Sidcot School Acceptable Use Policy (Staff) 2026

1. Purpose and Scope

This policy sets out the standards for the acceptable use of Sidcot School's digital systems, networks, data and devices.

It applies to:

- All staff (teaching and non-teaching), contractors and volunteers
- All School systems, networks and accounts
- All School-owned and personal devices used for School business (BYOD)

This policy supports compliance with:

- Keeping Children Safe in Education (KCSIE)
- UK GDPR and Data Protection Act 2018
- National Cyber Security Centre (NCSC) guidance

2. Key Principles

Staff must use technology:

- Safely – protecting children and colleagues
- Lawfully – complying with all statutory obligations
- Professionally – maintaining appropriate conduct at all times
- Securely – protecting School systems and data

Staff are personally responsible for their use of digital technology and must read and sign this policy annually

3. Roles and Responsibilities

- **Head of IT Services**: security controls, system access, technical enforcement
- **Data Protection Lead (DPL):** GDPR compliance, data breaches, SARs
- **Designated Safeguarding Lead (DSL):** safeguarding concerns
- **All Staff**: compliance with this policy and reporting concerns promptly

4. Safeguarding and Professional Conduct

- Staff must only communicate with students via approved School systems

- Staff must not add or interact socially with current or former students under 21 years of age on personal social media without SMT approval. (See Staff Student Code Appendix 1)
- Digital communication must always be professional and appropriate.
- Personal mobile phones must not be used to contact students or take photos/videos.
- School provided devices must be used for trips where communication is required. Any student data including personal numbers must be deleted at the conclusion of the trip.
- Any safeguarding concern must be reported immediately to the DSL

5. Cyber Security Requirements

Staff must:

- Use strong passwords and Multi-Factor Authentication (MFA) must be used where available.
- Never share passwords
- Report any phishing or suspicious activity to itsupport@sidcot.org.uk immediately
- Lock devices when unattended.
- Only install approved software or hardware. All requests for new software/hardware must go through the Head of IT Services.
- Not attempt to investigate suspected cyber security incidents themselves or delete or alter potential evidence.

The School reserves the right to restrict access where devices or behaviour pose a security risk.

6. Data Protection and Information Handling

Staff must:

- Store School data only on approved systems.
- Use encrypted storage where required.
- Be familiar with and always abide by the UK GDPR and the Data Protection Act 2018, including the School's data classification and handling requirements.
- Never use unauthorized personal storage or cloud services
- Immediately report suspected data breaches to the Data Protection Lead at dpl@sidcot.org.uk

Subject Access Requests (SARs)

- Must be forwarded immediately to the DPL using dpl@sidcot.org.uk
- SARs can be in any format – they do not need to be digital, verbal requests are also valid

Failure to comply may result in disciplinary action.

7. Use of AI

Staff may only use AI tools that have been explicitly approved by the School. The Digital Strategy Lead can provide information on which tools can be used.

Staff must:

- Understand that AI outputs may be inaccurate or biased.
- Verify all AI-generated content before use, to ensure content does not promote stereotype, discrimination or inequality regarding protected characteristics.
- Retain full professional responsibility for any decisions, content or outputs produced using AI tools.
- Actively screen for “hallucinations” (convincingly written but entirely fabricated facts, fake citations or incurred data) before utilising AI-generated content in lessons or administrative work.

Ensure data is classified appropriately before use in any AI system and must not input Confidential, Sensitive or Safeguarding data into any AI tool unless explicitly approved. Co-Pilot is acceptable as it does not use the data input for training purposes. See Appendix 1 for classifications.

AI must not be used:

- For safeguarding decisions without human oversight
- In any way that compromises student welfare or data protection

8. Acceptable Use

Staff may:

- Use School systems for professional purposes
- Make limited personal use of School systems where this is reasonable and proportionate, provided that it takes place during breaks or outside core duties, does not affect work performance and does not create any risk or cost to the School.

Staff must:

- Treat digital technology equipment carefully and not act in any way that might cause damage
- Follow all security requirements.
- Ensure personal devices meet minimum security requirements (see BYOD section)

9. Prohibited Use

Staff must not:

- Accessing illegal, harmful or inappropriate content.
- Share or store School data via unauthorized channels
- Deliberately bypass or weaken security controls, including the use of VPNs, proxies or unauthorized authentication methods.
- Use systems for private business activities
- Use personal devices to photograph/video students
- Engage in behaviour that brings the School into disrepute
- Use School systems for gambling or political campaigning
- Use peer-to-peer software.
- Search for, or display, any material considered illegal or offensive.
- Publish anything to the Internet at School or via social media which causes offence or brings the School into disrepute as this may lead to disciplinary action.
- Use photos of students for external websites or promotion, unless the permission of the parents has been obtained. (See Digital Safety Policy 12.1)
- Open unexpected attachments or click suspicious links from unknown or unsolicited senders, as these are primary attack vectors.

10. Email and Communication Standards

Staff must:

- Staff must check email and Teams messages in line with role requirements
- Use School accounts for all School related communication.
- Ensure communications are professional and appropriate.
- Check recipients carefully before sending data
- Use BCC where appropriate
- Avoid sharing unnecessary personal information
- Only communicate with students using their School email account. Unless authorised to do so by the Head of IT Services eg Exam results. Failure of students to make use of the School email will not be deemed sufficient for authorisation of sending to a personal email address.
- Report any communication that is inappropriate, offensive, discriminatory, threatening, or raises safeguarding concerns.

11. Bring Your Own Device (BYOD)

Personal devices used for School work must:

- Be encrypted
- Use screen locking/password protection
- Be kept fully updated (OS and software)

- Have anti-virus / endpoint protection installed

The School reserves the right to verify device compliance with these requirements and to restrict or block access from non-compliant devices.

12. Remote Working

Staff must:

- Use secure Wi-Fi connections
- Protect devices and screens from unauthorized access
- Never leave devices unattended in public places
- Ensure that unauthorized individuals cannot access School systems or data

13. Monitoring

The School monitors the use of its IT systems, networks and devices to ensure:

- Safeguarding of students and staff
- Protection of School systems and data
- Compliance with legal and regulatory obligations

Monitoring may include, but is not limited to:

- Network and internet activity
- Email and communication systems (including Teams)
- File access, storage and transfer
- System access logs and authentication data

Monitoring is carried out:

- In accordance with UK GDPR and the Data Protection Act 2018
- Under the School's legitimate interests and legal safeguarding duties
- In a manner that is proportionate, necessary and reasonable

Staff should have a limited expectation of privacy when using:

- School devices
- School accounts
- School networks
- Personal devices used to access School systems (BYOD)

The School reserves the right to access, review and disclose data where necessary to:

- Investigate safeguarding concerns
- Investigate suspected breaches of this policy
- Respond to security incidents

- Comply with legal obligations or law enforcement requests

Monitoring will not be excessive and will only be conducted for legitimate purposes.

Failure to comply with this policy may result in monitoring records being used in disciplinary procedures.

14. Incident Reporting

Staff must report any of the following concerns as soon as possible, to the following staff:

- Safeguarding concerns → DSL
- Cyber/security issues → IT Support
- Data breaches → Data Protection Lead

Cyber security incidents must be reported, where possible, within one hour of discovery and staff must not attempt to investigate incidents themselves or delete evidence. Prompt reporting is essential to reduce risk.

15. Data Breaches

Staff must report:

- Mis-sent emails
- Lost devices
- Unauthorised access including unexpected password reset prompts, unusual network activity or receiving/sending unauthorised emails.
- Incorrect use of CC/BCC
- All suspected breaches using the MSP form here: Report a GDPR Breach

The School may need to report breaches to the ICO within 72 hours.

16. Training and Review

- Staff must complete annual training on safeguarding, data protection and cybersecurity
- Additional training may be required following policy updates or incidents
- This policy will be reviewed annually by the Board of Governors
- Staff must confirm acceptance each year

17. Breaches and Enforcement

Failure to comply with this policy may result in:

- Disciplinary action

- Loss of system access
- Referral to external authorities where appropriate

Serious breaches may constitute gross misconduct

18. Declaration

I confirm I have read and agree to this policy.

Name:

Signature:

Date:

Appendix 1

Classification	Description	Examples	Handling Requirements
Public	Information approved for public release	Website content, newsletters, published policies	May be shared freely. No special controls required.
Internal	Routine School information not intended for public disclosure	Staff communications, internal procedures	Share within School systems only. Do not publish externally without approval.
Confidential	Sensitive personal or operational data	Staff records, student academic data, emails containing personal data	Store only on approved systems. Do not share externally without authorisation. Use secure methods when sending.
Safeguarding / Highly Sensitive	Critical information relating to student welfare, protection or high-risk personal data	Safeguarding records, medical information, SEND data	Strictly limited access. Must only be shared with authorised staff on a need-to-know basis. Never input into AI tools or unapproved systems. Use secure storage and transfer methods at all times.