

BOLD FUTURES



Bold Futures Federation

Acceptable Use of IT and Digital Technology Policy – Staff, Governors and Other Adults

Document Name: Acceptable Use of IT and Digital Technology Policy – Staff, Governors and Other Adults

Document ID: N/A

Current Version: 3.0

Status: Approved

Signed *L.Coombs, L.manser*
Print Name: L.Coombs, L.Manser

Signed: Robyn Jarret (Governor Approval)
Print Name: Robyn Jarret

BOLD FUTURES



POLICY CHANGE HISTORY

Version	Date	Status	Policy Owner	Governor Approval	Comment
2.0	September 2025		LC		Update to include Bold Futures & new ICT provider
3.0	September 2026		LC & LM		Staff and Governor Acceptable Use of ICT Policies combined and updated to reflect current safeguarding, data protection, cyber security, artificial intelligence and digital technology expectations.

1. Introduction and Purpose

Bold Futures Federation recognises that digital technology is an essential part of teaching, learning, communication, administration and effective school leadership. The Federation provides staff, governors and other authorised adults with access to digital devices, networks, systems, software and online services to enable them to carry out their roles effectively.

With access to digital technology comes a responsibility to use it safely, lawfully, professionally and securely.

This policy establishes the standards of acceptable use expected of adults who access or use Federation digital technology, systems, information or networks. It is intended to:

- safeguard and protect pupils, staff and other members of the Federation community;
- protect personal, confidential and sensitive information;
- maintain the security and integrity of Federation systems, networks and devices;
- support compliance with safeguarding and data protection requirements;
- establish clear professional expectations for the use of digital technology;
- reduce the risk of cyber security incidents, data breaches and inappropriate use;
- ensure emerging technologies, including artificial intelligence, are used safely, ethically and responsibly; and
- provide clear procedures for reporting concerns, incidents and potential breaches.

The Federation recognises that technology and associated risks develop rapidly. The principles within this policy therefore apply to existing and emerging technologies, whether or not a particular platform, device or service is specifically named.

2. Scope

This policy applies across all schools within Bold Futures Federation.

It applies to:

- all teaching and support staff;
- senior leaders;
- governors;
- volunteers;
- supply and agency staff;
- trainee teachers and other trainees;
- contractors and consultants;

- external professionals using Federation systems, including our IT provider;
- visitors who are provided with access to Federation technology; and
- any other adult authorised to access Federation devices, networks, information or digital services.

Throughout this policy, these individuals are collectively referred to as **users** unless a section specifically relates to a particular group.

The policy applies to the use of:

- Federation-owned computers, laptops, tablets and other devices;
- internet and Wi-Fi access;
- Federation email accounts;
- cloud-based services;
- management information and safeguarding systems, including Arbor and CPOMS where authorised;
- telephones and communication systems;
- cameras and recording equipment;
- websites and online platforms;
- software, applications and digital services;
- artificial intelligence and generative AI tools;
- removable storage where its use has been authorised;
- remote access to Federation systems;
- equipment loaned for use away from school; and
- personal devices where they are used for authorised Federation business or connected to Federation systems.

The principles of professional conduct within this policy may also apply to the personal use of technology where that use affects safeguarding, confidentiality, professional boundaries, the security of Federation information or an individual's suitability to work with children.

3. Relationship with Other Federation Policies

This policy forms part of the Federation's wider framework for safeguarding, data protection and responsible use of technology.

It should be read alongside the:

- **Child Protection and Safeguarding Policy;**
- **Online Safety Policy;**
- **Data Protection Policy;**
- **Social Media Policy;**
- **Computing Policy;**
- **Remote Education Policy;**

- **Staff Code of Conduct;**
- **Behaviour Policy;**
- **Anti-Bullying Policy;**
- **Whistleblowing Policy;** and
- relevant Federation guidance concerning photography, video and image sharing.

Where an incident involving technology raises a safeguarding concern, the Child Protection and Safeguarding Policy takes precedence and safeguarding procedures must be followed immediately.

Where an incident involves the loss, unauthorised disclosure or inappropriate processing of personal data, the Data Protection Policy and the Federation's data-breach procedures must be followed.

Where a cyber incident has occurred, the Cyber Incident Response plan must be followed.

Detailed expectations regarding professional and personal social media use are contained within the Social Media Policy.

Detailed arrangements for protecting pupils from online harm, including filtering and monitoring, are contained within the Online Safety Policy.

4. General Principles of Acceptable Use

Users must use Federation technology responsibly, professionally and primarily for purposes connected with their role.

Users must:

- follow Federation policies and procedures when using digital technology;
- use only systems, applications and services that have been authorised for Federation use;
- comply with instructions relating to cyber security, data protection and safeguarding;
- take reasonable steps to protect Federation devices and information from loss, damage or unauthorised access;
- maintain appropriate professional boundaries when communicating electronically;
- immediately report safeguarding, cyber-security, data-protection or online-safety concerns through the appropriate Federation procedure; and
- cooperate with reasonable monitoring, investigation and security measures undertaken by the Federation.

Limited personal use of Federation technology may be permitted where this is reasonable, lawful, does not interfere with an individual's duties, does not incur inappropriate cost and does not compromise safeguarding, security or professional standards.

5. Accounts, Passwords and Access

Users will only be provided with access to systems, accounts and information appropriate to their role. Access rights will be based on operational need and will be reviewed as appropriate.

Each user is responsible for the security of their individual accounts and login credentials.

5.1 Accounts and access

Users must:

- use only their own authorised account;
- never knowingly allow another person to use their account;
- never use another person's account or attempt to discover another person's password;
- only access systems, files and information for which they have been authorised;
- lock their device whenever leaving it unattended;
- log out of systems when appropriate;
- use multi-factor authentication (MFA) wherever this has been enabled or required by the Federation; and
- immediately report suspected unauthorised access or unusual account activity to the appropriate senior leader and/or IT support provider.

Users must not attempt to bypass security controls or obtain access to systems, accounts, files or information for which they do not have permission.

Governors, volunteers, contractors and other authorised users who are provided with access to Federation systems or confidential information must follow the same expectations for account security and confidentiality as employees.

5.2 Federation password requirements

Passwords are an important part of protecting Federation systems, safeguarding information and personal data. All users must therefore follow the Federation's password requirements.

Passwords for staff and governor accounts must:

- contain a minimum of 12 characters;
- be sufficiently strong and difficult for another person to guess;
- not contain the name of any school within the Federation, the Federation name or a school's DfE number;
- not contain easily guessed personal information, such as the user's name, date of birth, class name, username or email address;

- not use common or predictable passwords or sequences, such as Password123, 12345678 or Qwerty;
- not simply be a minor or predictable variation of a previous password;
- be different from passwords used for personal accounts; and
- be kept confidential and never shared with colleagues, pupils, family members or any other person.

Users should use long, memorable passwords or passphrases that are difficult for another person to predict.

Passwords must not be displayed on or near devices, for example on sticky notes, or stored in an unsecured document or location.

Where separate passwords are required for different Federation systems, users should not routinely reuse the same password across multiple accounts.

5.3 Changing passwords

The Federation does not require users to change secure passwords routinely at short, fixed intervals. Repeated password changes can encourage predictable or weaker passwords and do not, by themselves, improve account security.

Instead, passwords must be changed immediately where:

- the user believes their password may have been disclosed, guessed or compromised;
- suspicious or unauthorised activity is identified on an account;
- a device or service containing stored login information has been compromised;
- there has been a relevant cyber-security incident; or
- the Federation or its IT provider instructs the user to change it.

The Federation will review its password-security arrangements at least annually and may require password changes where an increased risk is identified.

5.4 Multi-factor authentication

Multi-factor authentication (MFA) provides an additional layer of protection where a password is compromised.

Users must:

- set up and use MFA where required by the Federation;
- never share an MFA code with another person;
- never approve an MFA request that they did not initiate; and
- immediately report unexpected or repeated MFA requests, as these may indicate an attempt to access their account.

5.5 Privileged and administrator accounts

Administrator and other highly privileged accounts may be subject to additional password, access and authentication requirements determined by the Federation and its IT support provider.

Privileged access must only be provided where necessary for the user's role and must not be used for routine activity where a standard user account is sufficient.

The Federation may amend its technical password and authentication requirements in response to changes in cyber-security guidance, technology, identified risks or advice from its IT provider.

6. Cyber Security

Cyber security is the responsibility of everyone who uses Federation technology.

Users must remain alert to potential cyber threats, including:

- phishing emails;
- suspicious links and attachments;
- fraudulent requests for payments or information;
- attempts to obtain passwords or authentication codes;
- social engineering;
- malware;
- ransomware;
- unusual login requests;
- unexpected multi-factor authentication requests; and
- other suspicious activity.

Users must not open suspicious attachments, follow suspicious links or provide information in response to communications they believe may be fraudulent.

Users must never approve an unexpected MFA request.

Suspected cyber incidents must be reported immediately in accordance with Federation procedures.

Users must not:

- disable security software or other security controls;
- attempt to bypass the Federation's firewall, filtering or monitoring systems;
- install unauthorised software, applications, browser extensions or other programs;
- connect unauthorised equipment to the Federation network;
- intentionally introduce malicious software;
- attempt to access another user's account; or

- attempt to test, probe or compromise the security of Federation systems without explicit authorisation.
-

7. Devices and Equipment

Federation devices are provided to support authorised Federation activity.

Users are expected to take reasonable care of equipment provided to them.

Devices must:

- be kept physically secure;
- not be left unattended where they may be lost, stolen or accessed by unauthorised individuals;
- be locked when temporarily unattended;
- be stored securely when not in use; and
- be returned to the Federation when requested or when the user's role ends.

Where Federation equipment is used away from school, users must take appropriate precautions to protect both the device and the information accessible through it.

Federation devices must not be made available to family members, friends or other unauthorised individuals.

Loss, theft or damage must be reported promptly.

8. Personal Devices

Personal devices must not normally be used to store or process Federation personal or confidential information.

Where personal devices are permitted for a specific authorised purpose, users must comply with Federation requirements concerning safeguarding, confidentiality and data protection.

Personal devices must not be used to photograph or record pupils unless this has been explicitly authorised under Federation procedures.

Personal devices must not be accessible to pupils while being used for Federation business.

Where staff or governors are required to use a personal telephone for authorised Federation communication, reasonable steps must be taken to protect personal contact details and maintain professional boundaries.

Further requirements concerning personal devices, photography and communication with pupils are contained within the Child Protection and Safeguarding Policy, Online Safety Policy and relevant Federation guidance.

9. Data Protection and Confidential Information

All users have a responsibility to protect the information to which they have access.

Personal data must be processed in accordance with the Federation's Data Protection Policy.

Users must:

- only access personal or confidential information required for their role;
- keep information secure;
- use authorised systems to store Federation information;
- take particular care when working away from school;
- check recipients carefully before sending information electronically;
- use appropriate secure methods when transmitting confidential or personal information;
- avoid downloading personal data to local or personal devices unless authorised;
- ensure information displayed on screen cannot unnecessarily be viewed by others;
- lock devices when unattended; and
- report actual or suspected personal-data breaches immediately in accordance with Federation procedures.

Federation information must not be transferred to personal email accounts or unauthorised cloud-storage services.

Users must not disclose confidential information to individuals who are not authorised to receive it.

10. Email and Electronic Communication

Federation-provided accounts must be used for Federation business.

Personal email accounts must not be used to communicate confidential Federation information or to conduct school business where an authorised Federation system is available.

Users must:

- communicate professionally and respectfully;
- consider carefully whether email is the appropriate means of communication;
- check recipients before sending messages;
- take particular care when sending personal or confidential information;
- follow Federation procedures for communication with parents and carers;
- maintain professional boundaries in all electronic communication; and
- report inappropriate, threatening, suspicious or safeguarding-related communications.

Staff must not use personal email addresses, personal social-media accounts or personal messaging services to communicate directly with parents/ carers or pupils. All communication with parents/ carers will happen through Arbor or via the school office email.

Any communication raising a safeguarding concern must be dealt with in accordance with the Child Protection and Safeguarding Policy.

11. Social Media

Users must maintain appropriate professional boundaries when using social media.

Personal social-media accounts must not be used to conduct Federation business or communicate with current pupils.

Users must not publish confidential information, pupil information or Federation information without appropriate authorisation.

Users should recognise that privacy settings cannot guarantee that online material will remain private and that online activity may affect professional responsibilities.

Detailed expectations relating to:

- personal social-media use;
- official Federation accounts;
- communication with pupils and parents;
- online professional boundaries;
- publication of images and information;
- complaints and comments about the Federation; and
- conduct which may bring the Federation into disrepute

are set out within the Federation's Social Media Policy.

12. Artificial Intelligence and Generative AI

Bold Futures Federation recognises that artificial intelligence, including generative AI, can support professional practice when used appropriately.

AI tools must be used safely, ethically, transparently and in accordance with Federation expectations.

Users must:

- only use AI tools for Federation purposes where their use has been authorised;
- never enter confidential, sensitive or personally identifiable pupil, parent, staff or Federation information into an AI tool unless the tool and proposed use have been specifically approved;
- consider data protection and safeguarding implications before using AI;
- critically evaluate AI-generated information for accuracy, bias and appropriateness;
- recognise that AI-generated outputs may contain inaccurate or fabricated information;
- retain professional responsibility for all work produced with the assistance of AI;
- check AI-generated materials before they are shared with pupils, parents or colleagues;
- respect intellectual property and copyright; and
- follow any additional Federation guidance concerning approved AI platforms.

AI must not be used to make significant decisions about pupils or staff without appropriate human oversight and authorisation.

AI tools must not replace professional judgement.

Use of AI with pupils must be age appropriate, educationally justified and consistent with the Federation's Computing Policy, Online Safety Policy, Child Protection and Safeguarding Policy and Data Protection Policy.

13. Internet Access, Filtering and Monitoring

The Federation provides filtered and monitored internet access to support education and Federation business.

Users must not attempt to disable, circumvent or interfere with filtering, monitoring or other security systems.

Users must not deliberately access, create, download, store or distribute material that is illegal, harmful, discriminatory, extremist, sexually explicit, threatening, abusive or otherwise inappropriate.

Where inappropriate material is accessed accidentally, the user should:

1. stop accessing the content;
2. avoid unnecessarily copying, sharing or forwarding it;
3. report the incident promptly to a member of SLT and/or the school's IT provider (Harrap); and
4. follow safeguarding instructions where the content may relate to the safety of a child.

Accidental access that is promptly and appropriately reported will be considered differently from deliberate or repeated attempts to access prohibited material.

Filtering and monitoring arrangements, responsibilities and safeguarding procedures are set out in greater detail within the Federation's Online Safety Policy and Child Protection and Safeguarding Policy.

14. Software, Applications and Online Services

Only appropriately authorised software, applications and online services should be used for Federation purposes.

Users must not install software, applications, browser extensions or other programs on Federation equipment without appropriate authorisation.

Before a new online service or application is introduced, appropriate consideration must be given to:

- data protection;
- cyber security;
- safeguarding;
- age restrictions;
- terms and conditions;
- privacy;
- accessibility; and
- educational or operational purpose.

Where a service will process personal data, relevant Federation data-protection procedures must be followed.

15. Removable Media and External Storage

The use of removable storage devices, including USB drives and external storage, should be avoided where secure Federation-approved alternatives are available.

Removable media must not be used to store or transfer personal, confidential or sensitive information unless specifically authorised and appropriately secured.

Unknown or untrusted removable media must never be connected to Federation devices.

Users must follow any technical restrictions or instructions issued by the Federation or its IT support provider.

16. Photography, Video and Audio Recording

Photographs, videos and audio recordings involving pupils must only be created for legitimate and authorised Federation purposes.

Federation equipment should be used for such recordings wherever possible.

Users must follow Federation procedures relating to:

- consent and other lawful bases;
- safeguarding;
- storage;
- publication;
- sharing;
- retention; and
- deletion.

Personal devices must not be used to photograph or record pupils unless explicitly authorised.

Images or recordings must not be transferred to personal accounts or unauthorised services.

Further requirements are contained within the Child Protection and Safeguarding Policy, Data Protection Policy, Social Media Policy and Federation photography/image-sharing guidance.

17. Remote and Home Working

Users accessing Federation systems away from school remain subject to this policy.

When working remotely, users must:

- use Federation-provided equipment wherever practicable;
- prevent family members or other individuals from accessing Federation devices or information;
- consider the privacy of their working environment;
- secure devices when not in use;
- use authorised methods to access Federation systems;
- use MFA where required;
- avoid accessing sensitive information using insecure or public devices;
- take appropriate care when using public Wi-Fi; and
- report loss, theft, unauthorised access or other security concerns immediately.

Where remote education is being provided to pupils, users must also follow the Federation's Remote Education Policy, Online Safety Policy and Child Protection and Safeguarding Policy.

18. Unacceptable Use

Federation systems, networks and devices must not be used to:

- access, create, store, send or distribute illegal or inappropriate material;
- bully, harass, intimidate, discriminate against or threaten another person;
- access or distribute sexually explicit material except where access is specifically required and authorised for a legitimate safeguarding purpose;
- compromise the safeguarding or welfare of a child;
- disclose confidential information without authority;
- impersonate another user;
- access another person's account or information without authorisation;
- deliberately introduce malware or compromise cyber security;
- circumvent security, filtering or monitoring systems;
- conduct unauthorised commercial activity;
- gamble;
- engage in unlawful activity;
- infringe copyright or intellectual-property rights;
- undertake unauthorised political campaigning using Federation resources;
- damage the reputation or operational security of the Federation through inappropriate use;
- store Federation information in unauthorised locations; or
- use technology in any manner inconsistent with the professional responsibilities associated with working with children.

This list is not exhaustive. Users are expected to exercise professional judgement and seek advice where they are unsure whether a particular use is appropriate.

19. Reporting Concerns and Incidents

Users must report concerns promptly.

Safeguarding or online-safety concern involving a child

Report immediately to the Designated Safeguarding Lead (DSL) in accordance with the Child Protection and Safeguarding Policy.

Suspected personal-data breach

Report immediately in accordance with the Data Protection Policy and Federation data-breach procedure.

Cyber-security incident

Report immediately to the appropriate senior leader and/or IT support provider in accordance with Federation procedures outlined in the Cyber Incident Response Plan.

Examples include:

- compromised accounts;
- phishing;
- malware or ransomware;
- suspicious login activity;
- lost or stolen devices;
- accidental disclosure of information;
- unexpected MFA requests; or
- suspected unauthorised access.

Concern about the conduct of an adult

Concerns must be reported through the appropriate safeguarding, low-level concern, allegations or whistleblowing procedure.

Users must not attempt to conduct their own investigation into a safeguarding or potentially criminal incident.

20. Monitoring

The Federation reserves the right to monitor the use of its devices, networks, systems and services where this is lawful, proportionate and necessary for purposes including:

- safeguarding;
- cyber security;
- preventing or detecting misuse;
- investigating suspected breaches;
- maintaining system integrity; and
- meeting legal and regulatory responsibilities.

Users should have no expectation that activity conducted using Federation systems is entirely private.

Any monitoring of personal data will be undertaken in accordance with applicable data-protection requirements and Federation policy.

21. Responsibilities

All users

All users are responsible for:

- reading and following this policy;
- protecting their accounts and devices;
- completing required training;
- maintaining confidentiality;
- reporting concerns promptly; and
- using technology safely, responsibly and professionally.

Staff

Staff have an additional responsibility to:

- model safe and responsible use of technology to pupils;
- maintain appropriate professional boundaries;
- follow safeguarding and data-protection procedures;
- supervise pupils' use of technology appropriately; and
- report concerns relating to pupils' online safety.

Governors

Governors are responsible for:

- following this policy whenever accessing Federation information or systems;

- maintaining the confidentiality of information obtained through their governance role;
- using secure Federation-approved methods of communication and information sharing;
- undertaking relevant safeguarding, data-protection and cyber-security training; and
- providing appropriate strategic oversight of digital safeguarding and security, including the allocation of a designated Governor .

The governing body has strategic oversight of the Federation's arrangements for safeguarding, online safety and appropriate use of digital technology.

Senior Leaders

Senior leaders are responsible for ensuring that:

- appropriate policies and procedures are in place;
- users receive appropriate training and guidance;
- responsibilities for digital security are clearly assigned;
- safeguarding, data-protection and cyber-security incidents are appropriately managed;
- access to systems is proportionate to users' roles; and
- the Federation works effectively with its IT support provider.

IT Support Provider

The Federation's IT support provider works with senior leaders to maintain appropriate technical security, including access controls, system security, updates, backups, filtering and monitoring arrangements and other agreed technical safeguards.

22. Breaches of this Policy

Any suspected breach of this policy will be considered appropriately and proportionately.

Depending upon the nature of the incident, action may include:

- advice or additional training;
- restriction or withdrawal of access to Federation systems;
- investigation under relevant Federation procedures;
- disciplinary action;
- safeguarding action;
- referral to the Data Protection Officer;
- notification to relevant external agencies or regulatory bodies; and/or
- referral to the police where criminal activity is suspected.

A safeguarding concern will always be managed in accordance with the Federation's Child Protection and Safeguarding Policy.

23. Training and Awareness

All relevant users will be made aware of their responsibilities for acceptable use of technology.

Staff training will include appropriate updates relating to:

- safeguarding and online safety;
- data protection;
- phishing and social engineering;
- cyber security;
- password and account security;
- reporting cyber incidents;
- personal-data breaches;
- artificial intelligence and emerging technology; and
- changes to Federation systems or procedures.

Governors will receive appropriate information and training to enable them to fulfil their strategic oversight responsibilities.

24. Review

This policy will be reviewed annually or sooner where necessary because of:

- changes to legislation or statutory guidance;
- changes to Department for Education digital and technology standards;
- safeguarding developments;
- significant technological developments;
- changes to Federation systems or infrastructure;
- introduction of significant new technologies, including AI; or
- learning arising from an incident.

The policy will be approved by the governing body and communicated to relevant users.
