Acceptable Use Policy

Written by	Reviewed and Ratified by Governors	Shared with Staff	Last Updated	Review cycle	Next Review due
Polly Ross Headteacher	September 2026	September 2026	September 2026	Annual	September 2027

1. Introduction

This Acceptable Use Policy (AUP) sets out the expectations for the safe, lawful and professional use of technology, devices, networks, systems and online platforms by all staff, volunteers, contractors and visitors.

The school recognises that digital technologies are essential to teaching, learning, safeguarding, administration and communication. All users are therefore expected to use school systems responsibly, securely and in accordance with:

- UK GDPR
- Data Protection Act 2018
- Keeping Children Safe in Education
- DfE cyber security standards for schools
- the Staff Code of Conduct
- safeguarding procedures
- all related school policies

This policy applies to:

- school-owned devices
- personal devices used for school business (BYOD)
- cloud systems
- email and messaging systems
- internet and Wi-Fi access
- remote and home working
- social media
- monitoring technologies
- AI and generative AI platforms

FINAL

Any misuse may result in removal of access rights, disciplinary action, referral to external agencies, and where appropriate, legal action.

2. Monitoring, Privacy and Data Protection

The school may undertake proportionate monitoring of systems, devices and network usage for safeguarding, cyber security, legal compliance, performance management, attendance, service protection and investigation of suspected misconduct.

2.1 Lawful basis

Monitoring will only take place where there is a clear lawful basis under UK GDPR, including:

- **public task**
- **legal obligation**
- **legitimate interests**
- where necessary, vital interests or safeguarding duties

2.2 Transparency

The school will:

- clearly explain the purpose of monitoring
- inform staff what data may be collected
- ensure monitoring is necessary and proportionate
- complete a Data Protection Impact Assessment (DPIA) for higher-risk monitoring
- keep records secure and only for as long as necessary
- recognise increased privacy expectations in home-working environments

2.3 Types of monitoring

Monitoring may include:

- network and internet activity logs
- filtering and firewall alerts
- device audit logs
- login records
- email metadata
- CCTV and access control systems
- attendance and timekeeping systems
- safeguarding keyword alerts
- productivity and usage reports on school-owned systems

2.4 Exceptional covert monitoring

Covert monitoring will only be authorised in exceptional circumstances where there is reasonable suspicion of serious misconduct, unlawful activity, or safeguarding risk. Covert monitoring may only be

FINAL

authorised by the **Headteacher in consultation with the Chair of Governors** and must only proceed after:

- Obtaining legal advice from the school's HR/legal advisors
- Completing a Data Protection Impact Assessment (DPIA)
- Documenting the justification, scope, and duration of monitoring
- Ensuring the monitoring is necessary, proportionate, and lawful

All covert monitoring must be reported to the governing board at the earliest appropriate opportunity.

3. Cyber Security and Data Protection Responsibilities

All users must:

- use systems in accordance with data protection law
- keep passwords confidential
- use multi-factor authentication (MFA) where enabled
- lock devices when unattended
- report suspected phishing, malware or breaches immediately
- only use approved systems and software
- follow ICT and safeguarding procedures

Users must not:

- bypass filtering, monitoring or security controls
- share passwords or authentication codes
- use another person's login
- store confidential school data in unapproved locations
- use personal cloud storage for school information

4. Use of School ICT Systems

Users will:

- only access systems they are authorised to use
- use the internet professionally and lawfully
- use removable media only where approved and encrypted
- only install software authorised by the Headteacher, Network Manager or ICT support provider

Users will not:

- access, upload, store or share inappropriate, harmful or illegal material
- deliberately access blocked content
- download unauthorised software, browser extensions or apps

Limited personal use of personal devices may take place only during unpaid breaks, lunch periods, or outside directed working time, in approved staff areas.

FINAL

School-owned devices must not be used for personal purposes at any time unless expressly authorised in writing by the Headteacher for exceptional circumstances (e.g., emergency contact)."

5. Email, Messaging and Communications

Staff must:

- use only approved school email accounts for school business
- verify recipients before sending personal data
- use encryption or secure links where appropriate
- report suspicious emails immediately
- use only approved communication platforms for contact with pupils and parents

Staff must not:

- use personal email for school business
- use personal messaging apps to communicate with pupils or parents
- forward school data to personal accounts

6. School-Owned Devices

Users must:

- use school devices only for professional purposes
- keep devices secure and under supervision
- transport devices safely
- never leave devices visible in unattended vehicles
- keep systems updated as directed
- report loss, theft, damage or compromise immediately
- permit remote locking or remote wiping where required
- return all devices and accessories at the end of employment or loan

6.1 Asset Loan Authorisation Process: All requests to remove school devices from site must be:

- Approved in writing by the Headteacher or Network Manager
- Recorded on the Asset Loan Form, which must include:
    - Device type and serial number
    - Issue date and expected return date
    - Device condition at time of issue
    - User acknowledgment of remote wipe/security controls
    - User signature confirming acceptance of this policy

Asset Loan Forms are stored securely by the Office Manager and reviewed termly to ensure all outstanding loans are accounted for.Users must return devices immediately upon request or at the end of their employment/loan period.

FINAL

7. Personal Devices (Personal Use Only)

Personal devices are **not permitted for any school business purpose**, including accessing pupil data, staff data, email, cloud systems, safeguarding systems, MIS platforms, assessment tools or any confidential School information.

Personal devices may only be brought on site for **limited personal use during unpaid breaks in approved staff areas**, subject to the following:

- devices must remain on silent during working time
- devices must be securely stored away from pupils
- devices must not be used for calls outside approved staff areas
- devices must not connect to School systems, email or cloud storage
- devices must not be used for photography, video or audio recording involving pupils, staff, parents or visitors
- devices must not be used to contact pupils or parents

Users must not:

- store school data locally
- photograph or record pupils, staff or parents
- connect personal devices to internal School networks unless using an approved guest network
- sync or transfer School files to personal devices or cloud services

Any accidental access to School data on a personal device must be reported immediately.

8. Photography, Video and Audio:

Images, video or audio recordings involving pupils, staff, parents or visitors may only be created, stored or shared using approved school systems and devices and where:

- there is a clear educational, safeguarding or operational purpose
- consent and lawful basis requirements are met
- retention arrangements are clear

8.1 Approved systems
Photography and recording for school purposes must only be conducted using:

- School-owned iPads/ phones
- School cameras
- Approved school platforms

8.2 When recording is permitted
Recording is only permitted where:

- There is a clear educational, safeguarding or operational purpose
- Appropriate consent has been obtained and recorded
- The lawful basis under UK GDPR has been identified
- Retention arrangements are clear and documented

8.3 Consent and permissions

FINAL

Before taking photographs or recordings:

- Check the school's photographic consent register to ensure parents have given permission
- Be aware of any pupils who must not be photographed (e.g., children in care, those subject to court orders)
- Ensure pupils are appropriately dressed and the content is appropriate

8.4 Storage and retention

- Images must be stored only on approved school systems
- Images must be deleted in line with the school's retention schedule
- Images must not be stored on personal devices or personal cloud storage

8.5 Parents' own photography at school events
Parents may take photographs/videos at designated school events (e.g., performances, sports days) for personal use only, subject to the following conditions:

- Images must not be shared on social media if they include other children
- Parents must respect the wishes of other families
- The school will communicate these expectations before each event

9. Social Media and Online Professionalism

Staff must maintain professional boundaries online at all times.

Staff must:

- follow the Staff Code of Conduct
- apply suitable privacy settings
- ensure personal use does not undermine professional standards, confidentiality, safeguarding duties or the reputation of the school
- use only authorised school accounts for official posts

10. Home and Remote Working

Where working remotely, staff must:

- use approved systems and secure connections
- prevent access by family members or others
- use privacy screens or position screens away from public view where necessary
- securely dispose of printed documents
- avoid discussing confidential matters in public spaces

FINAL

- report any home-working data breach immediately

Sensitive personal data must only be transferred where strictly necessary and must be encrypted, pseudonymised or stored only within approved school cloud systems.

11. Artificial Intelligence (AI) and Generative AI

Staff may only use AI tools that have been approved by the school.

Staff must not input into public or unapproved AI systems any:

- pupil data
- SEND information
- safeguarding records
- medical information
- behavioural records
- staff personal data
- assessment information
- confidential school business

Before any AI system is adopted, the school must ensure:

- data protection due diligence is completed
- a DPIA is undertaken where required
- safeguarding implications are assessed
- human oversight remains in place
- outputs are checked for bias, accuracy and appropriateness

AI-generated content must always be professionally reviewed before use with pupils, parents or staff.

12. Training and Reporting Concerns

All users must:

- complete cyber security, safeguarding and data protection training
- participate in refresher training
- act as digital role models for pupils
- report concerns, misuse, phishing attempts or breaches immediately to the Headteacher or ICT lead

12.1 What constitutes a serious incident
A **serious incident** includes:

- **Data breaches** affecting personal data of pupils, staff or parents (e.g., unauthorised access, loss of device containing data, data sent to wrong recipient)
- **Safeguarding concerns** identified through monitoring or reported by staff
- **Cyber security incidents** including suspected malware, ransomware, phishing compromise, or unauthorised access to systems
- **Loss or theft** of devices containing school data

FINAL

- **Suspected deliberate misuse** of systems that may constitute gross misconduct

12.2 Reporting process

Immediate action (within 1 hour of discovery where possible):

- Report to the Headteacher (or Deputy Headteacher in their absence)
- For safeguarding concerns, also report immediately to the Designated Safeguarding Lead (DSL)
- For data breaches, also report to the school's Data Protection Officer
- For cyber security incidents, also report to Partnership Education

Within 24 hours:

- Complete an incident report form
- The Headteacher will determine whether external reporting is required (e.g., to the ICO, police, LADO, local authority)

Follow-up:

- All serious incidents will be logged and reviewed by the governing body
- Lessons learned will be shared with staff as appropriate

13. Breaches of this Policy

Failure to comply may result in:

- withdrawal of access rights
- internal investigation
- disciplinary action
- referral to governors
- referral to police, LADO, DPO, ICO or other agencies where appropriate

14. Staff Declaration

I confirm that I have read, understood and agree to comply with this Acceptable Use Policy.

Name: _____
Signature: _____
Date: _____

FINAL