The Park Federation Academy Trust

ICT, Internet and E-mail

Acceptable Use Policy 2023

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

Approval

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

Dr. Martin Young

Date of approval **September 2023**
Date of review **September 2024**

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 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 General Data Protection Regulation

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

3. Definitions

- **"ICT facilities":** includes all facilities, systems and services including but not limited to network infrastructure, desktop computers, laptops, tablets, phones, music players or hardware, software, 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 and 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 academy's ICT facilities includes:

- Using the 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 academy, or risks bringing the academy into disrepute

- Sharing confidential information about the 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

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 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 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.

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 Principal or Network Manager may withdraw permission for it at any time or restrict access at their discretion.

Personal use is permitted provided that such use:

- Does not take place during 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 of academy network and use of ICT facilities

The academy 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 academy monitors ICT use in order to:

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

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 it 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.

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 schools 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 or Teaching Assistant, who should look out for inappropriate content material along with any inappropriate comments that appear underneath the video.

- 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 for pornographic images or any other data or items banned under academy rules or legislation.

The academy 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 academy's rules.

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

6.3 Unacceptable use of ICT and the internet outside of academy

The 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 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

7.1 Access to ICT facilities and materials

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

However, parents 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 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 academy 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 academy cannot guarantee security. Staff, children, parents and others who use the academy's ICT facilities should use safe computing practices at all times.

8.1 Passwords

All users of the 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 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 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 pupil 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 organizational 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 minimize 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 1) to help you understand cyber security terminology.

The academy will:

- Work with Academy Council members and 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:
    - Dial 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 and visitors

Parents 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 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
- Safeguarding and child protection
- Behaviour
- Staff discipline
- Data protection
- Remote learning
- Mobile phone usage

Appendix 1: Glossary of cyber security terminology

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

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

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