ICT and Internet Acceptable Use policy

The Federation of Abbey Infant and Abbey Junior Schools

Approved by:	Governing Body	**Date:** 2022
Last reviewed on:	Jan 2022	
Next review due by:	XXXX	

Contents

1. Introduction and aims

Information and communications technology (ICT) is an integral part of the way our school works, and is a critical resource for pupils, staff (including senior leadership teams), governors, volunteers and visitors. It supports teaching and learning, pastoral and administrative functions at our school.

Why do we need an AUP?

All staff (including support staff), governors, volunteers, contractors and visitors have particular legal / professional obligations and it is imperative that all parties understand that online safety is part of safeguarding as well as part of the curriculum, and it is everybody's responsibility to uphold the school's approaches, strategy and policy as detailed in the Child Protection Policy and Safeguarding Across the Curriculum Policy, both found here: Safeguarding | The Federation of Abbey Infant and Abbey Junior Schools (abbeyfederation.co.uk)

The ICT resources and facilities our school uses pose risks to data protection, online safety and safeguarding, therefore this **policy aims to:**

- Set guidelines and rules on the use of school ICT resources for staff (including supply), pupils, parents, governors, contractors and visitors
- Establish clear expectations for the way all members of the school community engage with each other online
- Support the school's policy on data protection, online safety and safeguarding
- Prevent disruption to the school through the misuse, or attempted misuse, of ICT systems
- Support the school in teaching pupils safe and effective internet and ICT use

This policy covers all users of our school's ICT facilities, including governors, staff, pupils, volunteers, contractors and visitors. Breaches of this policy may be dealt with under our Behaviour Policy, Disciplinary Policy, Staff Code of Conduct, Low Level Concerns Policy or Child Protection Policy. All policies may be accessed here: Policies | The Federation of Abbey Infant and Abbey Junior Schools (abbeyfederation.co.uk)

2. Relevant legislation and guidance

This policy refers to, and complies with, the following legislation and guidance:

- Data Protection Act 2018
- The General Data Protection Regulation
- Computer Misuse Act 1990
- Human Rights Act 1998
- The Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000
- Education Act 2011
- Freedom of Information Act 2000
- The Education and Inspections Act 2006
- Keeping Children Safe in Education 2021
- Searching, screening and confiscation: advice for schools
- National Cyber Security Centre (NCSC)
- Education and Training (Welfare of Children Act) 2021

3. Definitions

- **“ICT facilities”:** includes all facilities, systems and services including but not limited to network infrastructure, desktop computers, laptops, tablets, phones, music players or hardware, software, cameras, video recorders, web-cams, websites, web applications or services, and any device system or service which may become available the future which is provided as part of the ICT service
- **“Users”:** anyone authorised by the school to use the ICT facilities, including governors, staff, pupils, volunteers, contractors and visitors
- **“Personal use”:** any use or activity not directly related to the users’ employment, study or purpose
- **“Authorised personnel”:** employees authorised by the school to perform systems administration and/or monitoring of the ICT facilities
- **“Materials”:** files and data created using the ICT facilities including but not limited to documents, photos, audio, video, video recordings, printed output, web pages, social networking sites and blogs

See appendix 6 for a glossary of cyber security terminology.

4. Unacceptable use

The following is considered **unacceptable use** of the school’s ICT facilities, personal computers or mobile phone use by any member of the school community. Any breach of this policy may result in disciplinary or behaviour proceedings (see section 4.2 below). Unacceptable use of the school’s ICT facilities includes:

- Using the school’s ICT facilities to breach intellectual property rights or copyright
- Using the school’s ICT facilities to bully, shame, embarrass, harass or intimidate someone else, or to promote unlawful discrimination
- Breaching the school’s policies or procedures
- Any illegal conduct, or statements which are deemed to be advocating illegal activity
- Online gambling, inappropriate advertising, phishing and/or financial scams
- Accessing, creating, storing, linking to or sending material that is pornographic, offensive, obscene or otherwise inappropriate or harmful
- Consensual and non-consensual sharing of nude and semi-nude images and/or videos and/or livestreams (also known as sexting or youth-produced sexual imagery)
- Activity which defames or disparages the school, or risks bringing the school into disrepute
- Sharing confidential information about the school, its pupils, or other members of the school community
- Connecting any device to the school’s ICT network without approval from authorised personnel
- Setting up any software, applications or web services on the school’s network without approval by authorised personnel, or creating or using any program, tool or item of software designed to interfere with the functioning of the ICT facilities, accounts or data
- Gaining, or attempting to gain, access to restricted areas of the network, or to any password-protected information, without approval from authorised personnel
- Allowing, encouraging or enabling others to gain (or attempt to gain) unauthorised access to the school’s ICT facilities
- Causing intentional damage to ICT facilities
- Removing, deleting or disposing of ICT equipment, systems, programs or information without permission by authorised personnel
- Causing a data breach by accessing, modifying, or sharing data (including personal data) to which a user is not supposed to have access, or without authorisation

- Using inappropriate or offensive language
- Promoting a private business, unless that business is directly related to the school
- Using websites or mechanisms to bypass the school's filtering mechanisms
- Engaging in content or conduct that is radicalised, extremist, racist, anti-Semitic or discriminatory in any other way

This is not an exhaustive list. The Federation of Abbey Infant and Abbey Junior School and Governing Body reserves the right to amend this list at any time. The senior leadership team will use professional judgement to determine whether any act or behaviour not on the list above is considered unacceptable use of the school's ICT facilities.

4.1 Exceptions from unacceptable use

Where the use of school ICT facilities (on the school premises and/or remotely) is required for a purpose that would otherwise be considered an unacceptable use, exemptions to the policy may be granted at the head teacher's discretion and approved by the governing body.

4.2 Sanctions

Pupils and staff who engage in any of the unacceptable activity listed above may face disciplinary action in line with the school's policies on behaviour, our disciplinary policy and the staff code of conduct:

https://primarysite-prod-sorted.s3.amazonaws.com/abbey-federation/UploadedDocument/ac5173ea-8127-4a8e-aa64-1c51c1ab8b29/14.10-behaviour-policy-nov-2021.pdf

https://primarysite-prod-sorted.s3.amazonaws.com/abbey-federation/UploadedDocument/aad07ee7e53f4fee8b9e2d9d8ae325ea/5-disciplinary-policy.doc

https://primarysite-prod-sorted.s3.amazonaws.com/abbey-federation/UploadedDocument/15d33976ad8b4768b4f7b7e67226a98b/code-of-conduct-for-staff-v1.3.docx

5. Staff (including supply, governors, volunteers, visitors and contractors)

5.1 Access to school ICT facilities and materials

The school's head teacher and network manager manages access to the school's ICT facilities and materials for school staff. That includes, but is not limited to:

- Computers, tablets, mobile phones and other devices
- Access permissions for certain programmes or files

Staff will be provided with unique log-in/account information and passwords that they must use when accessing the school's ICT facilities.

Staff who have access to files they are not authorised to view or edit, or who need their access permissions updated or changed, should contact the head teacher Dr R Kentish personally and discuss this with him your request. Once permission is granted, contact: Inny Choudhury on Inny.Choudhury@abbey-jun.sandwell.sch.uk

5.2 Use of Email and Phones

Email

The school provides each member of staff with an email address.

This email account should be used for work purposes only.

All work-related business should be conducted using the email address the school has provided and NOT a personal email address.

Staff must not share their personal email addresses with parents and pupils, and must not send any work-related materials using their personal email account.

Staff must take care with the content of all email messages, as incorrect or improper statements can give rise to claims for discrimination, harassment, defamation, breach of confidentiality or breach of contract.

Email messages are required to be disclosed in legal proceedings or in response to requests from individuals under the Data Protection Act 2018 in the same way as paper documents. Deletion from a user's inbox does not mean that an email cannot be recovered for the purposes of disclosure. All email messages should be treated as potentially retrievable.

Staff must take extra care when sending sensitive or confidential information by email. Any attachments containing sensitive or confidential information should be encrypted so that the information is only accessible by the intended recipient.

If staff receive an email in error, the sender should be informed and the email deleted. If the email contains sensitive or confidential information, the user must not make use of that information or disclose that information.

If staff send an email in error that contains the personal information of another person, they must inform the head teacher and the network manager immediately and follow our data breach procedure.

Phones – staff must abide to the same rules for ICT acceptable use as set out in Section 4

Staff must ensure that their personal mobile phone is switched off and left in a secure place (lockers), during contracted hours. This includes school trips, school events and clubs. The school will not take responsibility for items that are lost damaged or stolen.

Staff may use personal mobile phones during break times. This needs to be discreet, appropriate and not in the presence of pupils.

With permission form the head teacher some staff may be permitted to carry mobile phones. The same guidance applies to the use of these phones in school.

Staff who are provided with mobile phones as equipment for their role must abide by the same rules for ICT acceptable use as set out in section 4.

Staff must not give their personal phone numbers to parents or pupils. Staff must use phones provided by the school to conduct all work-related business. If a personal mobile is used, with permission from the head teacher then a member of staff must operate NO-CALLER ID when making calls.

Staff may take notes during a telephone conversation, to record the precise details of the conversation. Other members of staff may be present to take notes. The use of speaker-phone may be in use. This has been approved by the head teacher. This would happen in the following incidents:

- Discussing a complaint raised by a parent/carer or member of the public
- Calling parents to discuss behaviour or sanctions
- Taking advice from relevant professionals regarding safeguarding, special educational needs (SEN) assessments, etc.
- Discussing requests for term-time holidays

5.3 Personal Use

Staff are permitted to occasionally use school ICT facilities for personal use subject to certain conditions set out below. Personal use of ICT facilities must not be overused or abused. The network manager or head teacher may withdraw permission for it at any time or restrict access at their discretion.

Personal use is permitted provided that such use:

- Does not take place during contact/teaching time or non-break time

- Does not constitute ‘unacceptable use’, as defined in section 4
- Takes place when no pupils are present
- Does not interfere with your jobs, or prevent other staff or pupils from using the facilities for work or educational purposes

Staff may use the school’s mobile ICT facilities (laptops, iPads and phones) to store personal non-work-related information or materials (such as music, videos or photos), but this must be deleted when the device is returned.

Staff should be aware that use of the school’s ICT facilities for personal use may put personal communications within the scope of the school’s ICT monitoring activities. Where breaches of this policy are found, disciplinary action may be taken.

Staff are also permitted to use their personal devices (such as mobile phones or tablets) in line with this policy (see 5.2 Phones).

Staff should be aware that personal use of ICT (even when not using school ICT facilities) can impact on their employment by, for instance, putting personal details in the public domain, where pupils and parents could see them. Please also refer to the Staff Code of Conduct.

5.4 Personal social media accounts

Members of staff should ensure their use of social media, either for work or personal purposes, is appropriate at all times.

Staff should take care to follow the school’s guidelines on social media (see appendix 1) and use of email (see section 5.2 Email) to protect themselves online and avoid compromising their professional integrity.

The school has guidelines for staff on appropriate security settings for public, online accounts - Facebook etc. **Staff must read and adhere to this guidance** (see appendix 1).

5.5 Remote access

The head teacher and the school’s business manager has access the school’s ICT facilities and materials remotely.

- This is managed by the network manager and the head teacher
- Security arrangements are in place (see personal login details)
- Protocols for remote access are agreed with the headteacher

Staff accessing the school’s ICT facilities and materials remotely must abide by the same rules as those accessing the facilities and materials on-site. Staff must be particularly vigilant if they use the school’s ICT facilities outside the school and take such precautions as advised by the head teacher or network manager when setting up this access. Staff need to be vigilant against importing viruses or compromising system security.

Our ICT facilities contain information which is confidential and/or subject to data protection legislation. Such information must be treated with extreme care and in accordance with our data protection policy.

Our data protection policy may be found here: https://www.abbeyfederation.co.uk/gdpr-general-data-protection-regulation/

5.6 School social media accounts

The school does not have an official social media page [Facebook/Twitter/etc.] or public group chat pages such as WhatsApp.

The school has guidelines (Appendix 2) on group social media accounts used by parents. This also applies to group chat pages such as WhatsApp etc. Those who are authorised to manage the account must ensure they abide by these guidelines at all times.

5.7 Monitoring of school network and use of ICT facilities

The school reserves the right to monitor the use of its ICT facilities and network. This includes, but is not limited to, monitoring of:

- Internet sites visited
- Bandwidth usage
- Email accounts
- Telephone calls
- User activity/access logs
- Any other electronic communications
- See CCTV policy

Only authorised ICT staff may inspect, monitor, intercept, assess, record and disclose the above, to the extent permitted by law.

The school monitors ICT use in order to:

- Obtain information related to school business
- Investigate compliance with school policies, procedures and standards
- Ensure effective school and ICT operation
- Conduct training or quality control exercises
- Prevent or detect crime
- Comply with a subject access request, Freedom of Information Act request, or any other legal obligation

5.8 Remote Learning

Keeping Children Safe (Updated August 2021)
From September 2021, the duty to provide remote education remains for pupils who cannot attend school in order to comply with government Covid guidelines, so **safe remote learning remains a priority for 2021/22**.

Abbey is committed to providing safe remote learning and will ensure that staff who deliver remote learning and for the children who use online technology to access it, will do so in a safe way.

Staff guidance during remote learning:

Staff will not behave any differently towards students compared with being in school. Staff never attempt to arrange any meeting, including tutoring session, without the full prior knowledge and approval of the school, and will never do so directly with a pupil. The same applies to any private/direct communication with a pupil.

Staff will not attempt to use a personal system or personal login for remote teaching or set up any system on behalf of the school without SLT approval.

Staff will not take secret recordings or screenshots of myself or pupils during live lessons.

Staff will conduct any video lessons in a professional environment as in school. Staff will be correctly dressed and not in a bedroom (where this is unavoidable then there should be an appropriate filter in place to disguise the setting). The camera view will not include any personal information or inappropriate objects and where possible to blur or change the background.

Staff will complete the issue log for live lessons if anything inappropriate happens or anything which could be construed in this way. This is protection for staff and pupils.

Staff understand that in past and potential future remote learning and lockdowns, there is a greater risk for grooming and exploitation as children spend more time at home and on devices; staff must play a role in supporting educational and safeguarding messages to help with this.

Staff understand the responsibilities listed for my role in promoting Online Safety, as set out in the Child Protection policy. This includes promoting online safety as part of a whole school approach in line with the RSHE curriculum, as well as safeguarding considerations when supporting pupils remotely.

Staff understand that school systems and users are protected by security, monitoring and filtering services, and that the use of school devices, systems and logins of personal devices and at home (regardless of time, location or connection), including encrypted content, can be monitored/captured/viewed by the relevant authorised staff members.

Staff understand that they are a role model and will promote positive online safety and model safe, responsible and positive behaviours. They will adhere to the AUP by

not sharing other's images or details without permission

refraining from posting negative, threatening or violent comments about others, regardless of whether they are members of the school community or not.

Staff will not contact or attempt to contact any pupil or to access their contact details (including their usernames/handles on different platforms) in any way other than school-approved and school-monitored ways. Staff will report any breach of this by others or attempts by pupils to do the same to the head teacher.

Details on social media behaviour, the general capture of digital images/video and on my use of personal devices is stated in the AUP. If staff are unsure then they will seek guidance from the DSL.

Staff understand the importance of upholding their online reputation, professional reputation and that of the school), and will do nothing to impair either.

Staff agree to adhere to all provisions of the school Data Protection Policy/GDPR https://www.abbeyfederation.co.uk/gdpr-general-data-protection-regulation/ at all times, whether or not they are on site or using a school device, platform or network, and will ensure that they do not access, attempt to access, store or share any data which they do not have express permission for.

Staff will protect their passwords/logins and other access, never share credentials and immediately change passwords and notify the network manager/head teacher if they suspect a breach. Staff will only use complex passwords and not use the same password as for other systems.

Staff will not store school-related data on personal devices, storage or cloud platforms. USB keys, if allowed, will be encrypted, and staff will only use safe and appropriately licensed software, respecting licensing, intellectual property and copyright rules at all times.

Staff will never use school devices and networks/internet/platforms/other technologies to access material that is illegal or in any way inappropriate for an education setting. They will not attempt to bypass security or monitoring and will look after devices loaned to them.

Staff will not support or promote extremist organisations, messages or individuals, nor give them a voice or opportunity to visit the school. Staff will not browse, download or send material that is considered offensive or of an extremist nature.

Staff understand and support the commitments made by pupils/students, parents and fellow staff, governors and volunteers in their Acceptable Use Policies and will report any infringements in line with school procedures.

Staff will follow the guidance in the safeguarding and online-safety policies for reporting incidents: Staff understand the principle of 'safeguarding as a jigsaw' where their concern might complete the picture. Staff understand safeguarding issues as stated in KCSIE 2021 and the school's Child Protection Policy on handing incidents and concerns about a child in general, sharing nudes and semi-nudes, upskirting, bullying, sexual violence and harassment, misuse of technology and social media.

Staff understand that breach of this AUP and/or of the school's other safeguarding policies may lead to appropriate staff disciplinary action or termination of their relationship with the school and where appropriate, referral to the relevant authorities.

6. Pupils

Through Computing lessons, assemblies and PSHE, children will be taught the **SMART** rules:

SAFE	Keep safe by being careful not to give out personal information online.
MEETING	Never agree to meet anyone that you chat to on the internet; they may not be who you think they are. You can't be sure who you're talking to on the Internet.
ACCEPTING	Do not accept unusual e-mails. They may be trying to tempt you into opening them. They could contain viruses that can damage your computer. If this happens to you, tell an adult.
RELIABLE	Information on the internet may not be true – anyone can upload material to the internet. Always double check any information on a more reliable website.
TELL	If anything makes you feel worried tell your parents, teachers or an adult that you trust. They can help you to report it to the right place or call a helpline like ChildLine on 0800 1111 in confidence.

6.1 Access to ICT facilities

The following facilities are available to pupils, with the following terms and conditions:

- During remote learning, private class-based platforms will be used by pupils and supervised by staff
- "Computers and equipment in the school's ICT suite are available to pupils only under the supervision of staff"
- "Specialist ICT equipment, such as that used for music, or design and technology, must only be used under the supervision of staff"
- Where pupils are given laptops to use at home, there will be clear guidance and instruction shared with parents on their acceptable use. A contract is signed by parents for these devices.

6.2 Search and deletion

Under the Education Act 2011, and in line with the Department for Education's guidance on searching, screening and confiscation, the school has the right to search pupils' phones, computers or other devices for pornographic images or any other data or items banned under school rules or legislation.

The school can, and will, delete files and data found on searched devices if we believe the data or file has been, or could be, used to disrupt teaching or break the school's rules.

Staff members may also confiscate devices for evidence to hand to the police, if a pupil discloses that they are being abused and that this abuse contains an online element.

6.3 Unacceptable use of ICT and the internet outside of school

The school will sanction pupils, in line with the Behaviour Policy, if a pupil engages in any of the following **at any time** (even if they are not on school premises):

- Using ICT or the internet to bully or harass someone else, or to promote unlawful discrimination
- Breaching the school's policies or procedures
- Any illegal conduct, or statements which are deemed to be advocating illegal activity

- Accessing, creating, storing, linking to or sending material that is pornographic, offensive, obscene or otherwise inappropriate
- Consensual and non-consensual sharing of nude and semi-nude images and/or videos and/or livestreams (also known as sexting or youth produced sexual imagery)
- Activity which defames or disparages the school, or risks bringing the school into disrepute
- Sharing confidential information about the school, other pupils, or other members of the school community
- Gaining or attempting to gain access to restricted areas of the network, or to any password protected information, without approval from authorised personnel
- Allowing, encouraging, or enabling others to gain (or attempt to gain) unauthorised access to the school's ICT facilities
- Causing intentional damage to ICT facilities or materials
- Causing a data breach by accessing, modifying, or sharing data (including personal data) to which a user is not supposed to have access, or without authorisation
- Using inappropriate or offensive language

Pupils are directed to section 4.2 on AUP and must read Appendix 3

6.4 Access to personal ICT facilities and personal Mobile Phone Use

The school will work with parents and carers to organise the **safe use** of personal ICT which includes mobile telephones for our pupils.

Any parent wishing for their child to bring a mobile telephone to school must follow the guidelines of the AUP and sign an agreement, before a pupil is permitted to bring a mobile phone to school.

Permission must be provided by the parent using Appendix 7 and returned to the school – a copy of this agreement will be kept on record.

The mobile telephone must be switched off as the child enters the school property boundaries. The telephone will remain in the child's bag at all times during the school day and during after school events, clubs, trips and discos.

The school will not accept any responsibility for mobile telephones that are lost, stolen or damaged.

Where a pupil is found by a member of staff to be using a mobile telephone or any other personal ICT device, the item will be confiscated from the pupil and handed to a member of the school office team. The name of the pupil and details of the device will be taken. The device will then be stored in the school office in a locked and secure location.

The parent or carer of the child will be notified and asked to collect the device from the office at their earliest convenience. If the child requires their telephone for their unsupervised journey home and the parent and carer is not able to visit the office before this time, then a verbal arrangement will be made over the telephone and the child will be asked to collect their telephone at the end of the school day. If the practice continues more than three times and this has been documented, then the school will confiscate the phone until a parent or carer collects the phone from a senior teacher, where the matter will be discussed in full. An appropriate arrangement will be made with the parent, carer, child and senior teacher at this point.

If a pupil is found to making any recordings on their device, then this will be regarded as a serious offence and action will be taken in accordance with the school's Behaviour Policy. Recordings must be removed by the pupil in the presence of a senior teacher.

Should a pupil be found to be using their mobile telephone inappropriately, the school reserves the right to withdraw this privilege and they will no longer be able to bring a telephone into school. A meeting with a senior teacher will be arranged with parents or carers where the matter will be discussed in full.

Parents and carers are encouraged to talk to their child about the appropriate use of the internet, text messages, emails, photographs and multi- media recordings as they can put children at serious risk and used to bully pupils. Parents and carers should be aware of the websites that their children are accessing and

investigate the site rules and regulations; including age restrictions. Further advice for parents and carers on how to keep their child safe online, and on social networking websites can be obtained from visiting the school website and we recommend the NSPCC website www.nspcc.org.uk/onlinesafety

7. Parents

7.1 Access to ICT facilities and materials

Parents do not have access to the school's ICT facilities as a matter of course.

However, parents working for, or with the school in an official capacity (for instance, as a volunteer or as a member of the Friends of Abbey) may be granted an appropriate level of access, or be permitted to use the school's facilities at the headteacher's discretion.

Where parents are granted access in this way, they must abide by this policy as it applies to staff.

7.2 Communicating with or about the school online

We believe it is important to model for pupils, and help them learn, how to communicate respectfully with, and about, others online.

Parents play a vital role in helping model this behaviour for their children, especially when communicating with the school through our website and social media channels.

We ask parents to adopt our Home School Agreement and follow the AUP guidance in appendix 2.

8. Data security

The school is responsible for making sure it has the appropriate level of security protection and procedures in place. It therefore takes steps to protect the security of its computing resources, data and user accounts. However, the school cannot guarantee security. Staff, pupils, parents and others who use the school's ICT facilities should use safe computing practices at all times.

8.1 Passwords

All users of the school's ICT facilities should set strong passwords for their accounts and keep these passwords secure.

Users are responsible for the security of their passwords and accounts, and for setting permissions for accounts and files they control.

Members of staff or pupils who disclose account or password information may face disciplinary action. Parents or volunteers who disclose account or password information may have their access rights revoked.

All staff will store their passwords securely. Teachers will use passwords generated for pupils and keep these in a secure location in case pupils lose or forget their passwords.

8.2 Software updates, firewalls and anti-virus software

All of the school's ICT devices that support software updates, security updates and anti-virus products will be configured to perform such updates regularly or automatically.

Users must not circumvent or make any attempt to circumvent the administrative, physical and technical safeguards we implement and maintain to protect personal data and the school's ICT facilities.

Any personal devices using the school's network must all be configured in this way.

8.3 Data protection

All personal data must be processed and stored in line with data protection regulations and the school's data protection policy.

A link to our school's data protection policy can be found here https://www.abbeyfederation.co.uk/gdpr-general-data-protection-regulation/.

8.4 Access to facilities and materials

All users of the school's ICT facilities will have clearly defined access rights to school systems, files and devices.

These access rights are managed by network manager and the head teacher.

Users should not access, or attempt to access, systems, files or devices to which they have not been granted access. If access is provided in error, or if something a user should not have access to is shared with them, they should alert Inny Choudhury or Dr Kentish immediately.

Users should always log out of systems and lock their equipment when they are not in use to avoid any unauthorised access. Equipment and systems should always be logged out of and closed down completely at the end of each working day.

8.5 Encryption

The school ensures that its devices and systems have an appropriate level of encryption.

School staff may only use personal devices (including computers and USB drives) to access school data, work remotely, or take personal data (such as pupil information) out of school if they have been specifically authorised to do so by the headteacher.

Use of such personal devices will only be authorised if the devices have appropriate levels of security and encryption, as defined by the network manager.

9. Protection from cyber attacks

Please see the glossary (appendix 6) to help you understand cyber security terminology.

The school will:

- Work with governors and the IT department to make sure cyber security is given the time and resources it needs to make the school secure
- Provide annual training for staff (and include this training in any induction for new starters, if they join outside of the school's annual training window) on the basics of cyber security, including how to:
    - Check the sender address in an email
    - Respond to a request for bank details, personal information or login details
    - Verify requests for payments or changes to information
- Make sure staff are aware of its procedures for reporting and responding to cyber security incidents
- Investigate whether our IT software needs updating or replacing to be more secure
- Not engage in ransom requests from ransomware attacks, as this would not guarantee recovery of data
- Put controls in place that are:
    - **'Proportionate'**: the school will verify this using a third-party audit, to objectively test that what it has in place is up to scratch (360 online audit)
    - **Multi-layered**: everyone will be clear on what to look out for to keep our systems safe
    - **Up-to-date:** with a system in place to monitor when the school needs to update its software
    - **Regularly reviewed and tested**: to make sure the systems are as up to scratch and secure as they can be

- Back up critical data each day and store these backups on a cloud based backup systems/external hard drives that aren't connected to the school network and which can be stored off the school premises.
- Delegate specific responsibility for maintaining the security of our management information system (MIS) to [our cloud-based provider/our IT department] – Mr I Choudhury.
- Make sure staff:
    - Dial into our network using a virtual private network (VPN) when working from home
    - Enable multi-factor authentication where they can, on things like school email accounts
    - Store passwords securely using a password manager
- Make sure ICT staff conduct regular access reviews to make sure each user in the school has the right level of permissions and admin rights
- Have a firewall in place that is switched on
- Check that its supply chain is secure, for example by asking suppliers about how secure their business practices are and seeing if they have the Cyber Essentials certification
- Develop, review and test an incident response plan with the IT department, for example, including how the school will communicate with everyone if communications go down.

10. Internet access

The school wireless internet connection is secured.

Add further details about your school's wifi arrangements. For instance:

- All internet access is filtered through a Sophos Web Based filter. This allows the IT network manager to set different levels of access, lock and unblock sites and additionally keep check on which services users are actively searching for. This means that the searches of a dubious or worrisome nature (eg. Extremism, sexualised searches) can be checked and analysed for patterns and importantly tracked back to users.

10.1 Pupils

No pupil has unfiltered access. No pupil is allowed 'bring your own device' (BYOD)

10.2 Parents and visitors

Parents and visitors to the school will not be permitted to use the school's wifi unless specific authorisation is granted by the headteacher.

The headteacher will only grant authorisation if:

- Parents are working with the school in an official capacity (e.g. as a volunteer or as a member of the Friends of Abbey)
- Visitors may need to access the school's wifi in order to fulfil the purpose of their visit (for instance, to access materials stored on personal devices as part of a presentation or lesson plan)

Staff must not give the wifi password to anyone who is not authorised to have it. Doing so could result in disciplinary action.

11. Monitoring and review

The head teacher, Deputy and DSL monitor the implementation of this policy, including ensuring it is updated to reflect the needs and circumstances of the school.

This policy will be reviewed every three years.

The governing board is responsible for approving this policy.

12. Related policies

This policy should be read alongside the school's guidance and policies on:

- Safeguarding and Child Protection Policy (including online safety)
- Safeguarding across the curriculum
- Behaviour Policy
- Staff Code of Conduct
- Disciplinary Policy
- Data protection/GDPR
- Home School Agreement

Appendix 1: Facebook guidance sheet for staff

Don't accept friend requests from pupils on social media

10 rules for school staff on Facebook and Social Media Platforms

1. Change your display name – use your first and middle name, use a maiden name, or put your surname backwards instead
2. Change your profile picture to something unidentifiable, or if not, ensure that the image is professional
3. Check your privacy settings regularly
4. Be careful about tagging other staff members in images or posts
5. Don't share anything publicly that you wouldn't be just as happy showing your pupils
6. Don't use social media sites during school hours
7. Don't make comments about your job, your colleagues, our school or your pupils online – once it's out there, it's out there
8. Don't associate yourself with the school on your profile (e.g. by setting it as your workplace, or by 'checking in' at a school event)
9. Don't link your work email address to your social media accounts. Anyone who has this address (or your personal email address/mobile number) is able to find you using this information
10. Consider uninstalling the Facebook app from your phone. The app recognises wifi connections and makes friend suggestions based on who else uses the same wifi connection (such as parents or pupils)

Check your privacy settings

- Change the visibility of your posts and photos to **'Friends only'**, rather than 'Friends of friends'. Otherwise, pupils and their families may still be able to read your posts, see things you've shared and look at your pictures if they're friends with anybody on your contacts list
- Don't forget to check your **old posts and photos** – go to bit.ly/2MdQXMN to find out how to limit the visibility of previous posts
- The public may still be able to see posts you've **'liked'**, even if your profile settings are private, because this depends on the privacy settings of the original poster
- **Google your name** to see what information about you is visible to the public
- Prevent search engines from indexing your profile so that people can't **search for you by name** – go to bit.ly/2zMdVht to find out how to do this
- Remember that **some information is always public**; your display name, profile picture, cover photo, user ID (in the URL for your profile), country, age range and gender

What to do if…

A pupil adds you on social media

- In the first instance, ignore and delete the request. Block the pupil from viewing your profile

- Check your privacy settings again, and consider changing your display name or profile picture
- If the pupil asks you about the friend request in person, tell them that you're not allowed to accept friend requests from pupils and that if they persist, you'll have to notify senior leadership and/or their parents. If the pupil persists, take a screenshot of their request and any accompanying messages
- Notify the senior leadership team or the headteacher about what's happening

A parent adds you on social media

- It is at your discretion whether to respond (it is strongly recommended that you do not add parents as friends on Face Book). Bear in mind that:
    - Responding to one parent's friend request or message might set an unwelcome precedent for both you and other teachers at the school
    - Pupils may then have indirect access through their parent's account to anything you post, share, comment on or are tagged in
- If you wish to decline the offer or ignore the message, consider drafting a stock response to let the parent know that you're doing so

You're being harassed on social media, or somebody is spreading something offensive about you

- **Do not** retaliate or respond in any way
- Save evidence of any abuse by taking screenshots and recording the time and date it occurred
- Report the material to Facebook or the relevant social network and ask them to remove it
- If the perpetrator is a current pupil or staff member, our mediation and disciplinary procedures are usually sufficient to deal with online incidents
- If the perpetrator is a parent or other external adult, a senior member of staff should invite them to a meeting to address any reasonable concerns or complaints and/or request they remove the offending comments or material
- If the comments are racist, sexist, of a sexual nature or constitute a hate crime, you or a senior leader should consider contacting the police

Appendix 2: Acceptable use of the internet: Home School Agreement for parents and carers and other information relevant to AUP

The home school agreement asks that parents support the school policies, learning from home and uphold courteous standards towards all of our school community:

School

The School will:

* Ensure your child's physical and social well-being at all times, and foster feelings of confidence, self-worth, belonging and independence.
* Deliver a broad, balanced and carefully planned curriculum which meets the needs of your individual child.
* Provide a range of after school extra-curricular activities designed to enrich your child's experience.
* Ensure that all homework tasks are given regularly and on the agreed day, and that they reflect your child's learning needs.
* Actively welcome parents/carers into the life of the school and to ensure that the teaching staff are always available, by mutual agreement, to discuss any concerns you might have about your child's progress or general welfare.
* Keep you informed about the school's policies and guidelines on behaviour and equal opportunities, other general school matters and about your child's progress in particular.
* Ensure that all teaching staff keep up to date on important educational developments and initiatives which might affect your child, and to inform you of these at key meetings, where appropriate.
* Uphold the professional standards for teachers.

Parents/Carers

I/We undertake to:

* Ensure that my child attends school regularly and that absences are properly notified.
* Ensure that my child arrives and where appropriate is collected promptly at the beginning and end of the school day.
* Support the school's policies e.g. Behaviour; Uniform; Equal Opportunities.
* Support my child in his/her homework and wherever possible promote opportunities for learning at home.
* Ensure my child goes to bed at a reasonable time on weekdays.
* Attend Parents' Evenings and discussions about my child's progress at school.
* Support the school in preparing children for life in multicultural Britain including the promotion of tolerance, respect and the rule of law.
* Uphold courteous standards towards all of our school community.
* Sign up for Parent Pay.

Pupils

I agree to:

* Always try to do my best in lessons.
* Always try to remember to be polite and thoughtful towards others.
* Always try to enjoy school and help other children do the same.
* Help make our school the best place it can be by treating everyone fairly.

Agreement.

School R. Kerton

Parents/Carers

_____

Please print name

Pupil

_____

Please Print Name

Acceptable use of the internet: agreement for parents and carers

As a member of our school and our school community I will adhere to our policy and this guidance/information:

Online channels are an important way for parents/carers to communicate with, or about, our school.

The school uses the following channels:

- Email/text groups for parents (for school announcements and information)
- Parent Pay
- Schoolcomms
- School's official Website
  Home | The Federation of Abbey Infant and Abbey Junior Schools (abbeyfederation.co.uk)
- Online learning platforms such as Education City, Purple Mash, Timestables Rockstars and Spelling Frame
- Parents/carers also set up private/independent channels to help them stay on top of what's happening in their child's class. For example, class/year group Facebook groups, email groups, or chats (through apps such as WhatsApp).

When communicating with the school via official communication channels, or using private/independent channels to talk about the school, I will:

- Be respectful towards members of staff, and the school, at all times

- Be respectful of other parents/carers and children
- Direct any complaints or concerns through the school's official channels, so they can be dealt with in line with the school's complaints procedure

I will not:

- Use private groups, the school's Facebook page, or personal social media to complain about or criticise members of staff. This is not constructive and the school can't improve or address issues if they aren't raised in an appropriate way
- Use private groups, the school's Facebook page, or personal social media to complain about, or try to resolve, a behaviour issue involving other pupils. I will contact the school and speak to the appropriate member of staff if I'm aware of a specific behaviour issue or incident
- Upload or share photos or videos on social media of any child other than my own, unless I have the permission of other children's parents/carers

Appendix 3: Acceptable use agreement for Pupils

Acceptable use of the school's ICT facilities and internet: agreement for pupils and parents/carers

As a pupil of Abbey I will follow our Acceptable Use policy and this guidance

When using the school's ICT facilities and accessing the internet in school, I will not:

- Use them for a non-educational purpose
- Use them without a teacher being present, or without a teacher's permission
- Use them to break school rules
- Go on to any inappropriate websites
- Go on to any social networking sites (unless my teacher has expressly allowed this as part of my learning)
- Use chat rooms
- Open any attachments in emails, or follow any links in emails, without first checking with a teacher
- Use mean, rude or any inappropriate language when talking with people online, or in emails
- Send any photos, videos or livestreams of people (including me) who aren't wearing all of their clothes (semi-nude or nude images).
- Share my password with others or log in using someone else's name or password or log in to the school's network using someone else's details
- Bully other people

I understand that the school will check the websites I visit and how I use the school's computers and equipment. This is so that they can help keep me safe and make sure I'm following the rules.

I will tell a teacher or a member of staff I know immediately if I find anything on a school computer or online that upsets me, or that I know is mean or wrong.

I will always be responsible when I use the school's ICT systems and internet.

I understand that the school can discipline me if I do certain unacceptable things online, even if I'm not in school when I do them.

Appendix 4: Acceptable use agreement for staff (including supply), governors, volunteer, visitors and contractors

Acceptable use of the school's ICT facilities and the internet: agreement for staff, governors, volunteers and visitors

As a member of our school and our school community I will adhere to our policy and this guidance/information:

When using the school's ICT facilities and accessing the internet in school, or outside school on a work device, I will not:

- Access, or attempt to access inappropriate material, including but not limited to material of a violent, criminal or pornographic nature (or create, share, link to or send such material)
- Use them in any way which could harm the school's reputation
- Access social networking sites or chat rooms
- Use any improper language when communicating online, including in emails or other messaging services
- Install any unauthorised software, or connect unauthorised hardware or devices to the school's network
- Share my password with others or log in to the school's network using someone else's details
- Share confidential information about the school, its pupils or staff, or other members of the community
- Access, modify or share data I'm not authorised to access, modify or share
- Promote private businesses, unless that business is directly related to the school

I understand that the school will monitor the websites I visit and my use of the school's ICT facilities and systems.

I will take all reasonable steps to ensure that work devices are secure and password-protected when using them outside school, and keep all data securely stored in accordance with this policy and the school's data protection policy.

I will let the designated safeguarding lead (DSL) and ICT manager know if a pupil informs me they have found any material which might upset, distress or harm them or others, and will also do so if I encounter any such material.

I will always use the school's ICT systems and internet responsibly, and ensure that pupils in my care do so too.

Appendix 5: Glossary of cyber security terminology

These key terms will help you to understand the common forms of cyber attack and the measures the school will put in place. They're from the National Cyber Security Centre (NCSC) glossary.

TERM	DEFINITION
Antivirus	Software designed to detect, stop and remove malicious software and viruses.
Cloud	Where you can store and access your resources (including data and software) via the internet, instead of locally on physical devices.
Cyber attack	An attempt to access, damage or disrupt your computer systems, networks or devices maliciously.
Cyber incident	Where the security of your system or service has been breached.
Cyber security	The protection of your devices, services and networks (and the information they contain) from theft or damage.
Download attack	Where malicious software or a virus is downloaded unintentionally onto a device without the user's knowledge or consent.
Firewall	Hardware or software that uses a defined rule set to constrain network traffic – this is to prevent unauthorised access to or from a network.
Hacker	Someone with some computer skills who uses them to break into computers, systems and networks.
Malware	Malicious software. This includes viruses, trojans or any code or content that can adversely impact individuals or organisations.
Patching	Updating firmware or software to improve security and/or enhance functionality.
Pentest	Short for penetration test. This is an authorised test of a computer network or system to look for security weaknesses.
Phishing	Untargeted, mass emails sent to many people asking for sensitive information (like bank details) or encouraging them to visit a fake website.
Ransomware	Malicious software that stops you from using your data or systems until you make a payment.

TERM	DEFINITION
Social engineering	Manipulating people into giving information or carrying out specific actions that an attacker can use.
Spear-phishing	A more targeted form of phishing where an email is designed to look like it's from a person the recipient knows and/or trusts.
Trojan	A type of malware/virus designed to look like legitimate software that can be used to hack a victim's computer.
Two-factor/multi-factor authentication	Using 2 or more different components to verify a user's identity.
Virus	Programs designed to self-replicate and infect legitimate software programs or systems.
Virtual Private Network (VPN)	An encrypted network which allows remote users to connect securely.
Whaling	Highly targeted phishing attacks (where emails are made to look legitimate) aimed at senior executives.

Appendix 6: Consent/Agreement for pupils to have a mobile phone in school

Dear Parent/Carer

RE: MOBILE PHONE PARENTAL CONSENT and AGREEMENT

In accordance with our Acceptable Use Policy, we understand that your child will be bringing a mobile telephone into school on a regular basis. Please sign the letter below providing consent for your child to do this and to demonstrate that you have read our Acceptable Use Policy for Information Communication Technology, with particular reference to section 6.4.

Please be reminded that:

1. Your child needs to turn off their mobile telephone as they enter the school site. This telephone should be placed into their school bag and remain in the bag for the entire school day.

2. The school bears no responsibility for any mobile telephone/multi-media device which is lost, damaged or stolen.

3. Your child's phone should be appropriately named and marked so that your child can easily recognise it and staff members can make every reasonable effort to return it to your child if it has been lost, stolen, confiscated or misplaced.

4. Other multi-media devices are strictly prohibited on school site.

5. Should your child be found to be using their phone during the school day or inappropriately, the school reserves the right to withdraw this privilege and they will no longer be able to bring a phone into school.

6. A phone may be confiscated and kept in a secure location in school. Once confiscated, the phone will be only be returned to a parent/carer, unless permission is granted for the child to collect the phone from the school office.

7. Our school expectations and practice are clearly explained in the Acceptable Use Policy. By signing this permission slip, you are agreeing that you have read and understood our procedure and that you fully agree to comply with our policy.

Yours sincerely,

Executive Head Teacher

Dr. R Kentish

MOBILE PHONE PARENTAL CONSENT

I/We give permission for our child_____Class __

to bring their mobile telephone into school. We have read, understand and agree with the policy.

Signed:_____Date: _____