



The Welbeck Federation

Acceptable Use Policy

Executive Head Teacher Signature:	<i>L Jordan</i>
Date Adopted:	Sept 2026
Review Date:	Sept 2027

1. Introduction

Technology is an essential part of teaching, learning, communication and administration across The Welbeck Federation. The use of digital technologies provides significant educational benefits but also presents safeguarding, cyber-security and data protection risks.

This Acceptable Use Policy (AUP) outlines the expectations for all users of Federation ICT systems, devices, networks, online platforms and internet services. It applies to:

-  Staff
-  Governors
-  Volunteers
-  Visitors
-  Contractors
-  Pupils
-  Parents and carers (where applicable)

All users are expected to use Federation technology safely, responsibly, legally and respectfully.

2. Aims

The aims of this policy are to:

-  Protect pupils, staff and the wider school community.
-  Promote safe and responsible use of technology.
-  Safeguard personal and sensitive information.
-  Support teaching and learning.
-  Prevent misuse of ICT systems.
-  Ensure compliance with safeguarding, data protection and cyber-security requirements.

3. Scope

This policy applies to:

-  All Federation-owned devices.
-  Personal devices used for school purposes.
-  Internet access provided by the Federation.
-  Cloud-based services.
-  Email systems.
-  Microsoft 365 services.
-  Online learning platforms.
-  Social media use related to school business.

The policy applies both on and off site when school systems or information are being accessed.

4. Acceptable Use

Users must:

-  Use ICT systems primarily for educational and professional purposes.
-  Act respectfully and responsibly online.

-  Protect passwords and account information.
-  Follow safeguarding procedures.
-  Report concerns immediately.
-  Respect copyright and intellectual property.
-  Protect personal data.
-  Use only approved software and applications.
-  Follow the Federation's Online Safety Policy.

5. Unacceptable Use

The following activities are prohibited:

Content

-  Accessing inappropriate, obscene, violent or illegal material.
-  Creating, sharing or storing offensive content.
-  Accessing extremist or radicalising material.
-  Viewing or sharing pornography.

Conduct

-  Cyberbullying.
-  Harassment or discrimination.
-  Offensive or abusive language.
-  Sharing inappropriate images or videos.

Technical Misuse

-  Attempting to bypass filtering systems.
-  Installing unauthorised software.
-  Accessing accounts without permission.
-  Hacking, scanning or interfering with Federation systems.
-  Deliberately introducing malware or viruses.

Data Misuse

-  Sharing confidential information.
-  Accessing information without authorisation.
-  Sending personal data insecurely.
-  Breaching GDPR requirements.

Professional Conduct

-  Bringing the Federation into disrepute.
-  Using personal social media to communicate with pupils.
-  Recording pupils using personal devices without authorisation.
-  Using Federation systems for inappropriate personal business activities.

6. Artificial Intelligence (AI)

The Federation recognises the increasing use of AI technologies.

Staff and pupils may only use approved AI tools.

Users must:

-  Verify AI-generated information before use.
-  Not submit personal or confidential information into public AI platforms.
-  Ensure AI use complies with safeguarding and GDPR requirements.

-  Acknowledge AI support where appropriate.

AI must support learning and professional practice but must never replace professional judgement. This is particularly important in safeguarding, assessment and communication with families.

7. Staff Responsibilities

Staff must:

-  Model safe and responsible technology use.
-  Maintain professional boundaries online.
-  Use Federation email accounts for school business.
-  Keep passwords secure.
-  Lock devices when unattended.
-  Complete annual cyber-security and safeguarding training.
-  Report online safety concerns immediately.
-  Follow all Federation safeguarding procedures.

Staff must not:

-  Share passwords.
-  Use personal social media to communicate with pupils.
-  Upload images of pupils using personal accounts.
-  Store confidential information on personal devices unless authorised.
-  Use school technology for inappropriate purposes.

8. Pupil Responsibilities

Pupils must:

-  Use technology respectfully and safely.
-  Follow instructions given by adults.
-  Keep passwords private.
-  Report anything that makes them uncomfortable.
-  Use devices for learning purposes only.
-  Respect the privacy and rights of others.

Pupils must not:

-  Access inappropriate websites.
-  Use unauthorised social media.
-  Share passwords.
-  Bully others online.
-  Attempt to bypass filtering systems.
-  Use another person's account.

9. Mobile Phones and Personal Devices

Pupils

Where mobile phones are permitted:

-  Phones must be handed into the school office on arrival.
-  Phones remain switched off.
-  Phones must not be used during the school day.

- Any misuse will be dealt with through the Behaviour Policy.

Staff

Staff may use personal devices only in line with the Staff Code of Conduct.

Personal devices must not be used to:

- Store pupil information.
- Photograph pupils unless specifically authorised.
- Communicate with pupils through personal accounts.

10. Filtering and Monitoring

The Federation uses Atom IT to provide filtering, monitoring and cyber-security systems.

The Federation monitors:

- Internet activity.
- Search activity.
- User activity.
- Network security events.
- Safeguarding alerts.

Monitoring is conducted to:

- Safeguard children.
- Maintain network security.
- Investigate concerns.
- Meet statutory requirements.

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

11. Data Security

All users must:

- Use strong passwords.
- Protect sensitive information.
- Store information securely.
- Follow GDPR requirements.
- Report suspected data breaches immediately.

Federation devices are protected through:

- Filtering systems.
- Monitoring systems.
- Antivirus protection.
- Encryption.
- Security updates.
- Access controls.

Technical support is provided by Atom IT.

12. Reporting Concerns

All online safety concerns must be reported immediately to a Designated Safeguarding Lead.

Safeguarding Team	
Designated Safeguarding Lead  Lisa Jordan	Deputy Safeguarding Leads  Matt Walker  Joanne Turner  Caroline Goodall

Examples include:

-  Cyberbullying.
-  Online abuse.
-  Inappropriate content.
-  Suspicious online contact.
-  Safeguarding disclosures.
-  Data breaches.
-  Security incidents.

Concern records will be maintained through CPOMS where appropriate.

13. Sanctions

Failure to comply with this policy may result in:

Pupils

-  Removal of ICT access.
-  Behaviour sanctions.
-  Parent meetings.
-  Fixed-term suspension where appropriate.
-  External agency involvement.

Staff

-  Removal of ICT access.
-  Management action.
-  Formal disciplinary procedures.
-  Referral to external agencies where required.

The Federation reserves the right to refer illegal activity to the police.



ACCEPTABLE USE OF THE SCHOOL'S ICT SYSTEMS AND INTERNET: AGREEMENT FOR STAFF, GOVERNORS, VOLUNTEERS AND VISITORS

Name of staff member/governor/volunteer/visitor:

When using the school's ICT systems and accessing the internet in school, or outside school on a work device (if applicable), I will not:

-  Access, or attempt to access inappropriate material, including but not limited to material of a violent, criminal or pornographic nature (or create, share, link to or send such material)
-  Use them in any way which could harm the school's reputation
-  Access social networking sites or chat rooms
-  Use any improper language when communicating online, including in emails or other messaging services
-  Install any unauthorised software, or connect unauthorised hardware or devices to the school's network
-  Share my password with others or log in to the school's network using someone else's details
-  Take photographs of pupils without checking with teachers first
-  Share confidential information about the school, its pupils or staff, or other members of the community
-  Access, modify or share data I'm not authorised to access, modify or share
-  Promote private businesses, unless that business is directly related to the school

I will only use the school's ICT systems and access the internet in school, or outside school on a work device, for educational purposes or for the purpose of fulfilling the duties of my role.

I agree that the school will monitor the websites I visit and my use of the school's ICT facilities and systems.

I will take all reasonable steps to ensure that work devices are secure and password-protected when using them outside school, and keep all data securely stored in accordance with this policy and the school's data protection policy.

I will let the designated safeguarding lead (DSL) and ICT manager know if a pupil informs me they have found any material which might upset, distress or harm them or others, and will also do so if I encounter any such material.

I will always use the school's ICT systems and internet responsibly, and ensure that pupils in my care do so too.

I have read and understood the Federation Acceptable Use Policy.

Signed (staff member/governor/volunteer/visitor):	
Date:	



Eastlands Junior School

Pupil Acceptable Use Agreement

I will:

- 🌐 Use school technology safely.
- 🌐 Be kind and respectful online.
- 🌐 Keep my password private.
- 🌐 Tell an adult if something worries or upsets me.
- 🌐 Use technology for learning.

I will not:

- 🌐 Access inappropriate websites.
- 🌐 Share personal information.
- 🌐 Use another person's account.
- 🌐 Be unkind online.
- 🌐 Share photos or content without permission.

Pupil Name: _____

Signed: _____

Parent/Carer: _____

Date: _____



Netherfield Infant School

Pupil Acceptable Use Agreement

When I use computers, tablets or the internet at school, I will:

- 🌐 Listen to my teacher.
- 🌐 Use technology carefully.
- 🌐 Be kind to others.
- 🌐 Ask for help if I see something worrying.
- 🌐 Keep my password secret.

Pupil Name: _____

Signed: _____

Parent/Carer: _____

Date: _____