



Acceptable Use Policy for Adults

Date of document: September 2026
Date for review: September 2028
Lead reviewer: Deputy Headteacher
Approval by: Governing Body

All staff, governors, and volunteers at Swallowfield Primary School must be aware of this agreement and agree to follow it as a condition of their employment or involvement with the school. Failure to do so may result in disciplinary action.

It is vital that the school fulfils its legal obligations under the **UK General Data Protection Regulation (UK GDPR)**, the **Data Protection Act 2018**, the **Freedom of Information Act (2000)**, and the latest Department for Education statutory guidance (**Keeping Children Safe in Education 2026**). This Acceptable Use Policy (AUP) ensures that all adults are aware of their responsibilities regarding data protection, cybersecurity, and safeguarding.

1. Data to Which This Policy Applies

- **Personal Data:** Any information relating to an identified or identifiable living individual (e.g., name and address, name and date of birth).
- **Special Category (Sensitive) Data:** Data that could cause harm, distress, or embarrassment if made public or accessed without authorization (e.g., Special Educational Needs & Disabilities (SEND) records, racial/ethnic origin, medical data, payroll/bank details, phone numbers, or safeguarding information).
- **Confidential Data:** Other sensitive school records, including performance management documents, governance files, and commercial contracts.

2. Security of paper-based data

- Staff are responsible for ensuring that paper records containing personal or confidential data remain secure at all times.
- **On-Site:** Keep physical data locked away when not in use and out of sight or reach of pupils, visitors, or unauthorised personnel.
- **Off-Site / In Transit:** Paperwork containing personal data should only be taken off-site when strictly necessary. It must remain with you at all times during transit and be stored securely (e.g., in a locked bag or cupboard).
- Special category/sensitive records (e.g., Child Protection/CPOMS logs, SEND, medical, or payroll records) **must never be removed from the school site** unless explicitly authorized by the Headteacher.
- Paper records must **never be taken outside of the UK**.

- **Disposal:** All paper records containing personal data must be securely shredded once no longer required, in line with the school's Data Retention Schedule. (Note: Child protection records must be retained for longer statutory periods).

Security of electronic data

- **Passwords & Access:** You must use strong passwords/passphrases for all school accounts (email, network, MIS). Never share your passwords with pupils, other staff members, or external parties. Where Multi-Factor Authentication (MFA) is enabled, it must be used.
- **Screen Locking:** Always lock (Windows Key + L) or log out of your computer/device when leaving it unattended, even for a short period. You are legally and professionally accountable for any activity occurring under your credentials.
- **Data Storage & Removable Media:** Personal data must be stored on approved school cloud platforms (e.g., school server, Google Workspace) and **not** on local laptop drives or personal devices.
- Unencrypted USB drives are prohibited. If an encrypted USB drive is used, it must be authorised by the Headteacher, physically secured, and never taken outside the UK.
- School data must **never** be copied or downloaded onto home computers or personal unmanaged devices.
- **Photography & Media:** Photos and videos of pupils must **only** be taken using school-owned devices. Any exceptions must be explicitly authorised in advance by the Headteacher or Deputy Headteacher. Images must be uploaded to secure school storage and deleted from device local storage promptly.
- **AI Tools:** Staff must not input any pupil personal data, sensitive information, or confidential school data into generative AI tools (e.g., free ChatGPT).
- **Account Termination:** Upon termination of contract/employment, access to all school network accounts, emails, remote systems, and cloud storage will be disabled. Any physical hardware or encrypted devices must be returned to the office.

Release and data sharing

- Staff may share relevant information regarding pupils with colleagues when necessary for the performance of their professional duties and in the best interests of the child. (Exception: Where the Senior Leadership Team (SLT) has explicitly instructed that specific information remains confidential).
- **External Data Sharing:** When sharing data with external organizations (e.g., local authorities, secondary schools, social care), staff must verify the legitimate legal basis and identity of the recipient. School-to-school pupil data transfers must be processed by administrative staff using secure transfer networks (e.g., CTF / DfE Secure Access).
- **Staff Data Access:** Access to staff personal data (e.g., personnel files, contracts, pay scales) is restricted to personnel authorised by the Headteacher.
- **Communication Channels:** All professional correspondence must be conducted via your official school-provided email account. Staff must not use personal email accounts or personal messaging apps for school business.
- **Data Breaches:** The school takes data breaches very seriously. If you suspect or become aware of a personal data breach (e.g., sending an email to the wrong recipient, lost device, lost paperwork), you **must report it immediately** to the Headteacher.

Freedom of Information (FOI) and Subject Access Requests (SAR)

- Any member of staff or governor may receive a Subject Access Request (SAR) or Freedom of Information (FOI) request in writing or by email.
- If you receive such a request, you must forward it immediately to the Headteacher. Swallowfield Primary School has strict legal deadlines to respond (1 calendar month for SARs; 20 working days for FOI requests).
- Do not send a response yourself; await instruction from the Headteacher.
- **Professionalism:** Staff should be aware that email logs and internal electronic communications may be disclosable under a SAR or FOI request. All written communications must remain professional, objective, and respectful.

Appendix 1

The computer systems and internet infrastructure are owned by Swallowfield Primary and provided to staff to enhance teaching, research, administration, and school management. The school reserves the right to monitor internet access, network usage, and files stored on school systems to ensure pupil safety and network integrity.

By signing below, you agree to the following conditions:

- All internet and network activity must be professional and appropriate to educational and administrative purposes.
- Access must only be made via your authorised personal account credentials.
- Activity that threatens network security, bypasses filtering systems, or introduces malicious code/viruses is strictly forbidden.
- Using school systems for personal financial gain, gambling, personal social networking during working hours, political campaigning, or commercial advertising is forbidden.
- Copyright and intellectual property laws must be respected at all times.
- Posting anonymous messages, forwarding chain emails, or engaging in unapproved mass emailing is forbidden.
- Standard professional conduct applies to electronic communications; emails should maintain the same standards of tone and language as printed correspondence.
- Accessing, downloading, or sharing inappropriate, illegal, pornographic, offensive, or extremist material is strictly prohibited and constitutes gross misconduct.

Full name Post.....

Signed Date.....

Admin Approval (ICT Lead / Headteacher):

Access granted by Date