The Park Federation Academy Trust

ICT, Internet and E-mail Acceptable Use Policy

September 2025

Version	Date	Status and Purpose	Changes overview
1	04 August 2022	Final	Change of title and template
2	01 September 2023		8.6 added Accessing Organisational data from personal devices
3	27 February 2024	Periodic review	Introducing Hannah Ball Academy
4	July 2024	Periodic review	Updates provided by Forbes solicitors
5	August 2025	Periodic review	4.0 reference made to the AI policy

Approval

Signed by the CEO and Federation Principal on behalf of the Board of Directors

Dr. Martin Young

Dr. Martin Young

Date of approval **August 2025**
Date of review **September 2026**

Notes on Document Control

This document is the property of The Park Federation Academy Trust (TPFAT) and its contents are confidential. It must not be reproduced, loaned or passed to a 3rd party without the permission of the authoriser.

It is controlled within the Park Federation Academy Trust Admin Server where the electronic master is held and can be accessed on a read only basis, subject to security permissions.

Users of the document are responsible for ensuring that they are working with the current version.

Paper or electronic copies may be taken for remote working etc. However, all paper copies or electronic copies not held within the Admin Server are uncontrolled.
Hence the footer 'DOCUMENT UNCONTROLLED WHEN PRINTED' which must not be changed.

Once issued, as a minimum this document shall be reviewed on an annual basis by the originating team/function. Any amendments shall be identified by a vertical line adjacent to the right hand margin.

To enable continuous improvement, all readers are encouraged to notify the author of errors, omissions and any other form of feedback.

Contents

1. Introduction and aims

Information and communications technology (ICT) is an integral part of the way our trust/academy works, and is a critical resource for children, staff (including senior leadership teams), Academy Council members and Board Directors, volunteers and visitors. It supports teaching and learning, pastoral and administrative functions of the academy.

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

This policy aims to:

- Set guidelines and rules on the use of academy ICT resources for staff, children, parents and Academy Council members and Board Directors
- Establish clear expectations for the way all members of the academy community engage with each other online
- Support the academy's policy on data protection, online safety and safeguarding
- Prevent disruption to the academy through the misuse, or attempted misuse, of ICT systems
- Support the academy in teaching children safe and effective internet and ICT use

This policy covers all users of our academy's ICT facilities, including Academy Council members and Board Directors, staff, children, volunteers, contractors and visitors.

Breaches of this policy may be dealt with under our disciplinary policy, behaviour policy and staff code of conduct.

2. Relevant legislation and guidance

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

- Data Protection Act 2018
- The UK General Data Protection Regulation (UK GDPR) – the EU GDPR was incorporated into UK legislation, with some amendments, by The Data Protection, Privacy and Electronic Communications (Amendments etc) (EU Exit) Regulations 2020
- 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
- Education and Inspections Act 2006
- Keeping Children Safe in Education 2025
- Searching, screening and confiscation: advice for schools 2022
- National Cyber Security Centre (NCSC): Cyber Security for Schools
- Education and Training (Welfare of Children) Act 2021
- UK Council for Internet Safety (et al.) guidance on sharing nudes and semi-nudes: advice for education settings working with children and young people
- Meeting digital and technology standards in schools and colleges

3. Definitions

- **"ICT facilities":** includes all facilities, systems and services including but not limited to network infrastructure, desktop computers, laptops, chromebooks, 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 academy to use the ICT facilities, including Academy Council members, Board Directors, staff, children, 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 academy 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.

4. Unacceptable use

The following is considered unacceptable use of the academy's ICT facilities by any member of the academy community. Any breach of this policy may result in disciplinary or behaviour proceedings (see section 4.2 below).

Unacceptable use of the trust/academy's ICT facilities includes:

- Using the trust/academy's ICT facilities to breach intellectual property rights or copyright

- Using the academy's ICT facilities to bully or harass someone else, or to promote unlawful discrimination
- Breaching the academy'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 trust/academy, or risks bringing the academy into disrepute
- Sharing confidential information about the trust/academy, its children, or other members of the academy community
- Connecting any device to the academy's ICT network without approval from authorised personnel
- Setting up any software, applications or web services on the academy'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 academy'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 academy
- Using websites or mechanisms to bypass the academy's filtering mechanisms
- Engaging in content or conduct that is radicalised, extremist, racist, anti-Semitic or discriminatory in any other way
- Non compliance with our AI policies or procedures

This is not an exhaustive list. The academy reserves the right to amend this list at any time. The Principal, CEO or Board Directors will use professional judgement to determine whether any act or behaviour not on the list above is considered unacceptable use of the academy's ICT facilities.

4.1 Exceptions from unacceptable use

Where the use of academy ICT facilities (on the academy 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 Principal's discretion. For approval you would need to email or discuss with the Principal for such activities.

4.2 Sanctions

Children and staff who engage in any of the unacceptable activity listed above may face disciplinary action in line with the academy's policies. Which are either on the website or for staff in the secure server.

5. Staff (including Academy Council members and Board Directors, volunteers, and contractors)

5.1 Access to academy ICT facilities and materials

The trust/academy's Network Manager manages access to the academy's ICT facilities and materials for academy staff. That includes, but is not limited to:

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

Staff will be provided with unique log-in/account information and passwords that they must use when accessing the academy'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 Network Manager via email.

5.1.1 Use of phones and email

The academy 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 on their email accounts.

All work-related business should be conducted using the email address the trust/academy has provided.

Staff must not share their personal email addresses with parents and children, 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 confirmation given that the email has been deleted from your inbox and bin. If the email contains sensitive or confidential information, the user must not make use of that information or disclose that information.

If staff send an email in error that contains the personal information of another person, they must inform the Principal, Network Manager and Data Protection Officer (DPO) immediately and follow our data breach procedure.

Staff must not give their personal phone numbers to parents or children. Staff must use phones provided by the academy to conduct all work-related business.

Trust/academy 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.

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

5.2 Personal use

Staff are permitted to occasionally use academy ICT facilities for personal use. subject to certain conditions set out below. Personal use of ICT facilities must not be overused or abused. The CEO, Principal or Network Manager may withdraw or restrict 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 and non-break time
- Does not constitute 'unacceptable use', as defined in section 4
- Takes place when no children are present
- Does not interfere with their jobs, or prevent other staff or children from using the facilities for work or educational purposes

Staff may not use the academy'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 academy's ICT facilities for personal use may put personal communications within the scope of the academy's ICT monitoring activities (see section 5.4). Where breaches of this policy are found, disciplinary action may be taken.

Staff should be aware that personal use of ICT (even when not using academy ICT facilities) can impact on their employment by, for instance, putting personal details in the public domain, where children and parents could see them.

Staff should take care to follow the academy'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.

5.2.1 Personal social media accounts

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

The academy has guidelines for staff on appropriate security settings for Facebook accounts (see appendix 1).

5.3 Remote access

We allow staff to access the academy's ICT facilities and materials remotely via RDWeb.

Staff accessing the academy'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 academy's ICT facilities outside the academy and take such precautions as the Principal and Network Manager may require from time to time against importing viruses or compromising system security.

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

The Data Protection Policy can be found on the academy website.

For further information on remote access please refer to our remote access policy.

5.4 Monitoring and filtering of the trust/ academy network and use of ICT facilities

The trust has official social media accounts, authorised by the CEO. Staff members who have not been authorised to manage, or post to, the account, must not access, or attempt to access, the account.

The trust has guidelines for what may and must not be posted on its social media accounts. Those who are authorised to manage, or post to, the account must make sure they abide by these guidelines at all times.

To safeguard and promote the welfare of children and provide them with a safe environment to learn, the trust/academy reserves the right to filter and monitor the use of its ICT facilities and network. This includes, but is not limited to, the filtering and 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 trust/academy monitors ICT use in order to:

- Obtain information related to trust/academy business
- Investigate compliance with trust/academy policies, procedures and standards
- Ensure effective trust/academy 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

Our Trust Board is responsible for making sure that:

- The Trust meets the DfE's filtering and monitoring standards
- Appropriate filtering and monitoring systems are in place
- Staff are aware of those systems and trained in their related roles and responsibilities
- For the leadership team and relevant staff, this will include how to manage the processes and systems effectively and how to escalate concerns
- It regularly reviews the effectiveness of its monitoring and filtering systems

The Trust' s Senior Adviser for Safeguarding (DSL) will take lead responsibility for understanding the filtering and monitoring systems and processes in place.

Where appropriate, staff may raise concerns about monitored activity with their academy or the Trust DSL and IT Network manager, as appropriate.

5.5 Access to Email Messages

The Trust or the academy will not normally access any individual's mailbox without the permission of that individual. However, there may be occasions when the information must be accessed by the Network Manager and is deemed necessary to access a user's E-mail mailbox without the employee's permission, by Senior Managers of The Park Federation Academy Trust (TPFAT) e.g. Chief Executive Officer, Chief Operating Officer etc.

Examples of reasons for accessing an individual's mailbox are, but not limited to:

- To action subject access requests under the Data Protection Act
- To obtain Freedom of Information requests
- To obtain evidence in support of disciplinary action
- To obtain evidence in a criminal investigation
- To obtain evidence in legal proceedings
- To obtain access to TPFAT business data

5.6 Usage of YouTube for Education

Videos on the file-sharing website YouTube can be used to effectively support many areas of the curriculum. The popular site contains a selection of videos which cover the range of topics focused across the academies within The Park Federation Academy Trust – most noticeably, Science and History topics. Additionally, there is a variety of music, song and dance performances appropriate for children. When these videos are used safely and appropriately, they can be an extremely beneficial resource for Class Teachers and Support Staff.

However, there are potential risks when working with YouTube that staff should be aware of. For example,

despite a filter/flagging policy being in use on YouTube, inappropriate images, unsuitable written comments, or bad language can still all be accidentally revealed to the children. In order to prevent this from happening, the following precautions should be taken:

Finding suitable videos:

- Searches, or first observations of a potential video, should not be carried out with any child in the class room.

- Before showing a video to the class, the video should be watched and listened to carefully by the Class Teacher, who should look out for inappropriate content material along with any inappropriate comments that appear underneath the video.

- The class teacher should ensure that any YouTube comments or recommended watch lists in the YouTube sidebar are hidden from view.

- Teachers can ascertain whether YouTube videos are accessible through the Trust's filtering system by viewing the video whilst on site at a Federation academy, or via remote access. To request a YouTube video to be unblocked, the teacher must first obtain permission from the principal before submitting a request to the Network Manager.

- It is the class teacher's responsibility to make the final approval of a video.

Playing the video for the children:

- Using the remote control, the Smartboard should be frozen, stilled or muted (depending on the option available on your remote) prior to Full Screen mode being selected for the video. (This is so that no comments or any other videos can be seen by the children). When the video is ready, the Smartboard can be unfrozen and the video watched.

- Before the end of the video, pause it so 'recommended' videos that might potentially contain inappropriate language, are not revealed.

- When the video is finished, the Smartboard should once again be frozen, stilled or muted (or even turned off) so that the video can be exited and the YouTube window closed safely.

Should any inappropriate content be shown this MUST be reported to the Principal immediately and an email also needs to be sent to the IT Network Manager so that the content can be blocked through the Federation filtering system.

5.6 Email Phishing Guidance

Criminals send malicious email communications all the time to extract information from individuals. This is called phishing, which means tricking you into sending them sensitive information by clicking on links or opening attachments. They also try to persuade you to inadvertently install malware on your computer. The messages they send can place your data and computer at risk to all manner of threats.

We all get phishing emails so this may help you to spot them and avoid being phished!

1: Proceed with caution!

- Emails can come from anywhere so never assume they are genuine, especially if they are unexpected.

- Pause for a moment and consider the message carefully, whatever the format.

- **DON'T** automatically click on links or open attachments.
- **DON'T** automatically reply or try to unsubscribe.
- **DON'T** automatically contact any phone numbers in the message. Look up phone numbers from an official source such as the legitimate website of the sender.
- Remember that company logos, branding and web addresses can easily be forged in messages to make them look more realistic.

2: Things you should all look out for in a phishing Email:

- Is your name missing or incorrectly spelt? Reputable companies usually personalise their communications with your name.
- Is the grammar right and are there lots of spelling mistakes?
- If it appears to be from someone you know, does it look and sound right?
- Is the message requesting personal data or bank details?
- Are you asked to do something like validate account credentials or re-activate an account?
- Are you asked to make payments immediately?
- Has the message been sent to multiple recipients?
- Did the message come out of the blue? Companies don't just contact you asking questions or offering things without you doing something first.

3: Check for hooks

- Does the sender's address match the organisation that supposedly sent the message?
- Hover over all links to check where they really go.

4: What to do when you identify a phishing Email:

- You can report all suspected spam, phishing by forwarding it to the Network Manager then delete it from your "Inbox, Sent and Deleted item".

All cyber spam, phishing is reported to https://www.actionfraud.police.uk/report_fraud

6. Children

6.1 Access to ICT facilities

- Computers and equipment in the academy's ICT suite or classroom are available to children only under the supervision of staff
- Specialist ICT equipment, such as that used for music, or design and technology, must only be used under the supervision of staff

- Children will be provided with an account linked to the academy's virtual learning environment, which they can access from academy devices

6.2 Search and deletion

Under the Education Act 2011, and in line with the Department for Education's guidance on searching, screening and confiscation, the academy has the right to search children' phones, computers or other devices that the authorised staff member has reasonable grounds for suspecting:

- Poses a risk to staff or pupils, **and/or**
- Is identified in the academy rules as a banned item for which a search can be carried out as outlined in our Behaviour policy **and/or**
- Is evidence in relation to an offence

This includes, but is not limited to:

- Pornography
- Abusive messages, images or videos
- Indecent images of children
- Evidence of suspected criminal behaviour (such as threats of violence or assault)

Before a search, if the authorised staff member is satisfied that they have reasonable grounds for suspecting any of the above, they will also:

- Make an assessment of how urgent the search is, and consider the risk to other children and staff. If the search is not urgent, they will seek advice from the CEO, Principal and designated safeguarding lead.
- Explain to the child why they are being searched, and how and where the search will happen, and give them the opportunity to ask questions about it
- Seek the child's co-operation (if the child refuses to co-operate, you should proceed according to your behaviour policy)

The authorised staff member should:

- Inform the DSL (or deputy) of any searching incidents where they had reasonable grounds to suspect a child was in possession of a banned item. A list of banned items is available in the Safeguarding Policy.
- Involve the DSL (or deputy) without delay if they believe that a search has revealed a safeguarding risk

Authorised staff members may examine, and in exceptional circumstances erase, any data or files on a device that they have confiscated where they believe there is a 'good reason' to do so.

When deciding whether there is a 'good reason' to examine data or files on a device, the staff member should only do so if they reasonably suspect that the data has been, or could be, used to:

- Cause harm, **and/or**
- Undermine the safe environment of the school or disrupt teaching, **and/or**
- Commit an offence

If inappropriate material is found on the device, it is up to the DSL in conjunction with the Principal or CEO to decide on a suitable response. If there are images, data or files on the device that staff reasonably suspect are likely to put a person at risk, they will first consider the appropriate safeguarding response.

When deciding whether there is a good reason to erase data or files from a device, staff members will consider whether the material may constitute evidence relating to a suspected offence. In these instances, they will not delete the material, and the device will be handed to the police as soon as is reasonably practicable. If the material is not suspected to be evidence in relation to an offence, staff members may delete it if:

- They reasonably suspect that its continued existence is likely to cause harm to any person, **and/or**
- The pupil and/or the parent refuses to delete the material themselves

If a staff member **suspects** a device **may** contain an indecent image of a child (also known as a nude or semi-nude image), they will:

- **Not** view the image
- **Not** copy, print, share, store or save the image
- Confiscate the device and report the incident to the DSL (or deputy) immediately, who will decide what to do next. The DSL will make the decision in line with the DfE's latest guidance on searching, screening and confiscation and the UK Council for Internet Safety (UKCIS) et al.'s guidance on sharing nudes and semi-nudes: advice for education settings working with children and young people

Any searching of children will be carried out in line with:

- The DfE's latest guidance on searching, screening and confiscation
- UKCIS et al.'s guidance on sharing nudes and semi-nudes: advice for education settings working with children and young people
- Our behaviour policy

Any complaints about searching for, or deleting, inappropriate images or files on children's' devices will be dealt with through the academy complaints procedure.

6.3 Unacceptable use of ICT and the internet outside of academy

The trust/academy will sanction children, in line with its policy, if a child engages in any of the following **at any time** (even if they are not on academy 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 trust/academy'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 academy, or risks bringing the academy into disrepute
- Sharing confidential information about the academy, other children, or other members of the academy 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 academy'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

Sanctions may apply in line with our policies.

7. Parents/carers

7.1 Access to ICT facilities and materials

Parents/carers do not have access to the trust/academy's ICT facilities as a matter of course.

However, parents/carers working for, or with the academy 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 academy's facilities at the Principal's discretion.

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

7.2 Communicating with or about the trust/academy online

We believe it is important to model for children, 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 academy through our website and social media channels.

We ask parents to sign the agreement in appendix 2.

8. Data security

The trust/academy is responsible for making sure it has the appropriate level of security protection and procedures in place to safeguard its systems, staff and learners. It therefore takes steps to protect the security of its computing resources, data and user accounts. The effectiveness of these procedures is reviewed periodically to keep up with evolving cyber-crime technologies.

Staff, children, parents/carers and others who use the academy's ICT facilities should use safe computing practices at all times. We aim to meet the cyber security standards recommended by the Department for Education's guidance on digital and technology standards in schools and colleges, including the use of:

- Firewalls
- Security features
- User authentication and multi-factor authentication
- Anti-malware software

8.1 Passwords

All users of the trust/academy's ICT facilities should set strong passwords for their accounts and keep these passwords secure. These should be unique for every account to prevent hackers accessing multiple accounts.

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 children who disclose account or password information may face disciplinary action. Parents or volunteers who disclose account or password information may have their access rights revoked.

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

Passwords will be updated periodically.

8.2 Software updates, firewalls and anti-virus software

All of the trust/academy'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 academy's ICT facilities.

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

8.3 Data protection

All personal data must be processed and stored in line with data protection regulations and the academy's data protection policy. The Data Protection Policy is available on the academy website.

8.4 Access to facilities and materials

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

These access rights are managed by the Network 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 Principal, Network Manager or DPO immediately.

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

8.5 Encryption

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

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

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

8.6 Accessing Organisational data from personal devices

In order to ensure the security and confidentiality of organisational data, it is imperative that all personal devices used to access such data are equipped with encryption measures. Encryption adds an additional layer of protection, safeguarding sensitive information from unauthorized access or interception. Furthermore, it is crucial that these devices are regularly updated with the latest antivirus software. Keeping antivirus programs up to date helps detect and mitigate potential threats, reducing the risk of malware or viruses compromising organizational data. Additionally, it is vital to restrict the installation of applications solely to those sourced from trusted and verified platforms. By adhering to this policy, we minimise the chances of inadvertently introducing malicious software that could compromise the integrity of our data and systems. This proactive approach ensures the highest level of security and promotes responsible and secure usage of personal devices within the organization.

9. Protection from cyber attacks

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

The academy will:

- Work with Academy Council members, Board Directors and the IT department to make sure cyber security is given the time and resources it needs to make the academy secure
- Provide annual training for staff (and include this training in any induction for new starters, if they join outside of the academy'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 academy will verify this using a third-party audit (such as this one) 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 academy 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 and store these backups locally and remotely on backup systems/external hard drives that aren't connected to the academy network.
- Delegate specific responsibility for maintaining the security of our management information system (MIS) to our cloud-based provider.
- Make sure staff:
    - Remote into our network using a virtual private network (VPN) when working from home
    - Enable multi-factor authentication where they can, on things like academy email accounts
    - Store passwords securely using a password manager
- Make sure ICT staff conduct regular access reviews to make sure each user in the academy 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 academy 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'

10. Internet access

The academy wireless internet connection is secured.

Access Summary

Our service VPN network is hosted through TrustNet and internet filtering is provided through TrustNet (LGFLv2) and Atomwide.

All PCs on our network are protected using Sophos anti-virus, all access to the internet is filtered using multiple streams including key-words, word-group blockings and internet site blockings.

Any network devices that accesses services or internet using hardwired or wireless services within our academies are subjected to the same filtering policy as any other devices on our network. This would cover BYOD (Bring Your Own Device), e.g. laptops, tablets and mobile phones.

Many sites from the internet are filtered and therefore automatically blocked and cannot be unblocked.

Academies and schools work at "Secure and Detection level 3". This means that every effort is made to secure our systems internally and the same effort is given to detection of intrusion of our systems externally.

A copy of the Category Definitions from LGfL can be made available and put into a word document and stored on our network. The categories allow us to state that we are compliant with the "UK Safer Internet Centre" safeguarding of children and staff using our internet service.

In the event that the filter has not identified an inappropriate site then this must be reported to the Principal and Network Manager immediately.

10.1 Acces to Wi-Fi

Wireless Summary

1, TPFAT-Staff. Users (with an account on our domain) using TPFAT-Staff will be able to gain access to our network services through network authentication.

2. TPFAT-Student. Users (with an account on our domain) using TPFAT-Student are restricted to the children's' area which is only accessed by network authentication.

3. TPFAT-Guest. This account will give a user restricted internet access only, at the same time bypassing our network domain, (not visible to the user).

10.2 Parents/carers and visitors

Parents/carers and visitors to the academy will not be permitted to use the academy's Wi-Fi unless specific authorisation is granted by the Principal.

The Principal will only grant authorisation if:

- Parents are working with the academy in an official capacity (e.g. as a volunteer or as a member of the PTA)
- Visitors need to access the academy's Wi-Fi 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 Wi-Fi password to anyone who is not authorised to have it. Doing so may result in disciplinary action.

11. Monitoring and review

The CEO, Principal and Network Manager monitor the implementation of this policy, including ensuring it is updated to reflect the needs and circumstances of the Trust/academy.

This policy will be reviewed annually and the CEO is responsible for approving this policy on behalf of the Board of Directors.

12. Related policies

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

- Online safety
- Social media
- Safeguarding and child protection
- Behaviour
- Staff discipline

- Data protection
- Remote learning
- Mobile phone usage

Do not accept friend requests from pupils on social media

10 rules for trust/academy staff on Facebook

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

Check your privacy settings

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

What to do if …

A pupil adds you on social media

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

A parent/carer adds you on social media

- It is at your discretion whether to respond. Bear in mind that:
    - Responding to 1 parent/carer's friend request or message might set an unwelcome precedent for both you and other teachers at the academy
    - Children may then have indirect access through their parent/carer'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/carer know that you're doing so

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

- **Do not** retaliate or respond in any way
- Save evidence of any abuse by taking screenshots and recording the time and date it occurred
- Report the material to Facebook or the relevant social network and ask them to remove it
- If the perpetrator is a current pupil or staff member, our mediation and disciplinary procedures are usually sufficient to deal with online incidents
- If the perpetrator is a parent/carer 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 trust/academy. The academy uses the following channels: • Instagram • Email/text groups for parents (for school announcements and information) • PIOTA/Arbor • You tube • Our virtual learning platforms	
When communicating with the trust/academy via official communication channels, or using private/independent channels to talk about the trust/academy, I will: • Be respectful towards members of staff, and the trust/academy, at all times • Be respectful of other parents/carers and children • Direct any complaints or concerns through the trust/academy's official channels, so they can be dealt with in line with the trust/academy's complaints procedure I will not: • Use private groups or personal social media to complain about or criticise members of staff. This is not constructive and the trust/academy can't improve or address issues unless they are raised in an appropriate way • Use private groups or personal social media to complain about, or try to resolve, a behaviour issue involving other children. I will contact the academy and speak to the appropriate member of staff if I'm aware of a specific behaviour issue or incident • Upload or share photos or videos on social media of any child other than my own, unless I have the permission of the other children's parents/carers	
Signed:	**Date:**

Appendix 3: Acceptable use agreement for older pupils

Acceptable use of the academy ICT facilities and internet: agreement for children and parents/carers	
Name of pupil:	
When using the s=academy ICT facilities and accessing the internet in the academy, 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/video • Share my password with others or log in to the academy network using someone else's details • Bully other peopleI 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 academy's ICT systems and internet responsibly. I understand that the academy can discipline me if I do certain unacceptable things online, even if I'm not in the acdemy when I do them.	
Signed (pupil):	**Date:**
Parent/carer agreement: I agree that my child can use the trust/academy's ICT systems and internet when appropriately supervised by a member of staff. I agree to the conditions set out above for children using the academy ICT systems and internet, and for using personal electronic devices in the academy, and will make sure my child understands these.	
Signed (parent/carer):	**Date:**

Appendix 4: Acceptable use agreement for younger pupils

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

Name of pupil:

When I use the school's ICT facilities (like computers and equipment) and go on the internet in school, I will not:

- Use them without asking a teacher first, or without a teacher in the room with me
- Use them to break school rules
- Go on any inappropriate websites
- Go on Facebook or other social networking sites (unless my teacher said I could as part of a lesson)
- Use chat rooms
- Open any attachments in emails, or click any links in emails, without checking with a teacher first
- Use mean or rude language when talking to other people online or in emails
- Send any photos, videos or livestreams of people (including me) who aren't wearing all of their clothes
- Share my password with others or log in using someone else's name or password
- Bully other people

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

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

I will always be responsible when I use the trust/academy's ICT systems and internet.

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

Signed (pupil):	**Date:**

Parent/carer agreement: I agree that my child can use the trust/academy's ICT systems and internet when appropriately supervised by a member of staff. I agree to the conditions set out above for children using the ICT systems and internet, and for using personal electronic devices in the trust/academy, 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 trust/academy's ICT facilities and the internet: agreement for staff, governors, volunteers and visitors	
Name of staff member/governor/volunteer/visitor:	
When using the ICT facilities and accessing the internet in or outside the trust/academy 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 academy'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 academy'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 academy, its children or staff, or other members of the community • Access, modify or share data I'm not authorised to access, modify or share • Promote any private business, unless that business is directly related to the academy	
I understand that the school will monitor the websites I visit and my use of the school's ICT facilities and systems. I will take all reasonable steps to ensure that work devices are secure and password-protected when using them outside the trust/academy, and keep all data securely stored in accordance with this policy and the data protection policy. I will let the designated safeguarding lead (DSL) and ICT manager know if a child 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 trust/academy's ICT systems and internet responsibly, and ensure that children in my care do so too.	
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.
Breach	When your data, systems or networks are accessed or changed in a non-authorised way.
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.
Pharming	An attack on your computer network that means users are redirected to a wrong or illegitimate website even if they type in the right website address.

TERM	DEFINITION
Phishing	Untargeted, mass emails sent to many people asking for sensitive information (such as 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.
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	Programmes 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 people in an organisation.