ICT Acceptable Usage Policy

TPAT Policy Management

Document history					
Review date	**Version**	**Reviewer / owner**	**Executive approval**	**Approving body**	**Meeting date of policy approval**
11/2023	1	Director of IT	11/2023	FRAC	email approval 16 November 2023
11/2024	2	Director of IT	11/2024	FRAC	25/11/2024

Material changes since last publication	
Section	**Changes**
Version 2	No changes

This policy is reviewed annually. The next review is due by November 2025.

Contents

1. Introduction

    1.1 Aims and Scope

    1.2 Relevant Legislation and Guidance

    1.3 Other Linked Policies

2. Policy Statement

3. Provision of School Information and Communication Tools

4. Trust Property

5. Passwords

6. Software

7. Virus Protection

8. Use of Trust-Provided Equipment by Third Parties

9. BYOD / Use of Personal Devices

10. Remote Access

11. Privacy

12. Confidential Information

13. File Storage and Archiving

14. The Internet

15. Email

16. Social Media

17. Protection from Cyber Attacks

18. Telephones and Voicemail

19. Misrepresentation or Misuse of Technology

Appendix 1 Glossary of cyber security terminology

1. Introduction

The Trust intends and expects that all decisions, policies and procedures will be underpinned at all times by its vision and values:

Our aim:

To create centres of educational excellence that inspire all pupils to turn their potential into performance.

To achieve this our schools will:

- Provide a broad and balanced curriculum that allows pupils to develop their talents and ambitions.
- Deliver the highest quality learning opportunities facilitated by excellent teachers.
- Inspire our pupils to become confident, motivated and respectful individuals ready to make a positive contribution to society.

The Trust will support our schools by:

- Maximising the resources and expertise available to individual schools.
- Providing a platform for the sharing of excellent practice.
- Challenging and developing staff to turn their potential into performance.

1.1 Aims and Scope

Use of ICT resources and facilities within the Trust could also pose risks to data protection, online safety and safeguarding.

This policy aims to:

- Set guidelines and rules on the use of Trust ICT resources for staff, pupils, parents, Trustees and LAB members
- Establish clear expectations for the way all members of the Trust community engage with each other online
- Support the Trust's policies on data protection, online safety and safeguarding
- Prevent disruption that could occur to the Trust through the misuse, or attempted misuse, of ICT systems
- Support the Trust in teaching pupils safe and effective internet and ICT use

This policy covers all users of our Trust ICT facilities, including Trustees, LAB members, staff, pupils, volunteers, contractors and visitors.

1.2 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
- Searching, screening and confiscation: advice for Trusts
- National Cyber Security Centre (NCSC): Cyber Security for Trusts
- Education and Training (Welfare of Children) Act 2021
- UKCIS guidance on sharing nudes and semi-nudes: advice for education settings working with children and young people
- Meeting digital and technology standards in Trusts and colleges
- DfE BYOD Guidance

- NCSC BYOD Guidance

1.3 Other Linked Policies

- Cyber Security Policy
- Social Media Guidance Policy
- Data Protection Policy
- Online Safety Policy

2. Policy Statement

This policy sets out the Trust's expectation of everyone using its equipment and/or internet access. Illegal or immoral use is not acceptable and will result in relevant disciplinary action.

Information and communications technology (ICT) is an integral part of the way The Park Academies Trust works, and is a critical resource for pupils, Trustees, LAB members, volunteers and visitors. It supports teaching and learning, and the pastoral and administrative functions of the whole Trust.

3. Provision of School Information and Communication Tools

The Trust provides you with information and communications technology to carry out your job duties or school work. This may include computers, landline phones, VoIP phones, mobile/smart phones, printers, photocopiers and any other means of storing, copying and transmitting data. As such, these tools are principally intended to be used for Trust/School purposes.

Trust-provided communication tools may also be used for *appropriate* personal activity during the working school day, provided that such activity does not interfere with job performance, consume significant resources, give rise to additional costs or interfere with the activities of your Staff colleagues or other Students. Excessive or inappropriate use of Trust communication tools may give rise to disciplinary action.

The Trust permits personal use of communication tools on the express understanding that it reserves the right (for Trust/School purposes or as may be required by law) to review the use of, and to inspect all material created by or stored on, these communication tools (See also the section on "Privacy" below).

The Trust provide Wifi connectivity for Staff and Students via TPAT Connect, this allows all Internet activity to be accountable to the individual on any device by means of logging in on a daily basis.

The timeout of this logon is 14 hours, to prevent misuse of systems, and ensure the correct device is logged against that individual.

Use of Trust-provided communication equipment constitutes acceptance of the Trust's right to monitor communications and access files that are made on or with that equipment.

4. Trust Property

Trust-provided communication equipment, as well as all data, files and messages produced, transmitted or stored using such equipment, are and remain the property of the Trust, and are subject to reasonable Trust inspection on request.

For Staff, and any other recipients of Trust owned equipment, such as Volunteers, Trustees or LAB Members, upon termination of your employment or role, you are responsible for returning all Trust provided communication tools that may be in your possession (laptop computers, mobile phones etc.), as well as all electronic data produced and stored on them, and for returning or destroying any duplicates or hard copies of such data.

For Students, any device provided to you by the Trust remains the property of the Trust, and must be returned when you leave your School, unless otherwise agreed.

You must look after Trust-provided equipment as if it were your own property. If equipment is lost, stolen or damaged due to your negligence or abuse, the Trust reserves the right to charge you an amount up to the cost price of replacement equipment. The amount of the charge, and a suitable method of repayment, will be determined at the time of the loss, based upon the circumstances.

If you fail to return any Trust-provided equipment upon termination of employment, leaving School, or if it is returned in a damaged condition, the Trust reserves the right to make an appropriate deduction from your final salary payment.

5. Passwords

You are responsible for your personal password security and for actions taken when your passwords are used. You should not reveal your passwords to anybody.

You should not leave your computer logged on and unattended; lock the screen if you are going to be away from your desk for any length of time, particularly if you are working with confidential or personal data.

Students should take care to make sure they logoff when they are finished using ICT resources.

All users of Trust systems must set and maintain the security and confidentiality of their own password. If at any time you believe your password to be compromised, you must inform a member of staff, your line manager, a member of School SLT or the Trust IT Support Team immediately.

Passwords must be a minimum of 8 characters, following the NCSC guidance on secure password setting, available here: https://www.ncsc.gov.uk/news/ncsc-lifts-lid-on-three-random-wordspassword-logic

Passwords must be changed at least once every 180 days (at least once per academic year), be a minimum of 8 characters, and employ the three random word guidance set by the NCSC. You should use within your passwords uppercase, lowercase, numbers, non-alpha numeric etc. in order to meet complexity requirements. It is best to use passwords that are not easily guess, such as your own name, date of birth etc. For example, HorseWindowDoor7!

Users will also be invited to sign up for 2FA (two factor authentication) for external access to email, using secondary information to secure their account.

6. Software

It is the Trust's express policy to pay for the software it uses. You must not load, use, store or transmit any unlicensed or unauthorised software or applications on any Trust-provided computer or mobile/smart phone, whether situated on Trust premises or off-site, under any circumstances.

If you believe that additional licences or software programs may be useful to the Trust, you should discuss this with your line manager or Trust IT Support.

7. Virus Protection

Virus protection software is installed on all Trust computers, it is automatically updated, you are responsible for ensuring it is allowed to regularly update. You must never take any action that would circumvent virus protection. Please be especially careful of

email attachments and executable programs imported from the Internet, which may contain viruses, Trojans, worms etc.

Simple steps can be taken when looking at e-mail, do you recognise the sender, hovering over a link, does the address look genuine? Were you expecting this e-mail? If there are any suspicions, refer to Trust IT Support.

Our anti-virus products will block the ability to download known viruses or malware, scans are routinely run across all devices, but please also be vigilant. If there is any doubt, please seek the assistance of Trust IT Support.

8. Use of Trust-Provided Equipment by Third Parties

You must not permit friends, relatives or other third parties who are not employed by or students of the Trust and its School's to use your Trust-provided equipment, nor must you knowingly permit colleagues to use your assigned equipment for inappropriate purposes.

Non-Trust personnel who may require access to Trust-provided communication tools for legitimate purposes (e.g. clients or contractors) must first be provided with a copy of this Policy, and sign a written agreement confirming that they will comply with its provisions.

9. BYOD / Use of Personal Devices

The Trust allows the use of personal devices where appropriate. Measures have been taken appropriately to comply with both DfE BYOD Guidance and NCSC BYOD Guidance.

The use of TPAT Connect for user personal devices allows individuals to authenticate on a daily basis as and when they may require access to the Trust network, this authentication allows the device to be traceable to the individual login, as per Trust user access, and as suggested by DfE and NCSC.

Under no circumstances should a personal device be used for taking or storing photographs/videos of students.

This access expires after 14 hours.

The Trust operate a modern Wifi system, compatible with the latest security standards, it should be noted however that this can mean that some devices may be unsupported.

User guidance on successful access using Android, iOS, MacOS and Windows is included on the landing screen when connecting to TPAT Connect.

10. **Remote Access**

We allow Staff and Students to access the Trust's ICT facilities and materials remotely. They should connect using the TPAT VPN, or Forticlient VPN for MacOS.

All staff laptops are preconfigured to allow access to the TPAT VPN, this will allow access to shared drives and file shares, via their encrypted devices. Non-Windows based devices may access a Forticlient VPN which will allow them access to a remote desktop environment.

For Staff devices, a BitLocker encryption key will be issued, this should not be stored with the laptop, and only used for accessing the device.

In order to minimise attempts to compromise Trust systems, secure VPN access is restricted to the United Kingdom only, as recommend by the NCSC and DfE.

When accessing the Trust's ICT facilities and materials remotely must abide by the same rules as those accessing the facilities and materials on site. You must be particularly vigilant if they use the Trust's ICT facilities outside the Trust on a personal device and take suitable precautions such as having appropriate and up to date anti-virus software.

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.

Please see Trust Data Protection Policy for further guidance.

11. **Privacy**

The Trust will not frivolously or maliciously invade your privacy. However, because Trust-provided communication tools are principally intended for business/School purposes, your rights to privacy in this context are limited, and you should not expect information created, transmitted or stored on Trust communication systems to remain private.

In addition to routine access for maintenance and upgrades, the Trust is entitled to review your electronic messages, files and data without prior notice, in various circumstances, including (but not limited to) the following:

- Investigating alleged misconduct or behaviour
- Investigating complaints that Trust resources are being used to transmit discriminatory or offensive messages or otherwise infringe upon or violate any other person's rights
- Discovering the presence of illegal material or unlicensed software
- Counteracting theft or espionage
- Responding to legal proceedings that call for the disclosure of electronically stored evidence
- Investigating indications of impropriety.

12. Confidential information

As Staff, in order to perform your job responsibilities, you are given access to confidential data that are vital to Trust operations. You must respect the confidentiality of such data.

Because of the highly public nature of the Internet and email, you must exercise particular care when accessing or transmitting information via those channels.

The use of portable storage tools such as memory sticks or external hard drives is blocked and prohibited. Removal of any Trust information for any reason without the express prior permission of your School Data Protection Lead or Data Protection Officer is prohibited.

13. File Storage and Archiving

You are encouraged to create folders to keep your files and email records tidy, to ensure efficient working on your part, and to facilitate the retrieval of information by your manager or Teachers, if you are not able work or attend School. You should review the files you store on Trust systems for relevance on a regular basis, and transfer anything that is no longer current to an archive folder. Remember that files containing work-related information are the property of the Trust and should be retained for future reference in the same way that paper files would be.

Even though you may delete messages from your own areas, they may remain on recipients' computers or on the Internet indefinitely, therefore you should never exchange or upload any content which you may later regret.

14. The Internet

The Trust provides Internet access for legitimate use. Often, it is the most efficient means of finding out information or communicating with others. However, this is not always the case, so consider whether there may be quicker and more effective ways to achieve your objectives. You should not spend excessive amounts of time browsing the Internet, even for work-related reasons.

Be aware of copyright issues when downloading or copying data from the Internet. Just because it is easy to copy material electronically, that does not mean it is legal to do so. Most information available on the Internet is protected by copyright in the same way as physical materials like books, CDs and DVDs are. Breaching copyright using Trust equipment could result in the Trust having to pay substantial damages to the copyright owners, and in you being disciplined or dismissed. Familiarise yourself with the copyright conditions of the information you are looking at before you download or copy it.

Some websites may contain inappropriate or offensive images or data, and the Trust reserves the right to log, monitor or block incoming and outgoing Internet traffic from those sites. If you inadvertently connect to sites that contain sexually explicit, racist, violent or other potentially offensive material, you must immediately disconnect and advise your manager, Teacher or Trust IT Support that these sites are accessible, so that blocking action may be taken. The ability to connect to them does not imply that the Trust condones the visiting of such sites.

You may use Trust equipment to access the Internet during the working/School hours for *appropriate* personal purposes, e.g. checking your bank account, news etc. However, you are not under any circumstances to use Trust equipment to access any inappropriate sites at any time; contravention of this rule will result in disciplinary action.

15. Email

Email is a tool provided by the Trust to facilitate the conduct of work duties and communicating with Staff/Students. Your email accounts must only be used for messages and attachments relating to this. The Trust reserves the right to inspect the contents of any emails sent or received by Staff or Students.

You must never send out any email or attachment that might show the Trust in an unprofessional light. Email must never be used to express racist, sexist, or otherwise

offensive opinions, either inside or outside the Trust. Inappropriate use of email will be investigated under the Trust disciplinary procedures.

Please be security conscious. Email is **not** private; messages can be intercepted or wrongly addressed, and are easily forwarded to third parties. Do not allow anyone else to use your email ID and password, or leave your email logged on and unattended so that others could interfere with it. You will be held responsible for any inappropriate email activity using your accounts. Similarly, you must not send out emails purporting to be somebody else, and you must not read other people's emails without their express permission. Please be careful when giving out your email address, for example, signing up to trials, mailing lists etc. so as to minimise the receipt of junk mail.

The Data Protection Act 2018 covers information stored on email as well as other media, so care must be taken if emails contain any "personal data", i.e. any information about a living identifiable individual, such as their name, home address, home phone number, personal email address etc. An obvious example would be the receipt, storage or transmission of candidates' CVs. Such data must not be collected without the person's knowledge, it must not be disclosed or amended except for the purpose for which it was collected, and it must be accurate and up to date. Particular care must be taken if the data is confidential or sensitive (e.g. contains information about medical conditions, political or religious beliefs etc.). The individual in question has the right to inspect what is held about him or her on the email system, to demand correction of inaccurate information, to request blocking or erasure of damaging information, and even to sue for damage caused by inaccurate information.

"Personal data" must not be kept for longer than is necessary, so emails should be stored in such a way that they can be easily identified, reviewed and archived when they are no longer needed. If in doubt, you should seek guidance from your School Data Protection Lead (DPL), or Trust Data Protection Officer (DPO).

16. Social Media

Social media and networking sites such as Facebook, Twitter, LinkedIn etc. may be accessed on Trust provided equipment during the working day for Trust business purposes only, by designated individuals. Any inappropriate use of social media during working hours may give rise to disciplinary action.

If your job role involves posting tweets or updates on Trust or School social media sites, then the followers and fans attracted to those sites are deemed to be followers and fans of the Trust or School, not yours personally. If you leave the Trust's employment, you must not continue to use the same account or give the impression you are still a Trust representative.

You are also reminded that any social networking activities you conduct on Trust equipment must be lawful and appropriate and not in any way defamatory, malicious or likely to damage the reputation of the Trust.

Furthermore, if you use social media at any time and in any context to make comments of a negative or inappropriate nature about the Trust, its School's, its employees, students, clients, customers, suppliers or other business associates, which might damage the Trust reputation or interests, the Trust reserves the right to investigate your actions through the disciplinary procedure.

Students are not permitted to use Social Media using Trust technology at any time, they should not attempt to communicate with Trust staff at any time using any form of Social Media.

For Staff, please see Trust Social Media Guidance for further guidance.

17. **Protection from Cyber Attacks**

Please see the glossary (Appendix 1) to help you understand cyber security terminology.

The Trust will:

- Work with Trustees, LAB Members and the Trust IT Support team to make sure cyber security is given the time and resources it needs to make the Trust secure
- Provide annual training for staff (and include this training in any induction for new starters, if they join outside of the Trust's annual training window) on the basics of cyber security
- 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 Trust will verify this using a third-party audit (such as independent penetration testing, to objectively test that what it has in place is effective
- **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 Trust needs to update its software

- **Regularly reviewed and tested**: to make sure the systems are as effective and secure as they can be
- Back up critical data daily, weekly, monthly and yearly.
- Delegate specific responsibility for maintaining the security of our management information system (MIS) to data manager / business managers within schools, and the Director of IT
- Have firewalls in place, that are actively monitored
- Check that its supply chain is secure, for example by asking suppliers about how secure their business practices are and checking if they have the Cyber Essentials certification.
- Develop, review and test an incident response plan with Trust IT Support including, for example, how the Trust will communicate with everyone if communications go down, who will be contacted and when, and who will notify Action Fraud of the incident. This plan will be reviewed and tested annually. and after a significant event has occurred, using the NCSC's 'Exercise in a Box'.

Make sure users:

- Connect to our network using a virtual private network (VPN) when working from home
- Enable multi-factor authentication where possible
- Connect to TPAT Connect Wifi using account authentication so that device access is auditable

18. Telephones and Voicemail

Telephones should be answered in a friendly but professional manner, and as promptly as possible. With permission, Trust landlines may be used for reasonable personal use, but please bear in mind that Trust telephones are principally provided for business purposes, and excessive personal use may be grounds for disciplinary action. Under no circumstances should premium rate numbers be called, at any time.

When leaving voicemail messages, you should follow the same rules of professionalism that guide the use of e-mail.

19. Misrepresentation or Misuse of Technology

When using any Trust-provided communication tool, you represent the Trust. Email or Internet messages can be traced back to the Trust as their source. Therefore, you must exercise caution to protect the reputation and interests of the Trust.

Electronic forgery (misrepresenting your identity in any way while using electronic communication systems) is not allowed for any reason. You may not take any action to misrepresent the identity of the person responsible for a message. If you forward a message prepared by someone else, it should be sent "as is", or if changes are necessary, you must clearly indicate where the original message was edited e.g. by using brackets, asterisks, or other characters to flag edited text.

You must also recognise the other side of this issue, namely that others can misrepresent themselves. Therefore, you should be wary of electronic communication from unknown people.

Misuse of communication tools may interfere with business operations and may injure the Trust or other employees. As a general rule, you should not create or send any message, using any technological medium, that you would not want an outside party to view. Ask yourself whether you would be happy to see this on the front page of the local newspaper, and if the answer is no, then the message is probably not appropriate.

Examples of unacceptable use of technology include (this list is not exhaustive):

- Sexually explicit messages, images, cartoons or jokes
- Unwelcome propositions, requests for dates or love letters
- Profanity, obscenity, slander or libel
- Expressions of political beliefs
- Derogatory, defamatory, threatening, abusive, rude or offensive language
- Any message that could be construed as harassment or disparagement of others based on sex, race, sexual orientation, age, national origin, disability, or religious or political beliefs
- Commercial or for-profit activities unrelated to Trust operations
- Chain letters
- Excessive use of the technology for personal purposes
- Release of confidential, sensitive or proprietary information
- Any action that is illegal or harmful to the Trust or any School.

Misuse of Trust-provided technological tools, or any other failure to comply with this policy will be investigated through the Trust disciplinary procedure.

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 Trust 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.
Phishing	Untargeted, mass emails sent to many people asking for sensitive information (such as bank details) or encouraging them to visit a fake website.

TERM	DEFINITION
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/multifactor 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.