



# Keeping Staff Safe Online Policy

Date Approved	14 May 2025
Frequency	Annually
Date for Renewal	13 May 2026
Approved by	CHS Governing Body
Owner/Written by	Governors/Network Manager
Type	Statutory
Audience	All

This policy has been adopted by Crowdys Hill School Governing Body.

Signed:  Acting Headteacher

Signed: *Nicki Read & Bryony Hallows* Co-Chair of Governors

Date: 14 May 2025



## 1. Introduction and Rationale

This policy outlines how Crowdys Hill School ensures that staff and volunteers remain safe and protected while working with digital technologies, both on-site and remotely. Digital and online communication tools are integral to modern education and professional collaboration; however, their misuse or unsafe practices can pose risks to staff, pupils, and the wider school community. By adhering to this policy, as well as related policies (e.g., Staff Code of Conduct, Acceptable Use Policy, Data Protection Policy), employees can maintain a high standard of professional conduct and safeguard their personal information, their students, and the school's reputation.

## 2. Scope and Application

- This policy applies to all staff, volunteers, and visitors (where relevant) who use digital technology or online communication tools in a school-related capacity.
- It covers both on-site usage (e.g., within the school's network, using school devices) and remote usage (e.g., working from home, remote teaching).
- It should be read in conjunction with the Safer Working Practice guidance (including the April 2020 addendum) and other relevant policies (e.g., ICT/Online Safety Policy, Data Protection Policy, Staff Code of Conduct).

## 3. Key Principles

1. **Maintain Professional Boundaries:** Staff must keep personal and professional digital interactions separate, ensuring that all communications with pupils and families are channelled via secure, school-approved systems.
2. **Protect Confidential Data:** When handling any personal or sensitive information, staff must follow strict data protection protocols, especially when working remotely.
3. **Ensure Personal Safety:** Staff should avoid sharing personal phone numbers, emails, or social media details with pupils or parents, limiting risk to personal privacy and safeguarding.
4. **Follow Acceptable Use:** The school's Acceptable Use Policy remains in force whether staff are on-site or remote, preventing misuse of personal or school-issued technology.

## 4. Safe Remote Working

Where staff or volunteers are working off-site or conducting tasks (e.g., welfare checks, remote teaching, administrative duties):

### 4.1 Telephone Contact

- **Use of Personal Phones:** If a work phone is available, that should be used to make calls to families. If staff must use a personal device, they should block their number by dialling 141 (or equivalent) before making the call.



- **Avoid Storing Personal Data:** Staff should not record personal/confidential information about families on personal devices; secure school systems (e.g., encrypted school laptop, cloud-based tools) should be used instead.

#### 4.2 Emailing Confidential Information

- **Encryption/Password Protection:** When emailing documents containing personal or sensitive data, staff must either password protect the files (and share the password via a separate message/text) or use encrypted email where possible.
- **Professional Channels:** Use the official school email account for all communications with pupils, parents, or external agencies regarding confidential matters.

#### 4.3 Live Lessons and Video Meetings

- **Consent and Notification:** If a lesson or meeting is to be recorded, all participants must be made aware in advance.
- **Data Protection:** Recordings must follow the school's data handling and retention policies. The Data Protection Officer should be informed of the process if recordings store personal data.
- **Professional Environment:** Staff should ensure backgrounds and surrounding noise levels are appropriate and confidential data or visuals aren't displayed inadvertently on camera.

### 5. Data Protection and GDPR Compliance

Staff must comply with the UK GDPR, Data Protection Act (2018), and the school's Data Protection Policy:

- **Minimum Necessary:** Only collect and store personal data that is essential for professional duties.
- **Encryption:** Documents or files containing sensitive information (pupil data, staff records) must be stored securely and encrypted if taken off-site.
- **Reporting Breaches:** Any loss, theft, or accidental disclosure of sensitive data must be reported to the Data Protection Officer immediately, following the breach reporting protocol.

### 6. Keeping Safe and Professional Boundaries

#### 6.1 Digital Communications

- **No Personal Details Sharing:** Staff should not share personal phone numbers, personal email addresses, or private social media accounts with pupils or parents.
- **Open and Transparent:** Communications, both written and verbal, should remain professional, polite, and in line with Safer Working Practice guidelines.
- **Records:** Where relevant, staff should keep brief records of key communications (time, content summary) for accountability.

#### 6.2 Personal Social Media and Conduct



- Privacy Settings: Staff are advised to keep personal social media profiles private, ensuring pupils or parents do not have access to personal content.
- No Mention of Pupils or Parents: Staff must not reference or discuss pupils, parents, or internal school matters on personal social media.
- Professional Image: Even outside of school hours, staff actions (online or offline) may affect their professional standing, as indicated in the Staff Code of Conduct.

### 6.3 Protecting Staff Against Allegations

- Maintain Clear Boundaries: Staff are reminded that even inadvertent personal contact with pupils or parents can lead to misunderstandings or allegations.
- Report Concerns: If staff sense any boundary crossing or receive inappropriate communications, they must report it promptly to leadership (Headteacher, DSL).

## 7. Safer Working Practice Addendum

Ref: Safer Working Practice (April 2020)

- Staff must be aware that Safer Working Practice includes not only face-to-face interactions but also online/remote communications.
- Points include:
  - Avoiding personal chat with pupils on any non-school-approved platforms.
  - Upholding standards of behaviour that reflect positively on their professional role, whether interacting with pupils or sharing personal content publicly.

## 8. Reference to Other Policies

- Staff Code of Conduct: Sets out broader professional expectations and responsibilities.
- Acceptable Use Policy (AUP): Defines how staff, pupils, and volunteers should responsibly use the school's ICT resources.
- Data Protection Policy: Details obligations under GDPR, including secure handling of sensitive information.
- ICT/Online Safety Policy: Addresses pupil and curriculum-related e-safety measures.
- Behaviour and Safeguarding Policies: Outline disciplinary steps, child protection, and escalation procedures.

## 9. Monitoring, Review, and Compliance

- Monitoring: Senior leaders and ICT staff may monitor staff's remote sessions or logs as appropriate to maintain safeguarding standards.
- Review: This policy will be reviewed every two years or earlier if significant digital/legislative changes arise.



- Non-Compliance: Failure to follow this policy could result in disciplinary action under the school's procedures and, for serious breaches, referral to external authorities.

## 10. Conclusion

By following the guidelines in this Keeping Staff Safe Online Policy, staff and volunteers at Crowdys Hill School will uphold high professional standards, safeguard confidential data, respect personal boundaries, and maintain the trust of pupils, parents, and the broader community. Continuous adherence ensures a culture of responsible, transparent, and secure online practices aligned with legal and ethical requirements.

