



ICT Acceptable Use and Portable Devices 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:

Headteacher

Signed:

Nicki Read & Bryony Hallows

Co-Chair of Governors

Date:

14 May 2025

This ICT Acceptable Use and Portable Devices Policy outlines **Crowdys Hill School's** commitment to **responsible, lawful, and inclusive** use of information and communications technology (ICT) resources, including **portable devices**. It aligns with **UK GDPR**, the **Data Protection Act (2018)**, the **Equality Act (2010)**, the **SEND Code of Practice (2015)**, and local authority requirements. By defining standards for staff and volunteers, the policy ensures **non-discriminatory** and **safe** digital environments, particularly for individuals with disabilities or additional needs.

1. Introduction and Purpose

Objectives:

1. Define the **acceptable use** of all ICT systems and personal/portable devices within or used on behalf of the school.
2. Integrate a **disability-inclusive** approach, ensuring staff with SEND or other impairments receive reasonable adjustments.
3. Comply with **legal frameworks** (UK GDPR, DPA 2018) and **safeguarding duties** (KCSIE 2024), preventing unlawful or unsafe ICT practices.

2. Legal Framework and Guidance

Legislation / Guidance	Purpose	Application
UK GDPR & Data Protection Act (2018)	Governs lawful data handling	Ensures personal data stored on ICT or portable devices is safeguarded according to GDPR
Equality Act (2010)	Prohibits disability discrimination	Requires accessibility adjustments for disabled staff, ensuring fair device usage
SEND Code of Practice (2015)	Guidance on supporting individuals with SEND	Mandates inclusive processes in ICT usage (e.g., accessible devices/software)
Keeping Children Safe in Education (KCSIE) 2024	Statutory safeguarding guidance	Aligns acceptable use with protecting pupils' data and staff accountability
Local Authority Data Protection Policy	Sets local authority standards	Additional compliance for portable device encryption, usage logs, and ICT policies
Freedom of Information Act (FOIA)	Public right to access certain information	Some usage logs or data may be requested under FOIA, except personal data exempt
Protection of Freedoms Act (2012) (Biometric data)	Regulates use of biometric data in schools	Requires explicit consent for biometric systems, plus alternatives for staff/pupils

3. Scope and Definitions

- **Scope:** Applies to **all staff and volunteers** using school ICT systems or portable devices (laptops, tablets, USB devices, mobiles) for **Crowdys Hill School** tasks—on or off school premises.
- **ICT Systems:** Includes hardware (desktops, laptops, tablets), software, email, networks, internet, and digital communications.
- **Portable Devices:** School-issued laptops, USB drives, external hard drives, mobile phones, or personal devices used for school duties.
- **Acceptable Use:** ICT usage that respects confidentiality, digital security, and equality obligations.
- **Disability-Inclusive:** Staff or volunteers with disabilities must receive modifications (hardware, software, or support) so they are not disadvantaged.

4. Roles and Responsibilities

4.1 Governing Body

- Oversees compliance with legislation (UK GDPR, Equality Act).
- Conducts or commissions annual reviews of the ICT Acceptable Use policy.

4.2 Headteacher & Senior Leadership

- **Implementation:** Ensures staff know the policy, emphasising inclusivity for disabled staff/volunteers.
- **Authorises staff training** on safeguarding data and non-discriminatory device usage.

4.3 Data Protection Officer (DPO)

- **Advises** on lawful processing, special category data (e.g., SEND info).
- Investigates data breaches, notifies ICO if needed.

4.4 ICT Department / Support Team

- **Maintains** school ICT systems, installs licensed software, encrypts devices.
- Provides adaptations for staff with **disabilities or SEND** to ensure equitable access.

4.5 Staff and Volunteers

- **Adhere** to this policy's rules.
- Safeguard personal data, maintain confidentiality, respect equality.
- Immediately **report** suspicious activity (phishing, lost device) or policy breaches.

5. Acceptable Use Guidelines

5.1 Professional Conduct

1. **Language & Behaviour:** Communicate respectfully; no harassing, bullying, or discriminatory content (Equality Act compliance).
2. **Authorised Access Only:** No sharing passwords. Each user is responsible for actions performed under their login.
3. **Confidential Data:** Sensitive or personal data (including SEND or health info) must be **encrypted** and handled per UK GDPR.

5.2 No Unauthorised Software

- Install only **ICT-approved software** to avoid viruses or licence violations.
- Do not remove or disable protective software (firewalls, antivirus, encryption).

5.3 Online Communications

- Use **official school email** for pupil or parental communications, preserving accountability.
- Refrain from using personal email addresses to discuss school matters.
- Only post or distribute images (pupils/staff) with explicit permission, abiding by privacy laws.

5.4 Disability Accommodations

- Staff with **vision impairments** may require magnification or screen readers.
- Staff with **mobility impairments** may need alternative input devices.
- Non-compliance with these inclusivity measures is against **Equality Act** duties

6. Portable Devices Usage

6.1 Ownership and Accountability

1. **School-Issued Equipment:** Remains property of Crowdys Hill School; must be returned on termination of role or device replacement.
2. **Personal Devices:** If used for school tasks, must be password-protected, maintain up-to-date antivirus, and comply with encryption where feasible.

6.2 Security Measures

- **Encryption:** All laptops or USB drives storing personal data must use encryption or secure password.
- **Updates & Patches:** Staff keep device OS and security patches current.
- **Storage & Transport:** Devices never left in unsecured vehicles or public places; locked away when not in use.

6.3 Maintenance & Damage

- **ICT Support:** Only the ICT department may install or modify device software for staff.
- **Report Faults:** Immediately notify ICT or DPO for hardware issues, viruses, or suspected breaches.

7. Safe Remote Access and Cloud Services

- **VPN:** Staff using remote methods (VPN) must ensure home systems are also virus-protected and updated.
- **Cloud Platforms:** Any external platform (e.g., Office 365, Google Workspace) must be DPO/ICT-vetted for compliance with UK GDPR and accessibility standards.

8. Inclusive Data Protection

8.1 Reasonable Adjustments

- Staff/volunteers with **mobility or sensory disabilities** are provided with appropriate devices or software (speech-to-text, screen readers) to ensure **no discrimination**.
- The ICT support team or DPO can advise on suitable adjustments or third-party solutions.

8.2 Special Category Data (SEND / Health)

- EHCP or disability-specific data stored on portable devices or cloud services must be **encrypted** and shared only with authorised staff.
- Minimised handling to reduce risk of accidental disclosure, mindful that improper handling can lead to equality-based complaints.

9. Monitoring and Logging

- The school **may monitor** email, device usage, or logs for safeguarding or security.
- Any monitoring respects **UK GDPR** principles of necessity and proportionality (e.g., not to target staff with disabilities).

10. Data Breach and Incident Response

10.1 Reporting Incidents

- **Staff** must report lost/stolen devices, suspicious emails, or potential data misuse to the DPO/Headteacher.
- Provide full details (time, location, type of data at risk).

10.2 Containment & Notification

- The DPO, with ICT support, will **restrict further access**, attempt data retrieval, and evaluate risk.
- If high-risk personal data is involved, the DPO informs the **ICO within 72 hours**; impacted individuals are notified if required by GDPR.

11. Disciplinary and Enforcement

11.1 Minor Infractions

- Staff may face **additional training** or formal warnings for unintentional, low-impact policy breaches.

11.2 Major or Wilful Breaches

- e.g., deliberate data misuse, ignoring encryption on sensitive data, or discriminatory device usage.
- May result in **suspension, dismissal**, or referral to local authority or police if illegal activity is suspected.

12. Policy Review and Further Guidance

Review Cycle: Every year or upon significant changes to legislation (UK GDPR updates, local authority directives). Feedback from staff (including those with SEND) is encouraged, ensuring policy remains inclusive and compliant.

Contacts and Information

- **Data Protection Officer (DPO): Attila Tancos**
- **Headteacher: Emily Hibbard**
- **ICT Support: Attila Tancos**

Compliance Statement: This policy supports **UK GDPR, Equality Act (2010), SEND Code of Practice (2015), and Data Protection Act (2018)**, embedding a **culture of respect, accessibility, security, and accountability** in ICT usage. All staff and volunteers must adhere to these guidelines to safeguard personal data, maintain an **inclusive environment**, and uphold the school's safeguarding responsibilities.