WeST Acceptable Use Policy and Agreement

Person(s) responsible for updating the policy:	Pete Spreadborough, Head of Projects
Policy type:	Trust Wide
Approval level:	Executive Leadership Team
Date approved:	04/03/2026
Date of next review:	04/03/2028
Review frequency:	Biennial
Published on:	West Staff Website
Version History:	See final page

WeST Vision, Mission and Values:

https://www.weststt.org.uk/vision-mission-values

ICT Acceptable Use – One Page Summary

The Acceptable Use Policy sets out the minimum rules and expectations for using WeST ICT resources safely and responsibly. All staff, governors, volunteers and contractors given access to WeST ICT must agree to the Acceptable Use Policy. This Policy does not replace the full WeST ICT Security Policy Suite, Data Protection and Information Governance Policy Suite, and their associated policies including the WeST Safeguarding and Online Safety Policies.

All staff are expected to:

- have read and understood the Acceptable Use Policy and understand that it forms part of the wider WeST ICT Security Policy Suite.
- agree to comply with all applicable WeST ICT, Safeguarding, Data Protection and Information Security Policies.
- contact the relevant team if unsure about any aspect of acceptable use, or if they wish to raise any concern, in accordance with the "Reporting ICT Security, Safeguarding and Data Protection Concerns" section of the ICT Security Policy.

All users of WeST ICT equipment and systems must:

- immediately report any concern relating to pupil safety to the Safeguarding team
- immediately report any suspected compromise of account credentials to WeST Digital
- immediately report any breach, misuse, or suspected security issues to WeST Digital
- not enter Confidential, Highly Confidential or pupil data into public or consumer AI
- not share my account credentials except where authorised ICT support requires
- not store Trust or School data on personal devices or personal cloud accounts
- not attempt to bypass or tamper with any security, filtering or monitoring controls
- not use consumer messaging platforms for Trust or School business
- use a unique password for every system and will use MFA where required
- only use Trust-approved systems for storing and sharing Trust information
- follow Trust security requirements when working remotely or from home

Staff must also be aware that:

- use of WeST ICT resources is subject to monitoring
- failure to comply with WeST ICT Policies may result in disciplinary action, up to and including summary dismissal for gross misconduct
- where a criminal offence is suspected, information may be shared with the police or other relevant authorities

Contents

1. Introduction

This policy forms part of the WeST ICT Security Policy Suite and should be read in conjunction with the overarching WeST ICT Security Policy.

For the purposes of this agreement, all School and Trust devices, networks and accounts (including Microsoft and Google accounts, and any other external or third-party work-related systems or services) are collectively referred to as "WeST ICT resources".

Westcountry Schools Trust (WeST) relies on technology to deliver education securely, efficiently and safely. This Acceptable Use Policy explains the responsibilities of all staff, governors, volunteers and contractors when using WeST devices, systems and data. It supports our obligations under safeguarding legislation, the Data Protection Act 2018 and UK GDPR.

By following this policy, users help protect pupils, colleagues, systems and information, and support the Trust's compliance with national cyber-security and information-governance standards.

Concerns must be reported in accordance with the "Reporting ICT Security, Safeguarding and Data Protection Concerns" section of the ICT Security Policy.

2. Purpose and Scope

2.1. Purpose

The purpose of this Acceptable Use Policy is to set out clear, practical rules for using WeST ICT resources, devices, accounts and data safely and responsibly. It aims to:

- protect pupils, staff and Trust information from harm, loss, misuse or unauthorised access
- support professional, ethical and lawful use of technology by all users
- reduce cyber-security risks and promote secure behaviours in line with NCSC guidance, ISO 27001 controls and UK GDPR/Data Protection Act 2018 requirements
- help all schools within WeST meet the DfE Meeting digital and technology standards in schools and colleges

This policy applies to all staff, governors, volunteers, contractors and any other user with access to WeST ICT resources. For clarity and ease of use, this policy highlights the critical rules that everyone must follow. More detailed technical and procedural controls are contained in the WeST ICT Security Policy and related documents.

2.2. Scope

This policy covers the use of:

- WeST and School-owned ICT devices, networks and systems
- Cloud-based systems provided by WeST (e.g., Microsoft 365)
- Personal devices used to access WeST systems (Bring Your Own Device, BYOD)
- Trust and School email
- Internet access via Trust and School networks

- Digital photos, video and media

This policy should be read alongside, not instead of, the wider ICT Security Policy Suite. Where a rule is critical, it is repeated here for clarity.

3. Roles, Responsibilities and Governance

3.1. Roles and Responsibilities

Roles, responsibilities, and accountabilities relating to this policy are defined in the WeST ICT Security Policy.

Where this policy introduces policy-specific responsibilities, these apply in addition to, and do not replace, the overarching roles and responsibilities set out in the WeST ICT Security Policy.

All individuals must comply with the responsibilities applicable to their role and must report suspected or actual issues, incidents, or non-compliance in accordance with Trust policies and procedures.

3.2. Governance

Governance and oversight of this policy are defined in the WeST ICT Security Policy and the Trust's governance procedures.

This includes the Trust's arrangements for:

- executive oversight and escalation
- assurance, audit, and independent scrutiny
- risk management and reporting to the Audit and Risk Committee

Compliance with this policy, and the effectiveness of the controls it establishes, are monitored through those established governance and assurance mechanisms.

4. Using WeST ICT resources

4.1. Ownership and access

- All ICT equipment and systems are owned by WeST or the School
- Users must only access systems and data they are authorised to use
- Access to data and systems is provided as appropriate to a person's role and is reviewed on a regular basis
- ICT teams may access, maintain, update or reallocate equipment at any time
- ICT equipment may be removed for maintenance, reallocation or operational reasons without prior notice

Maintenance includes, but is not limited to, software installation, updates, reconfiguration of settings and computer re-imaging. ICT teams will make every effort to minimise disruption, however, safeguarding or cyber-security requirements may take priority over operational needs.

4.2. Software, extensions and filters

- Only ICT teams may install software or browser extensions

- Users must not attempt to download or install software without permission
- Users must not attempt to bypass monitoring or filtering measures

Users must not alter any system, browser or network settings that relate to security, filtering, updates, device management or connectivity. Personal settings that do not affect system security (for example display, accessibility or audio settings) may be adjusted as needed.

4.3. Connecting equipment

- Users must not plug personal equipment (USB sticks, peripherals or smart devices) into WeST ICT resources unless authorised by ICT
- Users may only connect personal devices (phones, laptops, tablets) to approved WeST or School Guest WiFi networks, and must not connect them to internal WeST device networks or ethernet ports
- Users must not use the USB ports of Trust or School ICT systems to charge smart devices; a wall socket and appropriate charger must be used to prevent accidental data transfer or security risk

5. Accounts, Passwords and Authentication

5.1. Password Complexity

Passwords must be sufficiently complex to prevent easy guessing and automated 'brute-force' or dictionary attacks.

Where available, users should use secure password generation tools, such as Microsoft Edge's built-in password generator (right-click in a password field and select "Suggest strong password").

Where users create their own passwords, the recommended approach is the 'three random words' technique, combining three unrelated words (for example, CoffeeTrainFish). Where systems require numbers or symbols, these may be used as separators (for example, Coffee&Train6Fish).

5.2. Password uniqueness

The most significant password-related security risk is the reuse of the same password across multiple systems. A data breach in any single service immediately compromises the security of every account using that same password.

Passwords must:

- be unique to each system and account
- never be reused across different services
- never be shared between home and work accounts

5.3. Password storage

If users sign-in to Microsoft Edge using their School or WeST account, its Password Manager provides a secure method of storing passwords. This enables the use of unique passwords for

every system and reduces the risk of phishing attacks by only auto-filling credentials on the correct websites.

Passwords must:

- be committed to memory where practical (particularly your main work account password)
- be stored securely using an approved password manager
- not be written down

5.4. Multi-Factor Authentication (MFA)

Multi-factor authentication (MFA) provides significantly stronger protection than passwords alone by requiring two or more verification steps. For example, after entering a password, a system may require a one-time code sent to a trusted device.

This means that even if a password is compromised, an account cannot be accessed without possession of the trusted authentication device.

The following requirements apply:

- MFA is mandatory for all systems that support it
- MFA devices must be kept secure at all times
- loss or theft of an MFA device must be reported immediately to WeST ICT

5.5. Account security and responsibility

Users must remain vigilant for phishing and social engineering attacks. Suspicious emails, messages, links, or requests for information must be reported to WeST ICT immediately.

Users must report any suspected malware, unusual system behaviour, or security warning messages to WeST ICT immediately.

Users are responsible for all activity carried out using their accounts.

The following requirements apply:

- devices must be locked or logged out when unattended
- pupils must never be permitted to use a staff account
- staff must not share their account credentials with anyone
- staff may only access another staff member's account under direct supervision of the account owner and without being provided with their password
- staff must immediately report any suspected compromise of account credentials for any system to WeST ICT

An exception to password sharing is permitted only where authorised ICT support requires access for technical troubleshooting. In such cases, passwords must only be provided directly to WeST ICT staff and must be changed immediately after support has been completed.

6. Network Access and Security

Access to Trust and School internal ICT systems and networks is permitted only to registered users with an authorised account. Each user account is issued for the exclusive use of the individual to whom it is assigned.

WeST data is stored primarily on centrally managed platforms including Shared Network Drives, Microsoft SharePoint, Microsoft Teams, and individual OneDrives. In general:

- OneDrive should be used for personal work data (e.g. payslips, personal HR notes)
- specific systems designated for data types must be used as designated (e.g. CPOMS for safeguarding information, MIS for single central record of pupil data, etc.)
- Microsoft Teams and SharePoint must be used for all usual business and team data where a designated specific system does not exist
- shared network drives should only be used where a Team or SharePoint site does not exist

Users must:

- only access systems and data for which they have been explicitly authorised
- only use Trust-approved platforms for the storage and sharing of Trust data and must not create unmanaged data stores outside these platforms
- ensure files and files are assigned appropriate access controls and permissions
- report any system, folder, or resource that appears to permit access more widely than intended
- report any suspected weakness in access controls or data protection immediately to WeST ICT

Trust data must only be stored, processed, or shared using Trust-approved cloud platforms (such as Microsoft 365, MHR). The use of unauthorised cloud services is not permitted.

Any new third-party system or cloud service must be approved by WeST ICT and may be subject to a Data Protection Impact Assessment (DPIA).

All Trust networks are protected by centrally managed firewall, boundary and security monitoring controls. Users must not attempt to bypass or interfere with these protections.

Users must not make any physical or logical alteration to Trust or School ICT or network equipment unless authorised by WeST ICT Management. Users must not attempt to probe, scan, test, or exploit Trust systems or networks.

Any activity that threatens the confidentiality, integrity, or availability of Trust or School ICT systems or data is prohibited. This includes attempts to interfere with, disrupt, misuse, or compromise internal systems, networks, or other users' access.

7. Internet Access

Internet access is provided primarily for educational and professional purposes. Limited personal use is permitted where it does not interfere with Trust or School operations and complies fully with this policy.

Personal internet use must:

- take place during recognised break times or outside working hours
- not interfere with network performance or availability
- comply with professional conduct standards
- avoid accessing unlawful, inappropriate, or offensive material

All internet access is subject to filtering and monitoring. While filtering reduces access to inappropriate content, it may not block all unsuitable websites. Any inappropriate or concerning content encountered must be reported immediately to WeST ICT

The following activities are prohibited and may constitute misconduct or gross misconduct:

- accessing, creating, transmitting, or storing unlawful or inappropriate material
- transmitting defamatory, discriminatory, offensive, or harassing content
- disclosing confidential or personal Trust or School information without authorisation
- breaching copyright or licensing requirements
- using Trust systems for gambling, chain messages, or unauthorised messaging services
- accessing or distributing material that could present a safeguarding risk

Misuse of internet access may result in disciplinary action and, where appropriate, referral to external authorities.

8. Messaging Apps and Email

Trust or School business must not be conducted using consumer messaging platforms such as WhatsApp, SMS, Facebook Messenger, Signal, or any similar service.

Trust and School email accounts must be used for all official Trust and School communications wherever possible.

Personal email accounts may be accessed on Trust devices only during recognised break times and must not be used to conduct Trust or School business, communicate with parents, or transfer Trust information.

Email use must comply with the following requirements:

- language must be professional and appropriate
- unlawful, offensive, or inappropriate content must not be sent or stored
- copyright material must not be distributed without permission
- chain emails and spam must not be forwarded
- highly confidential information must only be sent using secure methods (encryption, secure portals, or password-protected documents with passwords sent separately)
- children's full names should not be included in subject lines and should be avoided in email content where possible

Trust and School email systems are managed in accordance with data protection legislation. Users must report any offensive or concerning communications immediately.

9. Use of Artificial Intelligence (AI) Tools

Artificial intelligence (AI) tools and services (such as Microsoft Copilot, ChatGPT, Google Gemini, image generators, transcription tools, and similar systems) can provide educational and productivity benefits. However, their use also presents data protection, safeguarding, and intellectual property risks.

WeST's default AI Tool is Microsoft Copilot, which is covered by an Enterprise privacy agreement if the user is logged-in using their WeST account.

The following requirements apply:

- AI Tools must only be used in accordance with the WeST AI Policy
- Trust or School Internal data, Confidential, or Highly Confidential information, must not be entered into public or consumer AI Tools
- Pupils' data must never be uploaded, processed, or analysed using public AI Tools
- Staff must not use AI Tools to generate or process safeguarding, child protection, or disciplinary records
- AI Tools must not be used to create or manipulate images, audio, or video of pupils or staff
- Any use of AI for assessment, feedback, or content generation must comply with Trust academic integrity policies

Users must:

- understand that most AI Tools retain, reuse, or train on submitted content
- verify the accuracy of AI-generated content before relying on it
- ensure AI-generated material is used ethically, transparently, and lawfully

Any proposed use of AI Tools for Trust business, teaching, or administration must be approved by WeST ICT and may be subject to a Data Protection Impact Assessment (DPIA).

Misuse of AI systems may result in disciplinary action.

10. Use of Personal Devices

Staff may access Trust or School systems using personal devices at their own discretion, provided the device meets security requirements.

Personal devices used to access Trust or School systems must:

- be secured with a password, PIN, or biometric control
- use a manufacturer supported operating system receiving security updates
- have all security updates applied automatically and promptly
- have appropriate malware protection
- have any insecure features disabled

Trust or School data must not be stored on personal devices or personal cloud services.

Staff may only use their personal devices to access School or Trust systems if they understand how to perform software updates

and apply appropriate security controls. Choosing to use a personal device for work purposes means accepting full responsibility for ensuring that device's security and suitability.

Use of personal devices is voluntary, except where required for multi-factor authentication. MFA use does not grant the Trust access to the personal device.

WeST ICT teams do not provide support for personal devices, except for guidance relating to required MFA systems.

When working remotely, staff must ensure:

- home Wi-Fi networks are secured with a password
- Trust systems are not accessed from shared or public computers
- screens and documents are protected from being overlooked
- Trust data is not printed or stored at home

11. Recording Devices and Image Capture

The Trust and its Schools support the appropriate use of digital media for educational and professional purposes. However, the use of any device capable of recording images, audio, or video presents safeguarding, privacy, and data protection risks and is strictly controlled.

Recording devices include, but are not limited to:

- digital cameras and video cameras
- mobile phones and tablets
- smart watches and smart glasses
- body-worn cameras
- wearable or covert recording devices
- laptops and webcams

The following requirements apply:

- Informed parental consent must be in place before photographs or video recordings of pupils are taken or used, in accordance with WeST Safeguarding and Data Protection Policies.
- Only Trust or School-issued and approved devices may be used to record images, audio, or video of pupils or staff
- Personal devices, including mobile phones, smart watches, smart glasses, and any other wearable or covert recording devices, must not be used to record pupils or staff under any circumstances
- Covert recording of any kind is strictly prohibited.
- Recording must only take place where there is a legitimate educational, safeguarding, or operational purpose and where appropriate consent has been obtained

All recordings must:

- be transferred to Trust or School systems as soon as possible
- be deleted from the original device and any associated cloud storage

- be stored, shared, and retained in accordance with data protection and safeguarding requirements

Images or recordings published internally or externally must:

- include only first names unless otherwise authorised
- comply with safeguarding, consent, and communications policies

Any unauthorised recording, attempted recording, or misuse of recording technology will be treated as a serious safeguarding and data protection incident and may result in disciplinary action.

12. File Storage and Removable Media

All Trust or School work must be stored on approved network or cloud storage systems.

Personal files must not be stored on Trust systems.

Use of removable media should be avoided and requires approval from WeST ICT.

Where removable media must be used:

- devices must be Trust-issued and encrypted
- confidential data must not be stored on unencrypted or personal devices
- off-site transfer of confidential data must use secure methods

13. Social Networking

Use of social media must comply with the Trust's Social Media Policy.

Staff must:

- protect the reputation of the Trust, School, staff, and students
- avoid sharing Trust information on personal social media accounts
- not publish opinions or information relating to pupils or colleagues
- not connect, engage with or message students via personal social media accounts

Official Trust or School social media use requires authorisation.

14. Filtering and Monitoring of ICT Systems

Filtering and monitoring controls are implemented in accordance with the Department for Education's digital and technology standards for schools and colleges. These controls are designed to safeguard pupils and staff, prevent access to harmful content, and detect misuse of Trust systems.

The Trust reserves the right to monitor the use of its ICT systems and networks to:

- ensure operational effectiveness
- maintain system security
- prevent or investigate policy breaches
- support safeguarding and legal obligations

Monitoring is carried out in accordance with data protection legislation and the Trust's privacy and monitoring notices. Monitoring may be performed manually or automatically using system monitoring tools. Monitoring may include the review of internet activity, email records, and stored data where necessary and proportionate.

Where unlawful activity is suspected, information may be shared with relevant authorities.

15. Failure to Comply with Policy

Failure to comply with this policy may result in disciplinary action. This includes deliberate attempts to access, create, store, or distribute material that presents a safeguarding risk to children or young people. Serious breaches may be treated as gross misconduct and may lead to summary dismissal.

16. Review

This policy will be reviewed at least biennially.

It will also be reviewed sooner where required as a result of:

- changes arising from annual reviews of the ICT Security Policy
- significant changes in technology, risk, or regulatory guidance
- identified incidents, audit findings, or assurance activity

Version History Log

Version	Description of Change	Date of Policy Release by WeST
0.1	Initial Draft	12/01/2026
0.2	Slight update to Agreement	02/02/2026
0.3	Amendment of governance arrangements to remove 'Governance Handbook'.	24/02/2026
1.0	Initial Issue	04/03/2026