Felsted

ONLINE SAFETY AND ICT ACCEPTABLE USE POLICY

INCLUDING EYFS AND BOARDING

Governors' Committee normally reviewing:	Regulatory Compliance and Governance Group
Date last formally approved:	Autumn Term 2026

Period of Review:	Annually
Next Review Date:	Autumn Term 2027

Person responsible for implementation and monitoring:	**Designated Safeguarding Lead** **Head of IT** Online Safety Officer
Other relevant policies: ● Safeguarding and Child Protection Policy ● Staff Behaviour Policy ● Policy for Gender Questioning Pupils ● Behaviour and Discipline Policy ● Anti-bullying Policy	● Social Media Policy ● RSE / PSHE Policy ● Promoting the Welfare of Pupils Policy ● Preventing Radicalisation Policy ● Equality Policy (Pupils)

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 and Child Protection 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 characteristics 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, school trips and remote working) 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.

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.

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.

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 accounts (including Gmail and other Google Apps), access to the School's database and

software systems (e.g. iSAMs, CPOMS, EdTech software etc.), PCs, chromebooks, mobile devices, microcontrollers, 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. Online Safety is overseen by the Designated Safeguarding Lead (DSL). who keeps 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 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. See the School's Safeguarding and Child Protection Policy for further information.

The School requires all users of the wireless and local network to login using their school supplied credentials, with the exception of guest wireless users who use a code to connect with the external only guest wireless system. The School has systems in place to safeguard children from potentially harmful and inappropriate material online when using the School's IT system and to monitor online activity. A reporting system is in place for the Designated Safeguarding Lead (DSL) and the Senior Leadership Team (SLT) to monitor online activity and easily identify any areas of concern.

The School recognises that notwithstanding the mobile phone ban, children may still have access to the internet via mobile phone networks (i.e. 3G, 4G and 5G), through other personal devices such as smart watches or laptops or tablets. The School's filtering and monitoring systems may not apply to content accessed via pupils' personal devices unless registered on the School's wireless network. To mitigate risk, the School requires any personal device used during the School day to connect to the internet only through the School's filtered wi-fi network. For pupils in Year 8 and below only a School Managed Device can be used in the classroom. For pupils in Year 9 upwards, compulsory school managed devices are being introduced as part of a phased scheme. Any safeguarding concerns arising from a pupil's use of a personal device must be reported to the DSL immediately.

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 are provided in Section 5.9 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 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 issues. Careful consideration is given to group interactions when raising awareness of online safety. Internet activities are carefully planned and well managed.

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. The use of any Edtech sites as a teaching and learning resource (for use by pupils and / or staff) must be approved through the software approval process so that the relevant data protection and cybersecurity checks can be carried out.

We believe it is essential for online safety guidance to be given to the pupils on a regular and meaningful basis. Online 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.

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, computer misuse, 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 speaking at parent events, information and guidance via School newsletters and working with parents on an individual basis where extra support is needed.

Screen Use in Early Years
The School has regard to Government guidance on screen use for children in the early years, including the impact of screen time on children's health, development and wellbeing. The School's approach to screen use in the EYFS setting is age-appropriate. Staff in the EYFS setting are aware of the risks associated with excessive or inappropriate screen use for young children and take steps to manage and limit children's exposure to screens in line with the guidance.

Purposeful Learning: Screen time is strictly limited and tied directly to specific educational goals. Passive viewing is banned.
Adult Guidance: Staff co-view and actively guide all screen interaction to foster language skills and engagement.
Balanced Play: Screens never replace physical exercise, social interaction, sensory activities, or outdoor play.
Filtering & Safety: All EYFS devices use age-appropriate content filters, and staff must preview and approve all digital content in advance.

5.3 Email

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

Use of the internet at Felsted through the Felsted School Network is subject to the Schools' online monitoring and filtering.

Whenever any inappropriate use is detected, it will be followed up through the School's monitoring and filtering processes.

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.
- Online 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 IT usage within the School's IT environment.

It is the responsibility of the School, by delegation to the Head of IT, to ensure that anti-virus (AV) protection is installed and kept up to date on all networked school machines. AV software is not installed on any Chromebooks in the school. ChromeOS and Google cloud security is

used for protection of the Chromebooks. 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 Use of generative AI

Any permitted usage by pupils of generative AI tools will only be permitted in circumstances subject to conditions imposed by guidelines issued by the School.

The School recognises that artificial intelligence, including generative AI, presents both significant opportunities and safeguarding risks in education. The School is committed to ensuring that the use of AI is safe, ethical, transparent and aligned with the School's safeguarding obligations.

The School will only use AI products that meet the DfE's *Generative AI: product safety expectations* and are subject to approval through the School's software approval process. Any use of generative AI by staff or pupils is carefully considered and assessed, evaluating the benefits and risks within the School's context.

The School is alert to the safeguarding risks arising from AI, including but not limited to:

- the generation of deepfake images and AI-generated intimate imagery;
- the potential for AI chatbots to produce harmful, inaccurate, or age-inappropriate content;
- the risk of 'cognitive offloading' where pupils defer their critical thinking to AI tools; and
- the use of AI to facilitate grooming, exploitation, or the creation of child sexual abuse material.

Any safeguarding or wellbeing concern arising from the use of AI tools should be reported to the DSL immediately, using the procedures set out in the Safeguarding and Child Protection Policy.

If using approved AI tools, pupils should ensure that they are using these in an academically honest way, which is consistent with the Academic Honesty policy. This includes:

- Avoiding 'cut and paste' completion of tasks using AI tools to generate answers
- Making a note of the source of information (including prompt questions) in order to provide appropriate citations and references
- Avoid using AI tools for wholesale translation of work from one language to another
- Ensuring all work that is submitted is their own work, unless properly referenced.

It is also important to be aware that the technology, despite its advances, still produces regular errors and misunderstandings and should not be relied on for accuracy. In particular, pupils should not use these tools to answer questions about health / medical / wellbeing issues, or indeed anything of a personal nature. It is always best to seek help and recommendations as to reliable resources from the Academic Office or the DSL / DDSL.

5.6 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 on 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 social media / 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.

5.7 Inappropriate Material

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

Deliberate access to inappropriate materials must be reported to the DSL and will be logged. Depending on the seriousness of the offence there will follow; investigation by the Deputy Head/Head in line with the School's Behaviour and Discipline Policy.

5.8 Viruses

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

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.

5.9 Devices

5.9.1 Devices to be used in an educational context (including in lessons and prep time)

The School is delivering a phased programme for school managed devices.

For the school year 2026/27:

- Year 5: School owned Chromebooks are provided to pupils.
- Year 6: School owned Chromebooks are provided to new pupils and for any replacement devices. All other devices are school managed.
- Years , 7 and 8: Pupils may only use a School Managed Chromebook or Laptop.
- Year 9: Pupils may use existing school managed chromebooks or for new pupils or new devices, these must be purchased or rented via the Easy4U programme. Any other devices are not permitted for use in school.
- Year 10 to Year 13: Pupils may continue to use their current device. For new pupils or new devices, these must be purchased or rented via the Easy4U programme.

Pupils are not permitted to use iPads or tablets for their schoolwork.

5.9.2 Mobile Devices

<u>Prep School</u>

With permission from the appropriate Head of Section or the HM, Year 7 and Year 8 pupils who travel on the School minibuses and other pupils with permission from the Head for a valid reason, 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 and collected at the end of the school day.

Boarders who board three nights or more are permitted to bring their mobile phones to the Boarding House. Pupils' phones are handed in for the school day and overnight, where they are stored in a locked cabinet in the Boarding House office. Pupils are permitted appropriate access to their phones during the evening as specified for each age group and for use only in the designated areas.

<u>Senior School</u>

- Mobile phones must be registered with HMs.
- Years 9 -11 only have access to their phones for short periods of time:
    - before the start of the school day at 8:15am
    - after the end of the school day at 5:45pm until the beginning of prep
    - phones must be handed in again before bedtime
- Sixth form pupils are prohibited from using a mobile phone or having a mobile phone visible around the school site during the School day (8.15am-5.45pm). y
- **Sixth Formers** are not permitted to use their mobile phones anywhere, including in houses, during lesson time, *even if they do not have a timetabled lesson*.
- During the school day but outside of lesson time, **Sixth Formers** may use their mobiles in houses *so long as not in the presence of younger pupils*.

Mobile phone misuse

- First offence: mobile phones will be confiscated for the remainder of the school day.
- Repeat offenders: as well as having their phones confiscated as above, repeat offenders can expect to serve a DHD. In extreme cases phones may be confiscated until the end of the working week and / or they may not be permitted to keep a mobile phone in school for an extended period of time (e.g. a fortnight).
- Social media offences usually attract a ban from having a phone in school (e.g. for a fortnight)

5.10 Monitoring

The School's Search Policy must be followed at all times.

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

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, the DSL must be informed and the Schools Search Policy followed.

5.11 Issues or Concerns

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

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

5.12 Termination of Access

Pupils in the Senior School Sixth Form preparing for university applications are encouraged to use an alternative email address for these communications, as Year 13 pupils will lose access to their Felsted School account (including email) 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 account (including email), 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.

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 the School's IT accounts (including email, Google accounts and iSAMS), IT 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 the Head, Deputy Head or CFO, access the email, 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.

The installation of any applications or use of software packages, including accounts with Edtech websites, must be authorised, and in some cases carried out, by the IT Department.

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 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. 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 Head of IT 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 or face 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 IT department must be notified immediately if this device is lost or stolen so that passwords to school accounts can be changed without delay.

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 Director of Operational Services (Operational staff) and the Head of Compliance (compliance@felsted.org) and Head of IT.

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 incidents involving either staff or pupils will be recorded to the DSL.

6.4.4 Inappropriate Material

All users are aware of the procedures for reporting accidental access to inappropriate materials. Any access to inappropriate materials must be reported to the DSL and logged. Depending on the seriousness of the offence, the School's disciplinary procedures will be followed.
Where the allegation(s) concern the Head, the staff member should report the matter to the Chair 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, 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.

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.

Our staff receive regular information and training on online safety issues and data protection in the form of INSET or operational staff training sessions. Data protection and cybersecurity 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 schoolwork 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 should follow the following points on email use:

- When publishing or transmitting information externally, be aware that they are representing the School and are 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 start 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 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.

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

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

Copyright
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 Use of generative AI

Staff use of generative AI tools is only permitted in the circumstances outlined in the 'Working Principles & Guidance on the use of AI at Felsted' and subject to any conditions imposed by that policy.

In particular, personal or confidential information should not be entered into generative AI tools apart from Google Gemini or Microsoft Co-Pilot via a school account. This technology can potentially store and/or learn from data inputted and staff should consider that any information entered into such tools is released to the internet.

It is also important to be aware that the technology, despite its advances, still produces regular errors and misunderstandings and should not be relied on for accuracy.

6.10 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.

6.11 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.

6.12 Remote Access

Due to the majority of the School's systems sitting in cloud-based environments, remote access to the school network is not commonly required. However, in exceptional circumstances, remote access to the network can be granted via a VPN connection after consultation with and approval by 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.

6.13 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.

6.14 Mobile and personal devices

Staff must be aware of the 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.

6.15 Termination of Access

Upon leaving the employment of Felsted School, members of staff shall have their School IT account (including Google Workspace. Windows domain and iSAMS) 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. Staff with role-based school accounts must delete any personal content from their account on the understanding that the account will subsequently be made available to their successor.

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

Online Safety Act 2023
Online Safety Act 2023 and reference the DfE's statutory *Filtering and Monitoring standards* (as referenced in *Keeping Children Safe in Education*) to ensure the policy reflects the current statutory context

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 Safeguarding and Child Protection 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, School IT accounts and software platforms provided via the School, accessed at any time (including during online learning) and equipment/devices and any personal devices (including hand held devices, watches or any other smart technology or 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 IT 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.

- Follow the mobile phone policy for pupils at all times to support the School being a mobile phone free environment during the school day and the appropriate use of mobile phones outside of the school day.

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 platforms 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.

Artificial Intelligence (AI) tools

Any use by pupils of generative AI tools is only permitted subject to conditions imposed by the guidelines issued by the School.

Mobile Phones
The mobile phone policy for pupils must be followed at all times to ensure the School is a mobile phone free environment during the school day (08:15-17:45), and the appropriate use of mobile phones outside of the school day.

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 Section 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 Section 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, or a member of the IT team.

Appropriate action will also be taken in line with the School's Behaviour and Discipline Policy, Anti-bullying Policy and the Safeguarding and Child Protection 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 – Years 9-13

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 smart technology or 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.

- Follow the school's mobile phone policy, to ensure the school is a mobile phone free environment during the school day (08:15-17:45) and the appropriate use of mobile phones outside of the school day.

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.

Artificial Intelligence (AI) tools
Any permitted usage by pupils of generative AI tools is only permitted subject to any conditions imposed by guidelines issued by the School and the School's Academic Honesty Policy.

Mobile Phones
The mobile phone policy for pupils must be followed at all times to ensure the School is a mobile phone free environment during the school day (08:15-17:45), and appropriate use of mobile phones outside of the school day.

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 IT 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 IT, 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 IT 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, Anti-Bullying Policy and the Safeguarding and Child Protection 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 CODE OF CONDUCT FOR IT

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 IT system for a purpose not permitted by its owner.***

    - I appreciate that IT 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 IT devices when used for school business
    - I understand that school IT systems, including my school email account, may not be used for private purposes other than what is permitted within section 6.7 (Email) and section 6.10 (Personal Use) of the School's Online Safety and ICT Acceptable Use Policy
    - 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 attempt to bypass security or monitoring systems.
    - 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 PLT/SLT and encryption approved by the IT 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.
    - I will ensure I comply with staff guidance regarding the use of AI and generative AI including the responsibility of teachers to check AI generated content for accuracy and appropriateness, and to limit the use of AI to agreed work processes.

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 Section/ 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 and Child Protection Policy and the Staff Behaviour Policy.

- I will ensure that I attend/complete all required training provided by the School, including e-safety training and use of the School's IT systems.

3. I understand that my use of school information systems, accounts, internet access and email may be monitored, reviewed and recorded to ensure policy and regulatory compliance, including for safeguarding and data protection purposes. The School may exercise its right to monitor and access use of the School's IT systems as per section 6.1 of the Online Safety and ICT Acceptable Use Policy.

- 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, Safeguarding and Child Protection Policy and the Staff Behaviour Policy.

4. ***I understand that I must comply with the School's Staff Behaviour Policy regarding the use of personal mobile phones.***

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

Signed: …… Print Name: …… Date: ……

Appendix 5 – BRING YOUR OWN DEVICE

1. Purpose

The purpose of this Bring Your Own Device (BYOD) policy is to enhance the educational experience for pupils by allowing them to use their personal devices for academic purposes and in a boarding environment. At the same time, the policy ensures that technology use is appropriate, secure, and does not interfere with the well-being or academic performance of pupils.

2. Scope

This policy applies to all pupils enrolled at the School, including both day and boarding pupils. It governs the use of personal devices on school premises, in classrooms, during study periods, in boarding areas and in social spaces. The policy applies during the hours a pupil is at school, including residential hours when pupils are in their boarding houses or on school-provided networks.

3. Approved Devices

- **Devices to be used in an educational context:**
    - All pupils are required to follow the guidelines within section 5.9.1 of the Online Safety and ICT Acceptable Use Policy for acceptable devices in an educational context.

- **Permitted Devices in the boarding environment**:
    - Laptops, Chromebooks, tablets (iPads, Android tablets), smartphones and smartwatches.
    - Any personal devices must meet the technical requirements set by the school's IT department (e.g., minimum operating system version, required apps).
    - Gaming consoles, unless specifically approved, are not allowed.

4. Acceptable Use

- **Educational Use**: Devices should be used primarily for academic purposes such as research, homework, online learning, and collaboration with peers and teachers.
- **Personal use:**
  Pupils must follow the School's Online Safety and ICT Acceptable Use Policy (section 5.8.2) for use of and access to personal mobile devices.

5. Network Access and Security

- **Wi-Fi Network**: pupils may connect their devices to the school's designated network, which has designated security categories for pupils, staff and administrative networks.
- **Authentication**: Access requires using school-issued credentials (username/password) to log into the network.
- **Content Filtering**: The school's content filtering system applies to all devices connected to the network, ensuring that inappropriate content is blocked.
- **Device Security**:
    - Devices must have up-to-date antivirus software and security patches.
    - Pupils are responsible for ensuring their device has a password or biometric security to prevent unauthorized access.

7. Privacy and Monitoring

- The School reserves the right to monitor network activity and inspect devices if there is suspicion of policy violation (e.g., cyberbullying, accessing inappropriate content, or illegal activity), as per the School's Online safety and ICT Acceptable Use Policy, usage agreements with pupils and staff and the School's Search Policy.
- Pupils are advised to keep sensitive or personal information secure and refrain from storing unnecessary personal data on school networks.

8. Responsibilities

For Pupils:

- Ensure that devices are charged and ready for use during school hours.
- Use devices responsibly and respectfully, adhering to the school's usage agreement.
- Report any damage, loss, or theft of devices immediately to boarding or IT staff.
- Keep devices in good working order, ensuring that they are updated with the latest software, including security patches.

For Parents/Guardians:

- Provide pupils with devices that meet the technical requirements specified by the school.
- Ensure devices are covered under personal insurance against damage or loss.
- Discuss with pupils the importance of responsible device usage, online etiquette, digital safety and complying with the usage agreement.

For School Staff:

- Monitor pupils' use of devices in classrooms and common areas to ensure compliance with the policy, while ensuring the School's search procedures are always followed.
- Address any violations of the policy in accordance with the school's behaviour procedures.
- Provide guidance to pupils on how to use their devices for educational purposes.

9. Liability

- **Loss or Damage**: The school is not responsible for the loss, theft, or damage of personal devices. Pupils and their parents are solely responsible for maintaining and insuring their devices.
- **Use of Devices**: Pupils are expected to take appropriate care to ensure their devices are not lost or damaged.

10. Disciplinary Action

- Violations of the BYOD policy by pupils will be dealt with through the School's Behaviour and Discipline Policy.

11. Agreement and Consent

Pupils and staff must review and sign the IT Usage Agreement Forms which acknowledge understanding and compliance with the Online Safety and ICT Acceptable Use Policy.