not create unnecessary business risk to the organisation by their misuse of the internet.

In particular, the following is deemed unacceptable use or behaviour by employees and volunteers (this list is non-exhaustive):

- Visiting internet sites that contain obscene, hateful, pornographic or other illegal material;
- Using the device to perpetrate any form of fraud, or software, film or music piracy;
- Using the internet to send offensive or harassing material to other users;
- Downloading commercial software or any copyrighted materials belonging to third parties, unless this download is covered or permitted under a commercial agreement or other such licence;
- Hacking, by means of entering or gaining access to a space/account, into unauthorised areas;
- Creating or transmitting defamatory or insulting material;
- Undertaking deliberate activities that waste employee's effort or networked resources;
- Deliberately or recklessly introducing any form of virus into the School's network.

<u>Chat rooms / instant messaging (IM)</u>
The use of chat rooms and instant messaging is permitted for business use only.

<u>Obscenities/pornography</u>
Staff must not write, publish, look for, bookmark, access or download material that might be regarded as obscene or pornographic.

<u>Copyright</u>
Staff should take care to use software legally and in accordance with both the letter and spirit of relevant licensing and copyright agreements. Copying software for use outside these agreements is illegal and may result in criminal charges. Staff should be aware of copyright law when using content you have found on other organisations' websites. The law is the same as it is for printed materials. Some digital content is published under Creative Commons (cc) licensing which allows some restricted re-use of said content, staff should be aware of these restrictions before reusing or adapting the content.

6.9 Social Media

Staff are required to follow the School's Social Media Policy in relation to use of Social Media, including the use of School accounts, and for advice on managing personal social media profiles.

6.10 Personal Use

Staff should ensure that usage is not excessive and does not interfere with work duties. Use should be restricted to non-working hours, unless this forms part of work responsibilities.

Use of facilities for leisure or personal purposes (e.g. sending and receiving personal email, personal phone calls and browsing the internet) is permitted so long as such use does not:

- incur specific expenditure for the School;
- impact on the performance of a member of staff's job or role (this is a matter between each member of staff and their line manager);
- break the law;
- bring the School into disrepute;
- detrimentally affect the network performance by using large amounts of bandwidth (for instance by downloading/streaming of music or videos);
- impact on the availability of resources needed (physical or digital) for business use.

6.11 Remote Access

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

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 iSAMS System () 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 6.3 of this policy.

6.12 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.

6.13 Mobile and personal devices

Staff must be aware of the Safeguarding (Child Protection and Staff Behaviour) Policy and the Social Media Policy, for staff obligations in relation to the use of mobiles and personal devices and electronic communication with pupils.

6.14 Termination of Access

Upon leaving the employment of Felsted School, members of staff shall have their Windows Domain, Google Workspace for Education and iSAMS System access withdrawn immediately. 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 a member of the IT department or by the Head of IT, after the employee leaves.

6.15 Complaints

Complaints and/or issues relating to online safety/e-safety should be made to the DSL.

Incidents should be logged and the School procedure for investigating an online safety/e-safety incident should be followed.

7. CURRENT LEGISLATION

7.1 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

7.2 Other Acts Relating to online safety/e-safety 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 (2014)
-
- Sexual communication with a child: implementation of s.67 of the Serious Crime Act 2015

APPENDIX 1: PUPILS' COMPUTER/DEVICE USAGE AGREEMENT – Years R- 4

The named responsible adult (class teacher/ learning assistant) will ensure they are aware of the School's Online Safety and ICT Acceptable Use Policy and Social Media Policy, available on the School website: https://www.felsted.org/parents/policies-school-information.

The named responsible adult will share the following rules with the children. They will sign on the children's behalf to state that the following rules for the use of School IT systems, accounts, equipment/devices are adhered to:

How I use technology at Felsted Preparatory School

I KNOW MY TEACHER WILL:

- ✓ Use the internet to help me research topics for my work.
- ✓ Use the internet to make pieces of work look well presented.

I KNOW:

- ✓ I can ask a member of staff if I need help.
- ✓ I can tell a member of staff straight away if I feel worried by anything that I see on the internet or receive in an email or message.
- ✓ To only send messages that are polite and friendly.
- ✓ To keep my personal information and passwords safe and will not give them out to anyone.
- ✓ How to look after myself and my friends by using the internet in a safe way.
- ✓ I understand that I should not use words on the internet or in emails that I would not use in front of a teacher.
- ✓ I understand that I should not use other people's passwords or login through another person's account.
- ✓ I understand that online bullying is when a person or a group of people are unkind by using ICT, mobile phones or the internet.
- ✓ That cyber-bullying will be dealt with as seriously as any real world bullying incident.

Staying safe
If at any time I feel unsafe using a computer/device then I will talk to a responsible adult straight away.

What I can expect to happen if I do not follow the rules
Appropriate action will be taken in line with the School's Behaviour and Discipline Policy, Anti-bullying Policy and the School's Safeguarding (Child Protection and Staff Behaviour) Policy.

On behalf of the children listed, the responsible adult agrees to the Terms and Conditions of the Pupils' Computer/Device Usage Agreement

Signed: …… Print Name: …… Date: …… Class list:

APPENDIX 2: PUPILS' COMPUTER/DEVICE USAGE AGREEMENT – Years 5-8

The School's Online Safety and ICT Acceptable Use Policy and Social Media Policy are available on the School website: https://www.felsted.org/parents/policies-school-information.

This agreement is for the use of School IT systems and School IT (Google) accounts accessed at any time (including during online learning) and equipment/devices and any personal devices (including hand held devices, watches or any other internet enabled device) brought on to the School site or at a School activity.

Pupils should also follow any additional code of conduct / guidelines put in place for online learning from home.

How I use technology at Felsted Preparatory School

I DO:

- ✓ Use internet enabled devices to help me research topics for my work.
- ✓ Use internet enabled devices to make pieces of work look well presented.
- ✓ Use internet enabled devices to communicate with members of staff if I need to be excused from lessons.
- ✓ Use internet enabled devices 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 email or message.
- ✓ Only send emails, messages or any communication 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 ICT systems will result in my access being suspended or permanently removed.

- ✓ Understand that online 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.

Social Media - for any pupils who access social media

If accessing Social Media sites, pupils should:

- Take responsibility for keeping details of their accounts private, using full privacy settings, logging off properly and not allowing others to use their accounts.

- Report anything offensive or upsetting that they see online to the appropriate bodies, either by using the "report abuse" tabs or by speaking to their parents or a member of staff.

- Inform the School if they see inappropriate postings by other students, so that steps can be taken to avoid possible repercussions.

Pupils should not:

- Access any social media that is for adults only or if the pupil does not meet the minimum age requirement.

- Access anonymous sites as there is a high risk that inappropriate comments can be exchanged, causing distress or endangerment.

- Include bad, offensive, explicit or abusive language or inappropriate pictures in messages.

- Include anything that could be upsetting, defamatory or insulting towards others or the School.

- Regard anything posted online as private. Remember that harassment, defamatory attitudes and racism are just some issues which could lead to prosecution.

It is a serious offence to use another person's account, or to create an account in another person's name without their consent.

Staying safe

If **at any time** you feel unsafe using a computer/device 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 School 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 the rules

If the Head, Designated Safeguarding Lead, Deputy Head, relevant Head of Phase or relevant responsible senior leaders consider that there has been a breach of this agreement and/or the school rules (for example following the HOWDI code or the Behaviour Charter) or there is a safeguarding risk to any individuals, then the Head can delegate responsibility for

the matter to be investigated and a search to be carried out by the most appropriate individual. This would normally be a member of the Leadership Team, Phase Leader, or a member of the ICT team.

Appropriate action will also be taken in line with the School's Behaviour and Discipline Policy, Anti-bullying Policy and the School's Safeguarding (Child Protection and Staff Behaviour) Policy.

School accounts may be suspended or deleted if necessary.

I agree to the Terms and Conditions of the Pupils' Computer/Device Usage Agreement

Signed: …… Print Name: …… Date: ……

APPENDIX 3: PUPILS' COMPUTER/DEVICE USAGE AGREEMENT – SENIOR SCHOOL

The School's Online Safety and ICT Acceptable Use Policy and Social Media Policy are available on the School website: https://www.felsted.org/parents/policies-school-information.

This agreement is for the use of School IT systems and School IT (Google) accounts, accessed at any time (including during online learning) and equipment/devices and any personal devices (including hand held devices, watches or any other internet enabled device) brought on to the School site or at a School activity.

Pupils should also follow any additional code of conduct / guidelines put in place for online learning from home.

How I use technology at Felsted School

I DO:

- Use internet enabled devices to help me research topics for my work.
- Use internet enabled devices to make pieces of work look well presented.
- Use internet enabled devices to communicate with members of staff if I need to be excused from lessons.
- Use internet enabled devices 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 email.
- Only send emails, messages or any communication 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.

Use of Social Media

If accessing Social Media sites, pupils should:

- Take responsibility for keeping details of their accounts private, using full privacy settings, logging off properly and not allowing others to use their accounts.

- Report anything offensive or upsetting that they see online to the appropriate bodies, either by using the “report abuse” tabs or by speaking to their parents or a member of staff.

- Inform the School if they see inappropriate postings by other pupils, so that steps can be taken to avoid possible repercussions.

Pupils should not:

- Access any social media that is for adults only or if the pupil does not meet the minimum age requirement.

- Access anonymous sites as there is a high risk that inappropriate comments can be exchanged, causing distress or endangerment.

- Include bad, offensive, explicit or abusive language or inappropriate pictures in messages.

- Include anything that could be upsetting, defamatory or insulting towards others or the School.

- Regard anything posted online as private. Remember that harassment, defamatory attitudes and racism are just some issues which could lead to prosecution.

It is a serious offence to use another person’s account, or to create an account in another person's name without their consent.

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 ICT systems (including the School wi-fi) will result in my access being suspended or permanently removed.

- Online 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.

- Online 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/device then find a responsible adult straight away and make sure that the Designated Safeguarding Lead or your HM are made aware of what is happening.

School Directory

Every pupil in the School is given an area on the Felsted School 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 the rules

If the Head, Designated Safeguarding Lead, Deputy Heads or relevant responsible senior leaders consider that there has been a breach of this agreement and/or the School Rules or there is a safeguarding risk to any individuals, then the Head can delegate responsibility for the matter to be investigated and a search to be carried out by the most appropriate individual. This would normally be a member of the Leadership Team, HM, or a member of the ICT team.

School accounts may be suspended or deleted if necessary.

Appropriate action will also be taken in line with the School's Behaviour and Discipline Policy and Anti-Bullying Policy as well as the School's Safeguarding (Child Protection and Staff Behaviour) Policy.

Any form of online bullying is regarded as an exceptionally serious offence.

I agree to the Terms and Conditions of the Pupils' Computer/Device Usage Agreement

Signed: …… Print Name: …… Date: ……

APPENDIX 4: STAFF COMPUTER / DEVICE AGREEMENT AND CODE OF CONDUCT FOR ICT – BOTH SCHOOLS

To ensure that members of staff are fully aware of their professional responsibilities when using IT systems and when communicating with pupils, they are asked to sign this code of conduct. Members of staff should consult the School's Online Safety and ICT Acceptable Use Policy and Social Media Policy for further information and clarification: https://www.felsted.org/parents/policies-school-information.

This agreement is for the use of School IT systems, accounts, equipment/devices and any personal devices brought on to the School site and used on the School network or at a School activity.

1. I understand that it is a serious offence to use the school ICT system for a purpose not permitted by its owner.

- I appreciate that ICT includes a wide range of systems, including Google and iSAMS accounts, mobile devices, tablets, digital cameras, email, social networking and that this agreement 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 online safety/e-safety with pupils 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 online safety/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 Online Officer, the Designated Safeguarding Lead or relevant Head of Phase/ Housemaster/ Housemistress
- I will ensure that electronic communications with pupils, including email, are compatible with my professional role and comply with the School's Safeguarding (Child Protection and Staff Behaviour) Policy.

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

- I will ensure that I comply with the School's Online Safety and ICT Acceptable Use 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 and access use of the School's information systems, including accounts, devices and internet access, as per section 6.1 of the Online Safety and ICT Acceptable Use Policy.

I agree to the Terms and Conditions of the Staff Computer/ Device 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.

APPENDIX 5: EXAMPLE OF ONLINE INCIDENT LOG

Details of ALL online safety/online safety incidents to be recorded by the/DSL.

This incident log will be monitored termly by the Head, Deputy Head, Designated Safeguarding Leads or members of the Leadership Team. Any incidents involving online bullying should be recorded in the Bullying Concerns 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