



# ICT AND INTERNET ACCEPTABLE USE POLICY

Last review date	September 2023
Date approved by the Trust Board	September 2023
Date for next review	September 2024

<b>Approved by Mounts Bay Academy Local Academy Committee for the 2023 24 academic year</b>	<b>November 2023</b>
---	----------------------

## 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.
1.1	All	Annual review incorporating KCSIE 2023.
2.0	All	Approved by Trust Board 20/09/23

# Contents

- Introduction ..... 5
  - Related policies..... 5
- Policy Statement and Aims ..... 5
- Relevant legislation and guidance ..... 6
- Definitions..... 6
- Unacceptable use ..... 6
  - Exceptions from unacceptable use ..... 7
  - Sanctions..... 8
- Staff (including governors, volunteers, and contractors) ..... 8
  - Access to school ICT facilities and materials..... 8
  - Use of phones and email ..... 8
  - Personal use..... 9
  - Personal social media accounts ..... 10
  - Remote access ..... 10
  - School social media accounts ..... 10
  - Monitoring of school network and use of ICT facilities ..... 10
- Pupils ..... 11
  - Access to ICT facilities ..... 11
  - Search and deletion ..... 14
  - Unacceptable use of ICT and the internet outside of school..... 14
- Parents..... 15
  - Access to ICT facilities and materials ..... 15
  - Communicating with or about the school online ..... 15
- Data security ..... 15
  - Passwords ..... 15
  - Software updates, firewalls, and anti-virus software ..... 15
  - Access to facilities and materials ..... 16
  - Encryption..... 16
- Protection from cyber attacks ..... 16
- Internet access..... 17
  - Pupils ..... 18
  - Parents and visitors ..... 18
- Monitoring and review ..... 18
- Disclaimer ..... 19
  - Appendix 1: Acceptable use of the internet: agreement for parents and carers ..... 20
  - Appendix 2: Acceptable use agreement for older pupils..... 21
  - Appendix 3: Acceptable use agreement for younger pupils..... **Error! Bookmark not defined.**

Appendix 4: Acceptable use agreement for staff, governors, volunteers and visitors .....	22
Appendix 5: Glossary of cyber security terminology .....	23

## 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 Staff Disciplinary Policy, Behaviour Policy or Codes 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 2023](#)
- [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 (mobile and landline), 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 5 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 proceedings or behaviour sanctions (see 'Sanction' section 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 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.

Requests for approval for such activities should be made in writing to the Principal.

## **Sanctions**

Pupils and staff who engage in any of the unacceptable activity listed above may face disciplinary action in line with the school's Staff Disciplinary Policy, Behaviour Policy or Codes of Conduct. Copies of our policies can be found on our website. Staff policies are on Teams.

We also reserve the right to impose appropriate sanctions, including revoking access to school systems and devices.

## **Staff (including governors, volunteers, and contractors)**

### **Access to school ICT facilities and materials**

The school's Digital Operations Leader 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 log-in/account information and passwords that they must use when accessing the school's ICT facilities.

Staff must not share these details or share equipment unless authorised by the Digital Operations Leader.

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 Digital Operations Leader.

Requests to access files/facilities should be made in writing to the Digital Operations Leader who will approve or deny access. The Digital Operations Leader will use professional judgement in these circumstances and seek approval from the Principal where appropriate.

### **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 should enable multi-factor authentication (where available) on their email accounts.

All work-related business must 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. Passwords to decrypt attachments should not be sent in the same email as the encrypted data.



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 Digital Operations Leader, Data Manager and Principal immediately and follow our data breach procedure.

Staff must not give their personal phone numbers to parents or pupils. Where provided, Staff must use phones provided by the school to conduct all work-related business. In other cases, staff must receive permission from the Principal before using personal phones for work-related matters.

School phones must not be used for personal matters.

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

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

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

We 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

We will not share such data with third parties without consent.

### **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 Digital Operations Leader 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
- Does not constitute 'unacceptable use', as defined in the 'Unacceptable Use' section of this policy.
- 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 on 'Monitoring of school network and use of ICT facilities')

Where breaches of this policy are found, disciplinary action may be taken.

Staff are 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 must adhere to the Staff Code of Conduct and Social Media policies 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 and must adhere to the Staff Code of Conduct and Social Media policies

### **Remote access**

We allow staff to access the school's ICT facilities and materials remotely when not on school premises.

- The ICT team manages the system
- 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 Digital Operations Leader may require from time to time against importing viruses or compromising system security.

Our ICT facilities contain information which is confidential and may be 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 can be found on our website - [Policies](#).

### **School social media accounts**

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

Those who are authorised to manage the account must ensure they abide by the school's Social Media policy at all times, which sets out what can and cannot be posted on its social media accounts. The Social Media policy can be found on our website - [Policies](#).

### **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 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 this '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 and Seesaw), which they can access from any device.

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

### **Apps**

There are apps that must be present on the Academy Digital Devices at all times

Mounds 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 (Jamf Student). 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 may 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 academy emails, signed into your Office 365 account using the Outlook app, 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:

- All Social media apps
- KiK, 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
- TikTok, 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 its supplied, complete and protective case, an additional cost may ~~the full cost of any repairs will~~ be charged.
  - There will be an additional 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.
  - iPads are entrusted to the students care at all times, if the ipad is lost or sustains damage, students and their families are required to pay for repair costs.

Table of charges 2023/24:

Charging Lead £5

Charging Block £10

Case £20

Bent iPad £10

1st Damage £50

2nd and Subsequent Damage £75

Full Cost of iPad £275

Students will be provided with unique log-in/account information and passwords that they must use when accessing the school's ICT facilities. Students must not share these details or share equipment unless authorised by the Digital Operations Leader.

## **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.

## **Unacceptable use of ICT and the internet, including 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
- Using ICT or the internet to breach intellectual property rights or copyright

## **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 or as a member of the PTA) 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 must not abuse access to school systems to find additional information about their child, or those linked

### **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 on admission of their child(ren) to the school.

## **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.

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 must keep their password secure, ideally with the use of a password manager to help them store their passwords securely. The IT department 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.

Users must not write passwords down

### **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 Trust's Data Protection policy can be found on our website - [Policies](#).

### **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 the Digital Operations Leader.

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 Digital Operations Leader 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.

### **Encryption**

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

School staff may only use personal devices to access school data (including storage devices such as USB drives), 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 Digital Operations Leader.

Personal USB/data sticks must not be used for work purposes.

### **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 once a day ~~(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
  - 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.

Full details of the school's policies and systems for internet access and online safety are contained in policies which can be found on our website.

All Trust schools follow the [guidance published by the Department for Education](#) with regard to filtering and monitoring. The Designated Safeguarding Lead in each school takes lead responsibility for ensuring appropriate filtering and monitoring systems are in place, in line with the requirements of KCSIE 2023.

- We have separate connections for staff/pupils/the public

## **Pupils**

Pupils have network configurations pre configured on their ipads. This provides a completely closed and secure network connection.

This ensures that student ipads receive the same level of filtering in all locations.

Students must not connect their own devices to the academy network.

- 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 10:30pm for KS4.

~~Explain your school's approach to the use of wifi by pupils, including:~~

- ~~Security and filtering settings are used for all digital devices provided or used~~

## **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 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 Digital Operations Leader 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 two years.

It is a Category B policy which is approved by the Trust Board and applies to all schools in the Trust, with school-specific elements approved by the Local Academy Committee.

**Disclaimer**

I have read and understood the ICT and Internet Acceptable Use Policy and agree to act in accordance with this policy as a condition of my employment by Leading Edge Academies Partnership.

Signed: .....

Name *(please print)*

**Appendix 1: Acceptable use of the internet: agreement for parents and carers**

<b>Acceptable use of the internet: agreement for parents and carers</b>	
<b>Name of parent/carer:</b>	
<b>Name of child:</b>	
<p>Online channels are an important way for parents/carers to communicate with, or about, our school.</p> <p>The school uses the following channels:</p> <ul style="list-style-type: none"> <li>• Our official Facebook page</li> <li>• Email/text groups for parents (for school announcements and information)</li> <li>• Our virtual learning platforms</li> </ul> <p>Parents/carers 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).</p>	
<p>When communicating with the school via official communication channels, or using private/independent channels to talk about the school, I will:</p> <ul style="list-style-type: none"> <li>• Be respectful towards members of staff, and the school, at all times</li> <li>• Be respectful of other parents/carers and children</li> <li>• 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</li> </ul> <p>I will not:</p> <ul style="list-style-type: none"> <li>• 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 cannot improve or address issues if they are not raised in an appropriate way</li> <li>• 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 am aware of a specific behaviour issue or incident</li> <li>• 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</li> </ul>	
<b>Signed:</b>	<b>Date:</b>

**Appendix 2: Acceptable use agreement for older pupils**

<b>Acceptable use of the school’s ICT facilities and internet: agreement for pupils and parents/carers</b>	
<b>Name of pupil:</b>	
<p><b>When using the school’s ICT facilities and accessing the internet in school, I will not:</b></p> <ul style="list-style-type: none"> <li>• Use them for a non-educational purpose</li> <li>• Use them without a teacher being present, or without a teacher’s permission</li> <li>• Use them to break school rules</li> <li>• Access any inappropriate websites</li> <li>• Access social networking sites (unless my teacher has expressly allowed this as part of a learning activity)</li> <li>• Use chat rooms</li> <li>• Open any attachments in emails, or follow any links in emails, without first checking with a teacher</li> <li>• Use any inappropriate language when communicating online, including in emails</li> <li>• Share any semi-nude or nude images, videos or livestreams, even if I have the consent of the person or people in the photo</li> <li>• Share my password with others or log in to the school’s network using someone else’s details</li> <li>• Bully other people</li> </ul> <p>I understand that the school will monitor the websites I visit and my use of the school’s ICT facilities and systems.</p> <p>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.</p> <p>I will always use the school’s ICT systems and internet responsibly.</p> <p>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.</p>	
<b>Signed (pupil):</b>	<b>Date:</b>
<p><b>Parent/carer agreement:</b> I agree that my child can use the school’s ICT systems and internet when appropriately supervised by a member of school staff. 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.</p>	
<b>Signed (parent/carer):</b>	<b>Date:</b>

**Appendix 4: Acceptable use agreement for staff, governors, volunteers and visitors**

<b>Acceptable use of the school’s ICT facilities and the internet: agreement for staff, governors, volunteers and visitors</b>	
<b>Name of staff member/governor/volunteer/visitor:</b>	
<p>When using the school’s ICT facilities and accessing the internet in school, or outside school on a work device, I will not:</p> <ul style="list-style-type: none"><li>• 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)</li><li>• Use them in any way which could harm the school’s reputation</li><li>• Access social networking sites or chat rooms</li><li>• Use any improper language when communicating online, including in emails or other messaging services</li><li>• Install any unauthorised software, or connect unauthorised hardware or devices to the school’s network</li><li>• Share my password with others or log in to the school’s network using someone else’s details</li><li>• Share confidential information about the school, its pupils or staff, or other members of the community</li><li>• Access, modify or share data I am not authorised to access, modify or share</li><li>• Promote private businesses, unless that business is directly related to the school</li></ul>	
<p>I understand that the school will monitor the websites I visit and my use of the school’s ICT facilities and systems.</p> <p>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.</p> <p>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.</p> <p>I will always use the school’s ICT systems and internet responsibly and ensure that pupils in my care do so too.</p>	
<b>Signed (staff member/governor/volunteer/visitor):</b>	<b>Date:</b>

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

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