



Acceptable Use Policy

Ratified by Governing Body

Review: September 2027

PURPOSE & SCOPE

Digital technology is an important part of teaching, learning and communication at Herrick Primary School. This policy sets out how school technology, devices, accounts, systems and information should be used safely, responsibly and appropriately by staff, governors and pupils. It also sets out the expectations for parents and carers when accessing or using school systems and online services.

The purpose of this policy is to:

- ensure that everyone understands their responsibilities when using school technology;
- promote responsible, respectful and appropriate use of devices, systems and online services;
- protect school accounts, devices, networks and systems from misuse or unauthorised access;
- ensure that personal, confidential and school information is handled securely;
- set clear expectations around the use of email, communication platforms, personal devices and social media;
- provide clear expectations for the appropriate use of artificial intelligence (AI);
- ensure that concerns, mistakes or suspected cyber-security incidents are reported promptly; and
- provide clear Acceptable Use Agreements for staff, governors, pupils and parents/carers within the appendices.

While this policy focuses on operational and security rules, safeguard-related risks—such as cyberbullying, harmful content, online safety education, and filtering/monitoring arrangements—are covered separately in the Online Safety Policy. This document should be read alongside the Online Safety Policy, Staff Code of Conduct, Child Protection and Safeguarding Policy, Data Protection Policy, and Social Media Policy.

RELATED LEGISLATION, GUIDANCE AND SCHOOL POLICIES

This policy should be applied alongside current legislation and guidance relevant to the use of school technology, including:

- Computer Misuse Act 1990.
- Copyright, Designs and Patents Act 1988.
- Data Protection Act 2018 and UK GDPR, as amended by the Data (Use and Access) Act 2025.

- Equality Act 2010.
- Education Act 2002 and Keeping Children Safe in Education 2026 where use of technology raises a safeguarding concern.
- DfE cyber-security standards and filtering and monitoring standards for schools and colleges.

It should also be read alongside the school's Online Safety Policy, Child Protection and Safeguarding Policy, Staff Code of Conduct, Data Protection Policy, Behaviour Policy, Social Media Policy and Privacy Notices.

ACCESS TO SCHOOL SYSTEMS AND ACCOUNTS

- Access to school networks, Wi-Fi, accounts, devices, cloud services and software is provided for authorised school purposes.
- Users must only access accounts, files, systems and information they are authorised to use.
- Passwords and authentication codes must be kept secure and must not be shared.
- Users must not use another person's account or allow another person to use their account.
- Multi-factor authentication must be used where it is provided.
- Devices must be locked or signed out when left unattended.
- Access may be withdrawn or restricted where there is a security, safeguarding, conduct or operational concern.

SCHOOL DEVICES, SOFTWARE AND EQUIPMENT

- School equipment must be handled carefully and used for its intended purpose.
- Users must not deliberately damage, alter or interfere with devices, networks or settings.
- Software, applications, browser extensions and other programs must not be installed without appropriate authorisation.
- Users must not connect unauthorised equipment or storage devices to school systems where this is prohibited by school or IT procedures.
- Lost, stolen, damaged or malfunctioning equipment must be reported promptly.
- School devices taken off site remain subject to this policy.

INTERNET AND NETWORK USE

- Internet and network access must be used responsibly and for authorised educational, professional or school purposes.
- Users must not attempt to bypass or disable school security, access controls, filtering or monitoring, including through unauthorised VPNs, proxies or similar tools.
- Users must not knowingly access, download, create, store or distribute illegal or inappropriate material using school systems.

- Users must not use school systems for unlawful activity, gambling, fraud, commercial activity not authorised by the school, or activity likely to damage the school's systems or reputation.
- Users must report accidental access to inappropriate material or a suspected security problem rather than attempting to investigate or conceal it.

EMAIL, MESSAGING AND COMMUNICATION

- School business must be conducted through school-approved communication systems.
- Users must communicate respectfully and professionally.
- Staff must not use personal email or personal messaging accounts to send confidential school information or pupil personal data.
- Staff must not communicate privately with current pupils through personal social-media, gaming or messaging accounts and must adhere to the school's Social Media Policy at all times when using social media in a personal or professional capacity.
- Users must not send messages that are threatening, discriminatory, abusive, defamatory, knowingly false or otherwise inappropriate.
- Unexpected attachments, links, QR codes, requests for passwords or unusual payment/login requests should be treated cautiously and reported when suspicious.

DATA, CONFIDENTIALITY AND PRIVACY

- Personal and confidential information must only be accessed where required for the user's role or learning.
- School data must only be stored, transferred and shared using authorised systems.
- Personal data must not be stored in personal email accounts, unauthorised personal cloud storage or other unapproved services.
- Users must take reasonable steps to prevent unauthorised people seeing confidential information on screens, printouts or devices.
- Printing containing personal or confidential information must be collected promptly and disposed of securely when no longer required.
- Suspected loss, disclosure or unauthorised access to personal data must be reported promptly in accordance with the school's data-breach procedure.

PHOTOGRAPHS, VIDEO AND AUDIO

- Staff must use school-authorised devices and systems when creating or storing photographs, video or audio of pupils, unless an exceptional arrangement has been explicitly authorised.
- Images and recordings must only be used for authorised school purposes and in line with the school's Privacy Notices and consent arrangements.

- Users must not copy, publish or share images or recordings from school systems without authorisation.
- Specific consent choices are dealt with separately in Appendix B where consent is the appropriate lawful basis.

GENERATIVE ARTIFICIAL INTELLIGENCE

- Only school-approved AI tools may be used for school business or pupil learning.
- Users must follow the age requirements and terms of use of any approved AI service.
- Confidential information, safeguarding information, special-category data or identifiable pupil information must not be entered into an unapproved AI service.
- Staff remain responsible for checking the accuracy, suitability, bias, copyright and quality of AI-assisted work before using or sharing it.
- AI must not be used to impersonate another person, fabricate evidence, complete work dishonestly or create material that breaches school rules or the law.
- Pupils may use AI in school only when a member of staff has authorised its use.

COPYRIGHT AND INTELLECTUAL PROPERTY

- Users must respect copyright, licensing and intellectual-property rights.
- Software, images, music, video, text and other digital material must not be copied, downloaded or distributed unlawfully.
- Sources should be acknowledged where appropriate and pupils must not present another person's or an AI system's work as entirely their own where this would be dishonest.

PERSONAL DEVICES AND REMOVABLE MEDIA

- Personal devices may only be connected to or used with school systems in accordance with school procedures.
- Personal devices must not be used to store confidential school information unless explicitly authorised and appropriately secured.
- Removable media such as USB drives must only be used where permitted and must meet school security requirements.
- Staff use of personal mobile phones, smart watches and other personal devices must comply with the Staff Code of Conduct, Social Media Policy and any school mobile-device procedures.

CYBER SECURITY AND REPORTING

- Users must be alert to phishing, fake login pages, malicious attachments, QR-code scams and other attempts to obtain passwords, money or information.
- Suspected compromised accounts, malware, ransomware, suspicious emails, lost devices and other cyber incidents must be reported promptly.

- Users must not attempt to investigate a cyber incident beyond the actions they have been instructed to take.
- Where a technology-use concern is also a safeguarding concern, the school's Online Safety and Child Protection procedures must be followed immediately.

MONITORING AND PRIVACY

The school may monitor activity on school networks, accounts and managed devices for safeguarding, cyber-security, operational and lawful purposes. Users must not attempt to interfere with monitoring. The detailed safeguarding arrangements for filtering and monitoring are set out in the Online Safety Policy, while privacy information explains what is monitored, why it is monitored, who can access relevant information and how it is retained.

PARENTS AND CARERS

- Parents/carers should use official school communication routes for school matters, communicate respectfully with staff and the wider school community, and follow any school expectations relating to social media and online communication.
- Parents/carers should not use school-provided access, accounts or information in a way that compromises another person's privacy or the security of school systems.
- Parents/carers are asked to read and discuss the pupil agreement with their child.
- Where consent is required for a particular optional use, the school will seek it separately and record the parent's/carer's choice.

BREACHES OF THIS POLICY

Breaches will be considered according to the circumstances and may result in restricted or withdrawn access, action under the Behaviour Policy, Staff Code of Conduct or disciplinary procedures, data-protection action, or referral to the DSL, IT support, the Data Protection Officer or an external authority where appropriate.

Nothing in this policy replaces the school's safeguarding procedures. A concern about a child's welfare must be reported through safeguarding procedures without delay.

REVIEW

This policy will be reviewed at least annually and sooner where there is a significant change to technology, cyber-security requirements, legislation, guidance or school systems.

APPENDIX A - STAFF AND GOVERNOR ACCEPTABLE USE AGREEMENT

I confirm that I have read the school's Online Safety Policy and Acceptable Use Policy and understand that the detailed safeguarding expectations for online safety are contained in the separate Online Safety Policy.

I agree that I will:

- Use school technology professionally, lawfully and primarily for authorised school purposes.
- Keep usernames, passwords and authentication methods secure and never allow a pupil or another person to use my account.
- Use multi-factor authentication where provided and report suspected account compromise immediately.
- Lock or sign out of devices when unattended.
- Use school-approved email, cloud storage, communication and collaboration systems for school business.
- Handle pupil, parent, staff and governor information in accordance with UK GDPR, the Data Protection Act 2018, the Data (Use and Access) Act 2025 and school policy.
- Only access personal data that I need for my role.
- Report safeguarding concerns arising online immediately to the DSL/deputy through the school's agreed process.
- Report phishing, malware, suspicious links, lost/stolen devices, security incidents and suspected data breaches promptly.
- Use photographs and video of pupils only on authorised school devices and in accordance with school privacy, consent and safeguarding arrangements.
- Maintain professional boundaries in all online communication and social media use.
- Use approved AI tools only in accordance with school guidance, age restrictions, safeguarding expectations and data-protection requirements.
- Check AI-generated output for accuracy, bias, suitability, copyright and safeguarding concerns before relying on or sharing it.
- Maintain appropriate supervision of pupils using devices and understand that filtering does not replace supervision.
- Report unsuitable content, filtering failures, monitoring concerns or unreasonable restrictions to the appropriate member of staff.
- Follow licensing and copyright requirements when downloading, copying, creating or sharing material.
- I will treat online bullying, grooming, sexual harassment, sextortion, cyberflashing, impersonation, doxxing, discriminatory abuse, deepfakes and harmful AI-generated content as potential safeguarding concerns and report them appropriately.
- I will be alert to phishing, QR-code phishing, fake login pages, malicious attachments, impersonation, payment scams and social-engineering attempts.
- I will verify unusual or sensitive requests through a trusted separate channel before acting.

- I will report suspected compromised accounts, malware, ransomware, data loss or other cyber incidents promptly.

I will not:

- Share passwords or authentication codes.
- Use a pupil account or allow pupils to use staff credentials.
- Attempt to bypass filtering, monitoring, firewalls or other security controls, including through VPNs, proxies or unauthorised software.
- Install software, applications, browser extensions or hardware without appropriate authorisation.
- Store school personal data on unauthorised personal devices, personal cloud storage or unencrypted removable media.
- Use personal email or personal messaging/social-media accounts to communicate confidential school information.
- Communicate privately with current pupils through personal social-media, gaming or messaging accounts.
- Photograph or record pupils on a personal device unless an exceptional arrangement has been explicitly authorised.
- Enter safeguarding information, confidential information, special-category data or identifiable pupil information into an unapproved AI service.
- Use AI to make safeguarding decisions or as a substitute for my professional judgement.
- Access, create, download, store or share illegal, discriminatory, sexually explicit, extremist, abusive or otherwise inappropriate material.
- Post confidential school information, pupil information, images or opinions online in a way that breaches professional duties or could place a child at risk.
- Investigate a child's private online activity independently; I will preserve relevant information and refer the concern to the DSL.

MESSAGING AND SOCIAL MEDIA

School business must use approved communication channels. Personal WhatsApp, Signal, Telegram, Messenger, Instagram direct messages or similar services must not be used to share pupil information, safeguarding information or other confidential school data. Where the school authorises a specific platform or account for a defined purpose, its use must follow school policy and data-protection requirements.

FILTERING AND MONITORING

I understand that school networks, accounts and managed devices may be filtered and monitored for safeguarding, cyber-security, operational and lawful purposes. Monitoring will be proportionate and handled in accordance with the school's privacy information and data-protection arrangements. I will not attempt to disable or circumvent these controls.

GENERATIVE AI

- I will use only AI services approved for the relevant school purpose.
- I will not assume AI output is accurate or appropriate.
- I remain responsible for resources, communications, assessments or other work I produce with AI assistance.
- I will not upload identifiable pupil work, photographs, recordings or personal data to an AI tool unless that use has been specifically approved.
- I will report harmful, sexualised, abusive, deceptive or otherwise concerning AI-generated content involving pupils through safeguarding procedures.

ACCEPTANCE

I understand that breaches may lead to withdrawal of access, safeguarding action, disciplinary action and/or referral to external authorities where appropriate.

Name: _____

Role: _____

Signature: _____ Date: _____

APPENDIX B – PUPIL AND PARENT ACCEPTABLE USE AGREEMENT

I confirm that I have read the school's Online Safety Policy and Acceptable Use Policy and understand that the detailed safeguarding expectations for online safety are contained in the separate Online Safety Policy.

For parents and carers

Technology is an important part of learning at Herrick Primary School. The school teaches pupils how to use devices and online services safely, respectfully and responsibly. School internet access and managed devices are filtered and monitored as part of the school's safeguarding arrangements.

This agreement is designed to be discussed with your child. It does not replace the school's Online Safety Policy, Child Protection and Safeguarding Policy or Behaviour Policy.

Our pupil rules: SAFE - KIND - SMART - TELL

SAFE

- I will keep my password private and will only use my own account.
- I will not share my full name, address, phone number, passwords or other private information online unless a trusted adult at school tells me it is safe and necessary.
- I will not try to get around the school's filters, security settings or monitoring.
- I will only use websites, apps, games, AI tools and online services that my teacher has allowed me to use.
- I will never arrange to meet someone I only know online. If anyone online asks to meet me, I will tell a trusted adult straight away.

KIND

- I will be respectful when I write, message, comment, create or share things online.
- I will not use technology to bully, frighten, embarrass, threaten or upset someone.
- I will not take, change or share a photo, video or recording of another person without permission.
- I will tell an adult if I see someone else being treated badly online.

SMART

- I know that not everything online is true.
- I will think carefully before I click links, open files or respond to messages.
- I will only download or upload things when my teacher says I can.
- I will respect other people's work and will not pretend that somebody else's work is my own.
- If I use an AI tool in school, I will only use it when my teacher allows me to and I will remember that AI can make mistakes.
- I will not type private information about myself or another person into an AI tool.

TELL

- If I see something online that worries, frightens or confuses me, I will tell a trusted adult.
- If somebody asks me for a picture, private information or to keep an online conversation secret, I will tell a trusted adult.
- If I accidentally open something inappropriate, I will close/minimise it if I can and tell an adult. I know I will not be in trouble for reporting it.
- If I receive an unkind or worrying message, I will not reply. I will show it to a trusted adult.
- I know that I can speak to my teacher, teaching assistant, DSL/deputy DSL or another trusted adult in school.

School devices and monitoring

I understand that the school may check activity on school accounts, networks and managed devices to help keep people safe and protect school systems. I will use school equipment carefully and tell an adult if something is damaged or not working properly.

Parents and carers

- Please discuss these rules with your child and reinforce safe, respectful and age-appropriate online behaviour at home.
- Please report online concerns that may affect your child's safety, wellbeing or school life to the school.
- Please understand that the school uses proportionate filtering and monitoring but no technical system can remove every online risk; education, supervision and reporting remain essential.
- Consent for specific uses of pupil images, video or publication will be managed through the school's separate privacy/consent arrangements rather than this agreement.

Agreement

Pupil: I have discussed these rules and agree to use school technology safely, kindly and responsibly.

Pupil name: _____ Year: _____

Pupil signature (where appropriate): _____ Date: _____

Parent/carers: I have read and discussed this agreement with my child.

Parent/carers name: _____

Signature: _____ Date: _____