

Document Title	Acceptable Use of ICT
Author/Owner (Name and Title)	ICT Support
Version Number	V2
Date Approved	26 August 2026
Approved By	Chief Executive Officer

Policy Category (Please Indicate)	1	Trust/Academies to use without amendment
	2	Academy specific appendices
	3	Academy personalisation required (in highlighted fields)

Summary of Changes from Previous Version

Version	Date	Author	Note/Summary of Revisions
V1	July 2026	Exec	New Policy
V2	Sept 2026	Exec	Updated Legislation

TABLE OF CONTENTS

1. Statement of Intent.....	3
2. Scope	3
3. Legal Framework	3
4. Roles and Responsibilities	4
5. Acceptable Use Agreement (AUA)	5
6. Acceptable Use	5
7. Unacceptable Use.....	5
8. Safeguarding and Online Safety	6
9. Monitoring and Privacy	6
10. Account Security	7
11. Data Protection and Information Handling	7
12. Communication and Professional Conduct	7
13. Use of Devices and Systems	8
14. Remote and Off-Site Working.....	8
15. Artificial Intelligence (AI) Use	8
16. Social Media and Online Activity.....	8
17. Safe Use of Images	9
18. Copyright and Intellectual Property	9
19. Breaches and Sanctions	9
20. Policy Compliance and Review.....	9

1. STATEMENT OF INTENT

Place Partnership (the Trust) promotes the safe, secure and effective use of ICT to support education, safeguarding, and business operations.

All users of Trust ICT systems must act responsibly, professionally and in line with Trust policies. ICT systems are a critical part of safeguarding and are therefore subject to monitoring, control and review.

This policy sets out the rules governing the use of ICT systems.

The Trust's approach to online safety, safeguarding risks, filtering, monitoring governance, and incident response is defined in the Online Safety Policy and Safeguarding Policy. All users must be familiar with these policies.

2. SCOPE

This policy applies to all users of Trust ICT systems, including:

- Staff
- Pupils
- Governors
- Contractors, visitors and third parties

It covers all Trust ICT resources including:

- Trust provided devices (such as, but not limited to, laptops, desktops, tablets, phones, reprographics equipment)
- Systems and software (Microsoft 365, MIS, cloud services)
- Network access (Wi-Fi, internet, remote access)
- Communications (email, Teams, telephony)
- Data and information storage

This policy applies both on and off Trust sites where Trust provided systems are accessed.

3. LEGAL FRAMEWORK

This policy operates within the following statutory, regulatory and organisational framework.

LEGISLATION

This policy should be read in conjunction with relevant UK legislation and statutory guidance.

The following list is not exhaustive but highlights key frameworks governing the safe and lawful use of ICT:

- Keeping Children Safe in Education (KCSIE) – September 2026
- Malicious Communications Act 1988
- Computer Misuse Act 1990

- Copyright, Designs and Patents Act 1988
- Regulation of Investigatory Powers Act 2000 (RIPA)
- Prevent Duty (Counter-Terrorism and Security Act 2015)
- Online Safety Act 2023 (UK)

LINKED DOCUMENTS

This policy will be implemented in accordance with the following Trust policies and procedures:

- Data Protection Policy
- Online Safety Policy
- Behaviour & Equivalent (Pupil)
- Safeguarding Policy
- Staff Code of Conduct
- Use of Artificial Intelligence Policy

Technical security controls and cyber risk management are defined within:

- Cyber Security Policy

All Trust policies are available by request from ICT Support.

4. ROLES AND RESPONSIBILITIES

ALL USERS

All Users must:

- Read, understand and comply with this policy
- Use ICT systems responsibly and professionally
- Protect their account credentials and data
- Report any concerns, incidents or breaches

STUDENT

In addition, pupils must:

- Understand the importance of adopting good online safety practice when using digital technologies.

STAFF

In addition, staff must:

- Model the appropriate use of ICT
- Support pupils to use technology safely
- Follow safeguarding reporting processes

DESIGNATED SAFEGUARDING LEAD (DSL)

- Has oversight of online safety and monitoring alerts (via E Safety Policy)
- Ensures safeguarding concerns identified through ICT systems are actioned in line with Trust safeguarding procedures

ICT SUPPORT

- Implement and maintain technical controls to ensure the safe and secure use of ICT systems
- Manage filtering and monitoring systems in line with safeguarding requirements
- Ensure systems are configured to protect users from inappropriate or harmful content
- Maintain appropriate security controls including access management, patching, anti-malware and network protection
- Investigate potential breaches, incidents or misuse of ICT systems
- Work with the Designated Safeguarding Lead (DSL) to ensure that monitoring and alerting systems are effective
- Support the review and continuous improvement of ICT safety and security arrangements

5. ACCEPTABLE USE AGREEMENT (AUA)

When logging on to a Trust system, users must signify their acceptance of this policy before proceeding: *"By signing on to this device, you agree to follow Place Partnership's ICT Acceptable Use Policy and End User Agreements"*

Age-appropriate end user agreements for pupils are displayed through academies and promoted with pupils where possible.

6. ACCEPTABLE USE

ICT systems provided by Place Partnership must only be used by authorised users for:

- Educational purposes
- Trust business operations
- Approved professional activities

All use must be lawful, appropriate, and consistent with professional standards.

7. UNACCEPTABLE USE

The following activities are not permitted:

SECURITY AND SYSTEM MISUSE

- Attempting to bypass security controls, filtering or monitoring
- Accessing systems or data without authorisation
- Using another person's account or sharing credentials
- Introducing malware or unauthorised software

- Conducting scanning, hacking, or testing activities

INAPPROPRIATE OR ILLEGAL ACTIVITY

- Accessing, creating or sharing inappropriate, offensive or illegal content
- Engaging in bullying, harassment, or discriminatory behaviour
- Bringing the Trust into disrepute

MISUSE OF RESOURCES

- Using Trust systems for personal activity
- Signing up to software services without approval from ICT Support
- Physically damaging the ICT facilities

This list is not exhaustive. Any activity deemed inappropriate or unsafe may be treated as a breach.

8. SAFEGUARDING AND ONLINE SAFETY

ICT systems form part of the Trust's safeguarding arrangements.

- Use of ICT systems may generate safeguarding alerts, which are reviewed by safeguarding staff.
- All concerns, including low-level concerns, must be reported in line with the Online Safety and Safeguarding policies.
- Users must not attempt to conceal activity or bypass safeguards.

9. MONITORING AND PRIVACY

All use of Trust ICT systems is monitored and logged.

Monitoring is undertaken to:

- Protect users
- Safeguard children
- Maintain system security

Access to staff accounts by ICT Support is with approval from the account holder. However, if there is a requirement to investigate breach of this policy or, in the event of prolonged staff absence, the Chief Executive Officer (CEO), Academy Principal or Executive leader can provide the necessary authorisation for line managers to access accounts.

In extreme circumstances, should there be an immediate requirement to protect the network, ICT Support reserve the right to:

- View any/all contents of file storage areas.
- View/access transactions across the network.
- View e-mails sent and perform message traces.
- Remove access to ICT services.

Users should have no expectation of privacy when using Trust systems.

10. ACCOUNT SECURITY

Users must:

- Keep passwords secure and confidential
- Not share accounts or credentials
- Use strong passwords in line with Trust requirements
- Lock devices when unattended

Privileged accounts:

- Must only be used for authorised tasks

11. DATA PROTECTION AND INFORMATION HANDLING

Users must:

- Handle all information in line with Data Protection (GDPR) requirements (refer to the Trust's Data Protection Policy)
- Only access data necessary for their role
- Use approved systems (e.g. OneDrive, SharePoint) for storage and sharing
- Ensure data shared externally is secure and authorised

Personal or sensitive information must not be:

- Stored on personal devices (unless authorised)
- Shared via unapproved platforms

12. COMMUNICATION AND PROFESSIONAL CONDUCT

All communication using Trust systems must be:

- Professional and appropriate
- Respectful and lawful

Users must:

- Use approved communication platforms only
- Not engage in harassment, bullying or inappropriate messaging

Staff must:

- Maintain clear professional boundaries
- Not communicate with staff, pupils or parents/carers through personal accounts or social media channels.

13. USE OF DEVICES AND SYSTEMS

Trust Devices:

- Must not be modified or reconfigured or relocated without ICT approval
- Must only use approved software and services
- That may leave site and contain sensitive data must be managed by Office 365 Endpoint Manager and have policies enforced to ensure the protection of such data. This will include; patch management, anti-virus, access restrictions and device encryption.

Personal Devices (BYOD):

- May only access Trust systems via approved methods
- Must not store Trust data locally unless authorised

Portable Media:

- Use of USB and external storage is strictly restricted

14. REMOTE AND OFF-SITE WORKING

When accessing Trust systems remotely, users must:

- Ensure devices are secure and updated
- Avoid accessing sensitive information in public or unsecured environments
- Protect physical documents and equipment

All policy requirements apply regardless of location.

15. ARTIFICIAL INTELLIGENCE (AI) USE

The use of AI tools must be safe, responsible, and approved.

Users must not:

- Enter personal, sensitive or safeguarding data into AI tools
- Use AI in a way that breaches data protection or academic integrity.

All use of AI must comply with Trust guidance and policies. (Refer to the Trust's policy on the use of AI).

16. SOCIAL MEDIA AND ONLINE ACTIVITY

Users must not:

- Use personal social media to communicate Trust business
- Post content that could damage the Trust's reputation

Professional standards apply to online activity both inside and outside work.

17. SAFE USE OF IMAGES

The Trust understands that recording images of identifiable individuals constitutes as processing personal data and as such it is done in line with data protection principles.

- Student and staff photographs are held electronically in management information systems for identification purposes. These images are not to be used for other purposes unless consent is obtained.
- Parents/carers may provide consent for the use of student's images for use in display and promotional work, including online content such as website and social media channels. This consent must be specifically implied and recorded electronically in management information systems. It can be removed at any time.
- Staff are allowed to use personal device to take image of pupils for business use under the following conditions:
 - Any image taken on a personal device, should only be from within a Trust approved app and saved directly to that app to be uploaded to the cloud when connectivity allowed.
 - Images should never be saved to personal camera roles or applications not authorised by the Trust.
 - Personal social media should never be used for the transfer of student images.

Further guidance is available from ICT Support on request.

18. COPYRIGHT AND INTELLECTUAL PROPERTY

Users must:

- Comply with copyright laws
- Only use licensed or permitted materials
- Acknowledge sources appropriately

Content created using Trust systems remains the property of the Trust.

19. BREACHES AND SANCTIONS

Failure to comply with this policy may result in:

- Removal of ICT access
- Disciplinary action
- Safeguarding investigation (where applicable)
- Legal action where laws are broken

Serious breaches may be treated as gross misconduct.

20. POLICY COMPLIANCE AND REVIEW

- All users must confirm acceptance of this policy (via Acceptable Use Agreements)
- The policy will be reviewed regularly in line with legal and technological changes

- Compliance will be monitored and enforced

APPENDIX 1 – ICT ACCEPTABLE USE AGREEMENT FOR STAFF, TRUSTEES, GOVERNORS AND VISITORS.

This agreement is designed to ensure that all staff, Trustees, Governors and visitors are aware of their responsibilities when using any Trust ICT systems. All staff, Trustees, Governors and visitors are expected to sign this agreement and adhere to its contents at all times.

- I will only use Trust ICT facilities and any related technologies for Trust approved business.
- I will comply with all ICT security measures and not disclose any passwords provided to me by the Trust or other related authorities. I understand that I am responsible for the security of my account.
- I understand that I must not allow pupils to use my computer login/password.
- I will not install or make changes to any hardware or software without prior permission from ICT Support.
- I understand that my use of the Internet and other related technologies is monitored and logged, and these logs can be made available on request to the Trust CEO.
- I will not attempt to bypass filtered Internet connections while working on Trust sites, using for example personal hotspots on mobile devices.
- I will not browse, download, upload or distribute any material that could be considered offensive, illegal or discriminatory.
- I understand that for any Trust employee, the publication or the electronic transference of any material that could be regarded as derogatory, relating to the Academy, its operations or stakeholders, is a disciplinary offence.
- I will only download files from trusted sources.
- I will only use approved communication systems for any Trust related business.
- I will ensure that all electronic communications with pupils and staff are compatible with my professional role.
- I understand that all reasonable precautions must be taken to avoid malware infection of Trust systems. Although phishing protection software is in place, I will still be vigilante and report any suspicious emails to ICT Support.
- I will support and promote the Trust's Online Safety Policy and help children and young people and adults to be safe and responsible in their use of ICT and related technologies.
- I will not give out my own personal details, such as a mobile phone number and personal email address, to pupils.
- I will respect copyright and intellectual property rights.
- I understand that data protection is a significant public issue, and I am familiar with the General Data Protection Regulation (GDPR).
- I will ensure that any personal data is kept secure and used appropriately, whether on site or accessed remotely. I understand that personal data should only be accessed remotely when authorised by the Trust.
- I will ensure that images of pupils and/or staff are only taken, stored and used for professional purposes in line with the Trust policy.
- I will ensure that my on-line activity, both within Trust and externally, will not bring my professional role into disrepute.

The Trust has a means to log network activity and may use these logs as evidence of misuse of the facility, or breach of the above conditions of use.

APPENDIX 2 – ICT ACCEPTABLE USE AGREEMENT FOR PUPILS – SECONDARY

Pupils must read and follow the conditions set out in this agreement when using ICT. If you need help or are unsure about anything written below, please ask a member of staff or refer to the main policy which supports this agreement. Any breach of the conditions below may lead to withdrawal of your access to ICT and the network.

PASSWORDS AND SECURITY

- I will only use my own ID and password to log onto a computer.
- I will not give out my password to anyone. If I suspect anyone knows my password, I will ask for it to be changed.
- I will log off properly after I have finished with the computer.
- I will not access any other user's files and folders without permission.

ONLINE

- I will only use the Academy's internet for school related work and educational purposes. I will not browse or download anything illegal.
- I will not create or share any material that is derogatory, may cause upset to others, or bring the Academy name into disrepute. If I do come across any such material, I will report it immediately to a member of staff.
- I understand why the Academy/Trust filters Internet content and I will not attempt to bypass the Internet filtering system.
- I will not attempt to access any social networking sites or chatrooms in school except those systems which are operated by, or for, the Academy/Trust for educational purposes.
- I will not attempt to buy goods or services via the Internet.

COMMUNICATION

I will only use the Academy's approved communication systems for schoolwork.

- I will not use abusive or threatening language in an e-mail or chat.
- If I am unsure about opening or downloading the contents of an e-mail, I will ask a member of staff.

IMAGES

- I will only take, store, and use images of pupils and/or staff for agreed Academy/Trust projects or purposes.
- I will not use or re-distribute images or video of others without their explicit permission.
- I will be mindful of any image I post online or send via social media, knowing that once sent they can be difficult if not impossible to retrieve.

SAFETY

I will not perform any actions which may compromise the stability or security of ICT services in the Academy/Trust.

- I will not disclose my personal details or share the personal details or images of others.
- I understand that people I may talk to online may not be who they say they are. I will not meet with anyone whom I contact via the Internet without obtaining permission from a parent/carer, or teacher.
- I know that all use of the network in the Academy/Trust is monitored, and many websites keep permanent records of any content I create or share.
- I will abide by copyright laws and will not plagiarise material from the Internet.

RESPECT

I will only communicate with others politely and sensibly.

- I will treat other people and ICT equipment with care and respect.
- I will not attempt to move, tamper with, or modify school PCs including disconnecting any cables.
- I will not take food or drink near to any computer.
- I will contact the ICT Support Team if I suspect that any equipment is faulty.
- I will not print anything in school other than schoolwork and I will print responsibly.

It is my responsibility to respect and follow all the above conditions which will help to keep me and others safe while using ICT.

APPENDIX 3 – ICT ACCEPTABLE USE AGREEMENT FOR PUPILS – KS2

RESPECT

When using ICT, I respect myself, others, and the equipment I use.

This means I:

- Always ask permission before using ICT.
- Ask if I need help.
- Am careful with the equipment I use.
- Will tell an adult if something in school doesn't work properly.

ONLINE

I will always ask permission before using the Internet.

I know that when I go online I will:

- Never deliberately search for something rude or violent.
- Always tell an adult if I see anything that makes me or my friends uncomfortable.
- Not believe everything I read on the Internet.
- Never open or download a file unless I know it is safe. If I'm not sure, I should ask an adult first.
- Respect copyright when using content from the Internet.

COMMUNICATION

When I communicate online using e-mail or social media, I communicate safely by:

- Always thinking and checking that what I write or post is kind, polite and respectful.
- Being kind to my friends and classmates and thinking about how the things I do or say online might make them feel.
- Not sending mean or bullying messages or forwarding them to other people.
- Speaking to an adult if someone is unkind to me or if I know someone else is upset or scared.
- Never talking to anyone I don't know.
- Telling an adult if someone asks to meet up with me in real life.

PROTECT

I protect myself and others by being aware that my full name, photo, birthday, address and phone number is personal information and is not to be shared online.

This means I:

- Stop to think about what I post or share online.
- Protect my friends' information in the same way.
- Protect my passwords and don't share them with anyone except my parent.
- Never answer questions online that ask for my personal information.

AT SCHOOL WE/I HAVE:

- Discussed ways to be a safe, responsible, and ethical user of ICT at school, home and everywhere.
- Presented my ideas around the ways that I can be a smart, safe, responsible, and ethical user of ICT.

APPENDIX 4 – ICT ACCEPTABLE USE AGREEMENT FOR PUPILS – KS1, EYFS

KEY STAGE 1

- I will ask a teacher or adult if I want to use the computers or tablets.
- I will only use activities that an adult has allowed me to use.
- I will take care of computers, tablets, and any other ICT equipment.
- I will ask for help from an adult if I am not sure what to do or if I think I have done something wrong.
- I will tell an adult if I see something on screen that upsets me.
- I know that if I break the rules, I might not be allowed to use a computer or tablet.

APPENDIX 5 – DOMAIN DEVICE LOGON MESSAGE

'By signing on to this device, you agree to follow Place Partnership Trust's Safe Use of ICT Policy and end user agreements.'