ICT AND INTERNET ACCEPTABLE USE POLICY

Last review date	NEW POLICY
Date approved by the Trust	Summer 2022
Date approved by the Local Academy Committee	February 2023
Date for next review	Summer 2023

Document Control

Document version numbering will follow the following format. Whole numbers for approved versions, eg 1.0, 2.0, 3.0 etc. Decimals will be used to represent the current working draft version, eg 1.1, 1.2, 1.3 etc. For example, when writing a procedural document for the first time the initial draft will be version 0.1.

The table below provides details of the changes made to this document, to inform those reviewing and approving the document.

Document Edition	Section	Details of Change
0.1	All	New Trust-wide policy adopted from The Key for School Leaders model policy.

Contents

Introduction

The Leading Edge Academies Partnership (the 'Trust') is a team of school leaders that aim to be Leading Edge and pioneering in their approach to education and well-being. We are a growing family of like-minded schools that offer a values-based education to the communities we serve and welcome staff, workers, students, parents/carers and volunteers from all different ethnic groups and backgrounds.

The term 'Trust Community' includes all staff, trustees, governors, students, parents/carers, volunteers and visitors.

We are a values-based Trust, which means all actions are guided by our three 'Es' as follows:

- **Excellence** – 'Outstanding quality'
- **Evolution** – 'Continuous change'
- **Equity** – 'Fairness and social justice'

This policy is based on the value of **'Equity'**

Related policies

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

- Online safety
- Child Protection and Safeguarding
- Behaviour
- Staff discipline
- Data protection
- Remote learning
- Social Media
- Staff Code of Conduct

Policy Statement and Aims

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

However, the ICT resources and facilities our schools use also pose risks to data protection, online safety and safeguarding.

This policy aims to:

- Set guidelines and rules on the use of school ICT resources for staff, pupils, parents and governors
- 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 student behaviour policy/staff discipline policy/staff code of conduct.

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
- National Cyber Security Centre (NCSC)
- Education and Training (Welfare of Children Act) 2021

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, websites, web applications or services, and any device system or service which may become available in 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, printed output, web pages, social networking sites, and blogs.

See appendix 6 for a glossary of cyber security terminology.

Unacceptable use

The following is considered unacceptable use of the school's ICT facilities 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 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
- 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 school reserves the right to amend this list at any time. The Principal or any other relevant member of staff 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.

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 headteacher's discretion.

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 student behaviour/staff discipline/staff code of conduct.

Sanctions may include iPad confiscation and/or limited access to ICT systems alongside other appropriate sanctions as per our behaviour and discipline policies.

Copies of the student behaviour policy, staff discipline policy, staff code of conduct or explain can be found on the school website or copies can requested.

Staff (including governors, volunteers, and contractors)

Access to school ICT facilities and materials

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

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

Staff will be provided with unique and secure log-in/account information and secure 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 ICT manager. Access will be granted at the Principal's discretion. Staff must ensure that deployed devices are running the latest software.

Mounts Bay Academy will install certain apps onto the digital device for you. You must not uninstall or remove these under any circumstances.

Each Digital Device will be recorded and logged to an individual student with a unique reference number.

The Academy's Digital Devices must have a lock code enabled which is automatically activated after a short period of time when any Digital Device is not in use. If the Digital Device is left unattended, the device lock should be activated.

Digital Devices are covered under the Academy's insurance for accidental damage and theft only. The **Digital Devices Rules MUST be followed** as a condition of the insurance. The Digital Devices **MUST be in the complete, if supplied, case at all times.** The Academy reserves the right to check digital devices for any breach of the rules.

Staff are responsible for the care and safe keeping of their Digital Devices at all times. Staff should report a missing Digital Device to the police within 24 hours, if a Digital Device is lost or stolen, and obtain an incident number, which must be supplied immediately to the academy. Staff should not Use the Digital Devices in a public place, as this increases the chances of theft. Staff should not take the Digital Devices to a non-approved external repair company as it will invalidate the warranty and we cannot guarantee the quality of repairs.

Staff should not leave the Digital Devices unattended in a public place or in plain sight within any vehicle.

There will be a charge (at the discretion of the Academy) up to the full value of a replacement Digital Device or any provided equipment if it is lost or willfully damaged.

Use of phones and email

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

This email account should be used for work purposes only. Staff are recommended to enable multi-factor authentication on their email accounts.

All work-related business should be conducted using the email address the school has provided.

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 which contains the personal information of another person, they must inform the ICT manager immediately and follow our data breach procedure.

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.

School phones must not be used for personal matters.

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.

The school can record in-coming and out-going phone conversations.

If we consider it necessary to record calls, callers **will** be made aware that the conversation is being recorded and the reasons for doing so.

Staff who would like to record a phone conversation should speak to the Principal or Senior Vice Principal.

All non-standard recordings of phone conversations must be pre-approved, and consent obtained from all parties involved.

The school may grant requests to record conversations when:

- 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 assessments, etc.
- Discussing requests for term-time holidays

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 ICT manager 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 time/teaching hours/non-break time/office hours
- Does not constitute 'unacceptable use', as defined in section 4
- Takes place when no pupils are present

- Does not interfere with their jobs, or prevent other staff or pupils from using the facilities for work or educational purposes

Staff may not use the school's ICT facilities to store personal non-work-related information or materials (such as music, videos, or photos).

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 (see section 5.5). 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.

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.

Staff should take care to follow the school's guidelines on social media (see appendix 1) and use of email (see section 5.1.1) to protect themselves online and avoid compromising their professional integrity.

Personal social media accounts

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

The school has guidelines for staff on appropriate security settings for social media (e.g. Facebook) accounts (see Appendix 1).

Remote access

We allow staff to access the school's ICT facilities and materials remotely.

Systems used include SIMS, Office 365, Remote Desktop, CPOMS, Edulink, Firefly

The ICT Team manages the systems

Staff access systems through password protection and the Firewall

Staff can request remote access via the ICT team which uses IT Manager.

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 the ICT manager may require from time to time against importing viruses or compromising system security. Staff should not use unsecured networks.

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.

The school's data protection policy can be found on the school's website.

School social media accounts

The school has an official Facebook, Twitter, Instagram and LinkedIn page, managed by the Communications Manager, Principal and ICT Manager. Staff members who have not been authorised to manage, or post to, the account, must not access, or attempt to access the account.

The school has guidelines for what can and cannot be posted on its social media accounts. Those who are authorised to manage the account must ensure they abide by these guidelines at all times.

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

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
- Safeguard our students and staff

Pupils

Access to ICT devices and facilities

Digital Devices provided for the students at the school are provided under usage conditions as defined by this policy. The primary 'Purpose' of the iPads is as a tool for learning.

The device will be entrusted to parents/guardians who will be overall responsible for the iPad and will be granted a licence to loan the same to their child on receipt of a signed copy of this policy. For the avoidance of doubt, the device shall at all times remain the property of the Academy and the student is only permitted to use the Digital device for the 'Purpose'.

The Academy reserves the right to remotely install a range of Software Applications (Apps) to be present on the digital device at all times as well as defining a list of apps or class of apps that may not be present on the digital device under any circumstances.

Specialist ICT equipment, such as that used for music or design and technology must only be used under the supervision of staff.

Pupils will be provided with an account linked to the school's virtual learning environment (Firefly), which they can access from any device.

Digital devices are provided to all students and they are allowed to use them outside of school at home, with the primary focus of learning.

Apps

Apps that must be present on the Academy Digital Devices at all times:

Mounts Bay Academy will install certain apps onto the digital device for you. You must not uninstall or remove these under any circumstances.

There will be a range of other apps available to you via the Digital Devices Management System. You can install any of these you find useful, however if you run out of space on your digital device, these must be the first to consider deleting.

You many not install any other apps, even in the event of a system failure that enables the App Store. If you do this, your digital device will be removed for wiping and reinstalling. Your digital device must be set up with the Managed ID supplied.

Your digital device must be set up to receive emails as required by the school, as well as key learning apps. These may change each year and staff and students will be informed at the end of the year.

Apps the MUST NOT be present at any time on any Digital Devices:

Many of these services can be accessed via web pages that are blocked by the Academy:

- Social media apps
- Ki, Snapchat and other messaging apps
- Video chat apps, other than Teams where permitted
- Any browser other than Safari or Microsoft Edge
- Apps that disable iCloud backups
- Streaming music or video
- Proxies or VPNs (Virtual Private Networks)

The Academy will scan Digital Devices for inappropriate use and appropriate disciplinary action taken. Parents can be given full access to inappropriate web browsing activity, even when attempts at accessing such content are blocked.

Parental Control

Parents should know the Digital Device screen-lock code at all times. Where a student refuses to supply such a code, the IT team can remotely remove it.

Digital Devices rules:

Digital Devices should only be used for tasks appropriate to lessons or learning activities as follows:

- Each Digital Device will be recorded and logged to an individual student with a unique reference number.
- The Academy's Digital Devices must have a lock code enabled which is automatically activated after a short period of time when any Digital Device is not in use.
- If the Digital Device is left unattended, the device lock should be activated.
- Digital Devices are covered under the Academy's insurance for damage and theft only. The **Digital Devices Rules MUST be followed** as a condition of the insurance.
- The Digital Devices **MUST be in the complete, supplied case at all times.**
- The Academy reserves the right to check digital devices for any breach of the rules.
- **The student will:**
    - Be responsible for the care and safe keeping of their Digital Devices at all times

- Share their Digital Device screen-lock passcode with their parents/guardians and permit them access to review work, read school newsletters and oversee the safe and proper use of the device.
- Ensure that there is enough free space on their Digital Devices to store any work that they may be asked to do.
- Bring their Digital Devices into the Academy each morning fully charged and ready for use in lessons. Parents/guardians agree that they will ensure that Digital Devices are charged overnight in a public place in the student's home.
- Hand their Digital Devices to the teacher when leaving the classroom during a lesson, unless otherwise instructed by the teacher.
- Place the Digital Devices in a recognised secure place should the student need to leave it unattended.
- Report a missing Digital Device to the police within 24 hours, if a Digital Device is lost or stolen, and obtain an incident number, which must be supplied immediately to the academy.
- Report any damaged, lost or theft of the Digital Device to the Academy within 7 days.

- **The student will not:**
  - Use the Digital Devices outside the main building without supervision by a member of staff.
  - Use the Digital Devices during break and lunch times without permission from a member of teaching staff.
  - Use the Digital Devices in a public place, as this increases the chances of theft.
  - Take the Digital Devices to a non-approved external repair company as it will invalidate the warranty and we cannot guarantee the quality of repairs.
  - Leave the Digital Devices unattended: in school (unless it is held in a secure place), in a public place or in plain sight within any vehicle.

- **Charges**
  - A table of charges for damages to the Digital Device, or the loss or damage of any accessories, will be published each year by the Academy. In the event of the Digital Device being damaged when not in any supplied, complete and protective case, the full cost of any repairs will be charged.
  - There will be a charge (at the discretion of the Academy) up to the full value of a replacement Digital Device if it is lost or willfully damaged.
  - The above charges will also apply if your child causes damage to another student's Digital Device.
  - A charge for the full purchase cost will be levied for uninsured loss, malicious damage and/or failure to return a Digital Device after a student has left the academy.

Table of charges 2022/23:

Charging Lead £5
Charging Block £10
Case £30
Bent iPad £10
1st Damage £50
2nd and Subsequent Damage £75

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.

The IT Support Team may review pupils' files and communications to ensure that you are using the system responsibly. Concerns will be reported to the Senior Leadership Team.

Unacceptable use of ICT and the internet

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 breach intellectual property rights or copyright
- 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
- Attempting to bypass or alter the digital device security settings

Parents

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) 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.

Parents do have access to school systems: Edulink, Firefly, Seesaw, Parentmail and should use appropriate safety and security.

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 sign the agreement in appendix 2.

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.

Passwords

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

Do NOT WRITE PASSWORDS DOWN

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.

Users should not use someone else's login name or password or allow their login name or password to be used by anyone else.

All staff will use a password manager to help them store their passwords securely. The IT dept will generate passwords for pupils using a password manager/generator and keep these in a secure location in case pupils lose or forget their passwords.

The school allocates passwords and may require password updates as necessary.

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.

Data protection

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

The school's data protection policy can be found on the website.

All users should of the schools ICT facilities, systems and digital devices should avoid sharing their home address, telephone number, Academy name or picture to people they meet on the internet.

Access to facilities and materials

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

These access rights are managed by the ICT Manager

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 the ICT Manager immediately.

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

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 ICT manager.

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 (such as this one) at least annually, to objectively test that what it has in place is up to scratch
    - **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 daily (it can be automatic) and store these backups on cloud based backup systems/external hard drives that are not 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 external support provider
- Make sure staff:
    - Dial into our network using a virtual private network (VPN) when working from home / have a global proxy set on devices
    - 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, who will be contacted when, and who will notify Action Fraud of the incident. This will be reviewed and tested at least annually and after a significant event has occurred, using the NCSC's 'Exercise in a Box'
- Work with our Trust to see what it can offer the school regarding cyber security, such as advice on which service providers to use or assistance with procurement.

Internet access

The school wireless internet connection is secured.

- The school uses filtering
- There are separate connections for staff/pupils/visitors

Inappropriate sites that the filter hasn't identified (or appropriate sites that have been filtered in error) must be reported immediately to the ICT Manager.

Pupils

- Wifi is available throughout the school
- Security and filtering settings are used for all digital devices provided or used
- Pupils can request access if they are having problems from the IT department
- Access to digital devices is limited to daytime in school and up to 9:00pm for KS3 and 9:30pm for KS4.

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 a member of the Senior Leadership Team.

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 PTA)
- Visitors 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.

Monitoring and review

The headteacher and ICT Manager monitor the implementation of this policy, including ensuring that it is updated to reflect the needs and circumstances of the school.

This policy will be reviewed every year.

The governing board is responsible for approving this policy.

Appendix 1: Social Media (e.g. Facebook) cheat sheet for staff

10 rules for school staff on Social Media (e.g. Facebook, Instagram)

Do not accept friend requests from pupils on social media

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. Do not share anything publicly that you would not be just as happy showing your pupils
6. Do not use social media sites during school hours
7. Do not make comments about your job, your colleagues, our school or your pupils online – once it is out there, it is out there
8. Do not 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. Do not 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 have shared and look at your pictures if they are friends with anybody on your contacts list
- Do not 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 have **'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 cannot **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 do to 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 is happening

A parent adds you on social media

- It is at your discretion whether to respond. 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 are 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: agreement for parents and carers

Acceptable use of the internet: agreement for parents and carers	
Name of parent/carer: **Name of child:**	
Online channels are an important way for parents/carers to communicate with, or about, our school. The school uses the following channels: • Our official Facebook, Instagram, LinkedIn and Twitter pages • Email/text groups for parents (for school announcements and information) • Our virtual learning platform – Firefly • Edulink • Parent Mail • SeeSaw Parents/carers may also set up independent channels to help them stay on top of what is happening in their child's class. For example, class/year 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, Instagram, LinkedIn or Twitter page, or personal social media to complain about or criticise members of staff. This is not constructive and the school cannot improve or address issues if they are not raised in an appropriate way • Use private groups, the school's Facebook, Instagram, LinkedIn or Twitter 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 am 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 I have read and understood the ICT and Internet Acceptable Use Policy and agree to act in accordance with this policy.	
Signed:	**Date:**

Appendix 3: Acceptable use agreement for older pupils

Acceptable use of the school's ICT facilities, digital devices and internet: agreement for pupils and parents/carers	
Name of pupil:	
When using the school's ICT facilities and digital devices at school or at home 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 • Access any inappropriate websites • Access social networking sites (unless my teacher has expressly allowed this as part of a learning activity) • Use chat rooms • Open any attachments in emails, or follow any links in emails, without first checking with a teacher • Use any inappropriate language when communicating online, including in emails • Share any semi-nude or nude images, videos or livestreams, even if I have the consent of the person or people in the photo • Share my password with others or log in to the school's network using someone else's details • Bully other people I understand that the school will monitor the websites I visit and my use of the school's ICT facilities and systems. I will immediately let a teacher or other member of staff know if I find any material which might upset, distress or harm me or others. I will always use the school's ICT systems and internet responsibly. 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.	
Signed (pupil):	**Date:**
Parent/carer agreement: I agree that my child can use the school's ICT systems and internet when appropriately supervised by a member of school staff and use the school's digital device provided to my child which may also be used at home. I agree to the conditions set out above for pupils using the school's ICT systems and internet, ~~and for using personal electronic devices in school~~, and will make sure my child understands these.	
Signed (parent/carer):	**Date:**

Appendix 5: Acceptable use agreement for staff, governors, volunteers and visitors

Acceptable use of the school's ICT facilities, digital devices and the internet: agreement for staff, governors, volunteers and visitors	
Name of staff member/governor/volunteer/visitor:	
When using the school's ICT facilities **and digital devices at school or at home** 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 am 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 and the school's digital device if provided, which may also be used at home with agreement. 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. I have read and understood the ICT and Internet Acceptable Use Policy and agree to act in accordance with this policy.	
Signed (staff member/governor/volunteer/visitor):	**Date:**

Appendix 6: 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.