High Ercall Primary School

Acceptable Use Policy – 2026-27

Staff, Governors and Volunteers with IT access

Document Status			
Date of Policy Creation	**February 2022**	**Named Responsibility**	Sarah Roberts
Date of review completion	**1st September 2026**	**Named Responsibility**	Gemma Lingham
Inception of new Policy	**2nd September 2026**	**Named Responsibility**	
Date of Policy Adoption by Governing Body		Resources – designated to the HT	
Policy Review		September 2027	

Contents

1. Introduction and Aims

Information and communications technology (ICT) is an essential part of teaching, learning, administration, and safeguarding within the school. This policy establishes the responsibilities, expectations and standards for all users, including staff, pupils, governors, volunteers, contractors and parents/carers. It ensures compliance with statutory duties, promotes safe and effective use of technology, and protects the school community from online risks, cyber threats and misuse of ICT resources.

2. Relevant Legislation and Guidance

This policy aligns with key UK legislation and statutory guidance governing data protection, online safety, communications monitoring, safeguarding and lawful handling of digital information within educational settings. It ensures that all ICT practices comply with national expectations and legal duties required of schools.

• Data Protection Act 2018, UK General Data Protection Regulation (UK GDPR) and the Data (Use and Access) Act 2025: These define lawful bases for processing personal data, ensuring confidentiality, integrity and accountability in all digital systems.
• Computer Misuse Act 1990: Sets criminal offences for unauthorised access, system interference and malicious activity.
• Human Rights Act 1998: Ensures monitoring and ICT controls respect privacy and proportionality expectations.
• The Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000: Enables schools to monitor communications for security, safeguarding and operational purposes.
• Education Act 2011 and Education and Inspections Act 2006: Allow schools to search, screen and confiscate devices where misuse is suspected, including digital content.
• Freedom of Information Act 2000: Governs public access to recorded school information, including digital documents.
• Keeping Children Safe in Education (KCSIE) 2026: Requires schools to maintain effective filtering, monitoring and safeguarding processes to protect pupils online.
• DfE Meeting Digital and Technology Standards in Schools (incl. cyber security standards): Sets expectations for secure systems, robust authentication, cyber hygiene and incident management.
• National Cyber Security Centre (NCSC) ‘Cyber Security for Schools’: Recommends best-practice technical controls, threat mitigation, and secure operational procedures.

These frameworks collectively ensure that ICT governance remains lawful, safe and effective, and they inform every section of this policy.

3. Definitions

For clarity and consistency, the following definitions apply throughout this policy. These terms are essential for understanding user expectations, monitoring arrangements, safeguarding requirements, and lawful ICT operation within the school.

• ICT Facilities: All hardware, software, systems, networks, cloud services, online platforms, communication tools, and school-managed digital devices. This includes laptops, tablets, desktop computers, servers, storage, email, learning platforms, and emerging technologies.
• Users: Anyone authorised to use school ICT systems, including staff, pupils, governors, volunteers, contractors, visitors, and third-party professionals.
• Personal Use: Any use of school ICT systems not directly related to teaching, learning, administration, safeguarding, or authorised school activity.
• Authorised Personnel: Staff designated to manage, monitor, support or maintain ICT systems, such as ICT managers, network technicians, data protection officers or senior leaders.
• Materials: Any digital content created, stored or transmitted using school ICT systems, including documents, photos, videos, emails, logs, messages, AI-generated outputs, and online posts.
• Monitoring Tools: Systems used to track, filter and record ICT use for safeguarding and compliance, such as filtering software, audit logs, device management systems or safeguarding alert platforms.
• Artificial Intelligence (AI): Any automated or algorithmic system capable of generating text, images or predictions. This includes chatbots, generative AI tools and automated content creators. AI use must comply with all data protection and safeguarding requirements.
• Cyber Security Incident: Any event that threatens confidentiality, integrity or availability of school data or ICT systems. Examples include phishing attempts, malware infections, data breaches or unauthorised access.
• Filtering and Monitoring: Statutory safeguarding measures that block harmful content and record user activity to protect pupils and staff online. These systems operate in accordance with DfE digital standards and Telford & Wrekin cyber security expectations.

4. Unacceptable Use

• Accessing or sharing pornographic, obscene, sexually explicit or otherwise inappropriate material, including making or sharing nude or semi-nude images of children, whether described as consensual or non-consensual, and including digitally altered, synthetic, AI-generated, deepfake or 'deep nude' imagery. Any such incident involving a child will be treated as a safeguarding concern and managed in line with the school's Child-on-Child Abuse Policy and current UKCIS guidance.

5. Staff (including governors, volunteers, and contractors)

Staff must use only school-approved AI tools and must use them safely, ethically and lawfully. Any use must comply with safeguarding, copyright, intellectual property and data protection requirements. Staff must:

5.1 Duty to Report

Staff must immediately report:

• Inappropriate content or suspicious online behaviour.
• Cyber security concerns, phishing attempts or unusual device activity.
• Data breaches or concerns relating to GDPR.
• Safeguarding concerns, following the school's procedures.

6. Pupils

Any AI-assisted work must be declared to staff where required and must follow the school's Artificial Intelligence & Emerging Educational Technologies Policy. AI must support learning rather than replace pupils' own thinking, creativity or assessed work.

7. Parents and Carers

Parents and carers play a vital role in supporting safe, respectful and responsible use of ICT within the school community. Their conduct online and offline directly influences pupil behaviour, safeguarding culture and the effectiveness of digital communication. This section outlines expectations for parents and carers when engaging with school ICT platforms, staff, pupils and the wider online environment.

7.1 Access to ICT Facilities and Materials

Parents and carers do not normally have access to school ICT systems. Access may be granted where a parent or carer is acting in an official capacity (e.g., volunteer, PTA role). All access must:

• Be formally authorised by the headteacher.
• Comply fully with this Acceptable Use Policy.
• Never be used to access confidential or sensitive information without permission.

7.2 Communicating with the School Online

Parents and carers must communicate respectfully and appropriately when using the school's online channels, including email, messaging platforms and social media. Expectations include:

• Using official channels to contact the school with queries or concerns.
• Avoiding the use of aggressive, abusive or disrespectful language towards staff or other families.
• Understanding that staff may not respond outside working hours.
• Recognising that safeguarding or sensitive matters should not be raised publicly online.

• Use online platforms to harass, intimidate or defame members of the school community, or to disclose confidential or safeguarding information. Concerns about the school should normally be raised through the school's published complaints or safeguarding procedures.

8. Data Security

Data security is essential for protecting pupils, staff and school operations. The school follows strict measures to ensure that all ICT systems, accounts and personal data remain secure and compliant with legislation and local authority requirements. All users must adhere to the expectations in this section.

8.1 Passwords

All users must create strong, unique passwords. Passwords must:

• Be kept confidential and never shared.
• Follow school-defined complexity standards.
• Not be reused across accounts or external services.
• Be changed immediately if compromise is suspected.

Staff must use the school's approved password manager where required. Pupils' passwords must be stored securely by staff.

8.2 Software Updates, Firewalls and Anti-Malware

All devices connected to the school network must:

• Install updates promptly to reduce security vulnerabilities.
• Use approved anti-malware protection.
• Not have security features disabled.
• Not install unauthorised software without approval.

All downloaded files must be checked for security risks before opening.

8.3 Data Protection

Personal data must be handled in line with UK GDPR, the Data Protection Act 2018, the Data (Use and Access) Act 2025 and the school's Data Protection Policy.

Users must:

• Only access data they are authorised to view.
• Not store personal data on unapproved devices or cloud services.
• Use encrypted storage/devices for sensitive data when required.
• Report any suspected breaches immediately.

8.4 Access Rights and Permissions

Access to systems, files and devices is role-based. Users must:

- Use only the permissions they have been assigned.
- Report unexpected or inappropriate access immediately.
- Log out and lock devices when not in use.
- Shut down devices at the end of each day.

8.5 Encryption

The school ensures appropriate encryption on all devices and systems. Staff may only remove personal data from the premises using encrypted, approved devices. Encryption must not be disabled.

8.6 Cyber Security Standards

The school aligns with national digital standards and Telford & Wrekin's Cyber Security Policy. Users must:

- Follow cyber security training and guidance.
- Recognise phishing attempts and suspicious emails.
- Report cyber concerns immediately.
- Avoid connecting unapproved devices to the school network.

These measures ensure resilience against threats such as ransomware, malware and unauthorised access.

9. Protection from Cyber Attacks

The school is committed to protecting its systems, data and users from cyber threats. Cyber security is a shared responsibility, requiring vigilance, training, and adherence to technical and procedural controls. This section incorporates all requirements from national standards, NCSC best practice, and the Telford & Wrekin Cyber Security Policy.

9.1 Training and Awareness

All staff, governors and volunteers will receive annual cyber security training. Training includes:

- Recognising phishing, social engineering and spoofing attempts.
- Understanding malware, ransomware and unsafe downloads.
- Safe password practices and multi-factor authentication (MFA).
- Secure device handling and physical security.
- Avoiding malicious websites and untrustworthy links.

New staff receive cyber training as part of their induction.

9.2 Recognising Cyber Threats

All users must be vigilant for signs of cyber compromise, including:

- Unexpected password prompts or MFA alerts.
- Slow or unusual device behaviour.
- Suspicious emails requesting account access or financial details.
- Alerts from filtering or monitoring tools.

Users must report concerns immediately.

9.3 Technical Controls

The school implements multi-layered technical protections, including:
• Firewalls and secure network segmentation.
• Anti-malware and endpoint detection tools.
• Email filtering and anti-phishing protection.
• Forced updates and patching across devices.
• Encrypted backups stored securely offsite or in cloud systems.
• Role-based access control and account audits.

9.4 Device and Remote Access Security

All remote access must use a school-approved secure method (e.g., VPN). Users must:
• Avoid storing data on personal devices.
• Use MFA where available.
• Ensure home networks are password-protected.
• Report any unusual login notifications.

9.5 Supply Chain and Vendor Security

Suppliers of digital services must meet cyber security expectations. The school will:
• Require suppliers to declare cyber security standards.
• Prefer suppliers with Cyber Essentials or equivalent certification.
• Review contracts for data handling and breach reporting obligations.

9.6 Backups

The school performs frequent backups to ensure continuity in case of data loss. Backups:
• Occur at least daily.
• Are stored securely (e.g., encrypted cloud or offline storage).
• Are tested regularly to confirm data recovery reliability.

9.7 Incident Response

The school maintains and regularly tests an incident response plan. It includes:
• Roles and responsibilities during a cyber incident.
• Communication arrangements if systems are unavailable.
• Procedures for reporting incidents to Action Fraud.
• NCSC ‘Exercise in a Box’ simulations.
Major incidents are escalated to Telford & Wrekin ICT Security.

9.8 Prohibited Actions

Users must never:
• Pay ransom demands.
• Attempt to hide or ignore suspicious activity.
• Install unauthorised software.
• Disable security features.
Such actions place the school at significant risk.

10. Internet Access

The school provides secure, filtered and monitored internet access to support teaching, learning and operational activities. Internet access is a privilege, not a right, and all users must follow the

expectations in this section to maintain a safe online environment.

10.1 School Internet Provision

The school's internet connection is protected using enterprise-grade filtering and monitoring systems. These systems:

- Block harmful, illegal or inappropriate content.
- Record user activity for safeguarding and compliance.
- Provide real-time alerts to designated safeguarding staff.
- Meet DfE filtering and monitoring standards.

Filtering is not infallible. Users must report any inappropriate content immediately.

10.2 Wi-Fi Network Structure

The school maintains separate secure Wi-Fi networks for:

- Staff – full access to approved systems and educational resources.
- Pupils – access suitable for learning, restricted through filtering.
- Visitors – limited, time-bound access where authorised.

Only authorised users may connect to the school's Wi-Fi. Staff must not share credentials with others.

10.3 Pupil Use of the Internet

Pupils may access the internet for learning purposes under staff supervision. They must:

- Use search engines and learning platforms responsibly.
- Avoid attempting to bypass filters or access restricted content.
- Report concerns immediately.

Use of the internet during unsupervised times is subject to monitoring controls.

10.4 Parent/Visitor Internet Access

Parents and visitors may only use school Wi-Fi where explicitly authorised. Authorisation is granted only when:

- A visitor requires internet access for a planned activity.
- A parent is volunteering in an official capacity.

All users must follow this Acceptable Use Policy when using school Wi-Fi.

10.5 Reporting Issues

All users must report:

- Inappropriate or harmful websites not blocked by filters.
- Slow or unusual network behaviour.
- Suspicious pop-ups or redirects.

Reports should be made to the ICT Manager or designated safeguarding staff.

10.1.1 Annual filtering and monitoring review

In accordance with KCSIE 2026 and the DfE Filtering and Monitoring Core Standard (updated June 2026), the effectiveness of the school's filtering and monitoring provision will be reviewed at least once every academic year. The review will involve the senior leader responsible for filtering and monitoring, the DSL, IT support and the responsible governor.

The review will consider the school's pupil risk profile, including age, SEND and EAL; use of generative AI; relevant safeguarding incidents; teaching requirements; BYOD or personal-device arrangements; and whether systems can appropriately address real-time, dynamic, personalised and AI-generated content.

Filtering and monitoring checks will be carried out and recorded from both safeguarding and technical perspectives. Records will identify when each check took place, who completed it, what was tested and any resulting action. New devices and services will be checked before deployment.

11. Monitoring and Review

The headteacher and designated ICT/digital lead, working with the DSL and IT support, oversee ongoing monitoring of:
• Artificial Intelligence & Emerging Educational Technologies Policy

12. Related Policies

This ICT and Internet Acceptable Use Policy should be read alongside the following school and local authority policies. Together, they provide a comprehensive framework for safeguarding, data protection, cyber security, and responsible digital behaviour.

• Safeguarding and Child Protection Policy – outlines statutory safeguarding duties and digital safety expectations.
• Online Safety Policy – provides detailed guidance on pupil online behaviour, filtering, monitoring and safe platform use.
• Data Protection Policy – establishes procedures for lawful data handling in line with UK GDPR and the Data Protection Act 2018.
• Staff Code of Conduct – sets professional expectations for staff behaviour, including communication and IT use.
• Behaviour Policy – outlines pupil behaviour standards, sanctions and expectations relating to online conduct.
• Mobile Phone / Smart Device Policy – defines expectations for staff and pupil use of personal devices (where applicable).
• Remote Learning Policy – covers secure and safe digital learning practices during remote or hybrid education.
• Telford & Wrekin Cyber Security Policy – provides mandatory local authority cyber standards that all users must follow.
• Artificial Intelligence & Emerging Educational Technologies Policy – provides the framework on responsible AI usage.

Appendix 1 – Staff, Governor and Volunteer Acceptable Use Agreement 2026–27

This annual acknowledgement summarises the key expectations in the High Ercall Primary School ICT and Internet Acceptable Use Policy. It does not replace the full policy.

• I will use school technology, accounts, networks and communications responsibly, professionally and primarily for authorised school purposes.

• I will protect passwords, use multi-factor authentication where provided, lock devices when unattended and immediately report suspected compromise, loss or theft.

• I will use official school systems for professional communication and will not use personal email, messaging or social-media accounts for confidential school business.

• I will not access, create, store or share illegal, harmful, extremist, discriminatory, pornographic or otherwise inappropriate content, and I will immediately report safeguarding concerns.

• I will not bypass or attempt to disable filtering, monitoring, security controls or device-management systems.

• I understand that school systems and school-managed devices may be filtered and monitored for safeguarding, security and compliance purposes.

• I will handle personal and special-category data in accordance with the school's Data Protection Policy and will report actual or suspected data breaches immediately.

• I will only use school-approved AI tools. I will not enter identifiable pupil, staff, safeguarding, special-category or confidential information into unapproved AI systems, and I remain responsible for checking the accuracy and appropriateness of AI-assisted work.

• I will not create, request, share or manipulate nude or semi-nude imagery of children, including AI-generated, deepfake or 'deep nude' content. I will follow safeguarding procedures immediately if I become aware of such content.

• I will maintain professional boundaries online and will not engage in online activity that could compromise safeguarding, confidentiality or my professional responsibilities.

• I understand that breaches may result in safeguarding action, restriction of access, disciplinary action and/or referral to external agencies where appropriate.

Name: _____

Role: _____

Signature / electronic acknowledgement: _____

Date: _____

Key guidance for 2026–27

• Department for Education, Keeping Children Safe in Education 2026 (in force from 1 September 2026).

• Department for Education, Filtering and Monitoring Core Standard (updated June 2026).

• Department for Education, Cyber Security Core Standard (updated June 2026).

• Department for Education, Data Protection in Schools (updated July 2026), including the Data (Use and Access) Act 2025 changes.

• Department for Education, Generative AI: Product Safety Standards (updated January 2026).

• UK Council for Internet Safety, Sharing nudes and semi-nudes: advice for education settings working with children and young people.