



Sidcot
Live Adventurously

Policy Name: Acceptable Use (Visitors)

Policy Number: 12.5

Date: 1 September 2026

1. Purpose

This policy sets out the expectations for all visitors using digital technology whilst on school premises, to ensure:

- Safeguarding of students and staff
 - Protection of personal data
 - Security of school systems and networks
 - Compliance with legal and regulatory requirements
-

2. Scope

This policy applies to:

- Use of **school-owned systems and networks**
 - Use of **personal devices** (phones, laptops, tablets, wearables, etc.)
 - Access to **school Wi-Fi or digital services**
-

3. General Responsibilities

All visitors must:

- Follow all school safeguarding, data protection, and IT security policies
 - Act in a professional manner consistent with the school's ethos
 - Seek guidance from a staff member if unsure about any activity
 - Report any concerns or incidents immediately (see Section 9)
-

4. Acceptable Use

Visitors may only use digital technology:

- For purposes directly related to their visit
 - In a manner that is lawful, respectful, and secure
 - Using authorised access methods provided by the school
-

5. Unacceptable Use

Visitors **must not**:

- Access or attempt to access **unauthorised systems or data**
 - Download, copy, or remove personal or confidential data without permission
 - Use school systems for:
 - Illegal activities
 - Offensive, inappropriate, or harmful content
 - Circumventing security controls (e.g. VPNs, proxies)
 - Introduce or connect **unapproved devices** (e.g. USB drives) to school systems
 - Share school information externally without written permission
-

6. Use of Personal Devices and Mobile Phones

- Personal devices must only be used in **designated or appropriate areas**, as directed by staff
 - Devices should be kept on **silent mode** where required
 - Use must not interfere with school operations or safeguarding
-

7. Images, Audio and Video

Visitors must not:

- Take photographs, audio recordings, or videos of students without **explicit prior permission**
- Capture staff or sensitive information without authorisation

Where permission is granted:

- Use must comply fully with the school's safeguarding and media policies
 - Images must not be stored, shared, or published outside agreed purposes
-

8. Social Media and Communication

Visitors must:

- Not contact students or families using personal communication channels
- Not share any information about students, staff, or the school on social media
- Maintain strict professional boundaries at all times

Any communication must take place through **school-approved channels only**.

9. Data Protection and Confidentiality

Visitors must:

- Comply with the **UK General Data Protection Regulation (UK GDPR)** and **Data Protection Act 2018**
- Treat all school-related information as confidential unless explicitly advised otherwise
- Not access, process, or store personal data unless authorised

Data must not be:

- Copied
 - Transferred to personal devices
 - Shared externally
-

10. Network and System Access

- Visitors must only use the **approved guest Wi-Fi** where provided
 - Access to internal systems is **restricted unless explicitly authorised**
 - All system use may be **monitored and logged** for security and safeguarding purposes
-

11. Security Requirements

Visitors must:

- Ensure devices are secure and protected (e.g. password, screen lock)
 - Not attempt to bypass security controls
 - Not install software or applications on school devices
-

12. Safeguarding Responsibilities

Visitors have a duty to:

- Act in a way that protects students from harm
 - Report any concerns about student safety or inappropriate technology use immediately
-

13. Incident Reporting

Any of the following must be reported immediately to a member of staff:

- Safeguarding concerns
- Suspicious or inappropriate technology use
- Data breaches or potential data loss
- Cyber security concerns (e.g. phishing, malware)

Where appropriate, concerns will be escalated to:

- Designated Safeguarding Lead (DSL)
 - IT Services
 - Senior Leadership Team
-

14. Monitoring and Enforcement

The school:

- Reserves the right to monitor and log all use of its systems and networks
 - May restrict or remove access at any time
 - Will take action in response to breaches, including:
 - Removal from premises
 - Reporting to relevant authorities (including police where necessary)
-

15. Legal Compliance

Visitors must comply with all relevant legislation including:

- Computer Misuse Act 1990
 - UK GDPR and Data Protection Act 2018
 - Safeguarding legislation
-

16. Agreement and Declaration

I confirm that I have:

- Read and understood this Acceptable Use Policy
- Agreed to comply with its requirements
- Understood that monitoring may take place

Name:

Organisation (if applicable):

Purpose of Visit:

Signature:

Date: