

Haddenham Community Infant School

Online Safety Policy (formerly E-Safety Policy)

- **Date Written / Reviewed:** March 2026
- **Date Adopted by Governing Body:** March 2026
- **Date for Next Review:** March 2027
- **Related Policies:** Child Protection & Safeguarding (incorporating KCSIE), Data Protection (UK GDPR), Behaviour Policy, Staff Code of Conduct, Remote Education

Contents

1. Introduction and Overview
2. Education and Curriculum
3. Expected Conduct and Incident Management
4. Managing the Technical Infrastructure (Filtering & Monitoring)
5. Data Security (UK GDPR Compliance)
6. Equipment and Digital Content

1. Introduction and Overview

Rationale

The purpose of this policy is to:

- Set out the key principles expected of all members of the school community at Haddenham Community Infant School with respect to the safe and responsible use of technology.
- Safeguard and protect pupils and staff in compliance with **Keeping Children Safe in Education (KCSIE)** and **UK GDPR / Data Protection Act 2018**.
- Assist staff working with children to work safely and responsibly online and to monitor their own practice.
- Set clear expectations of conduct regarding internet use for educational, professional, or personal purposes.
- Establish clear structures to address online harms, cyberbullying, and inappropriate conduct, cross-referenced with related school policies.
- Ensure all members of the school community understand that unsafe or unlawful behavior is unacceptable and subject to disciplinary or legal procedures.

Categorisation of Risks (The 4 Cs)

In line with national statutory guidance, online risks for our school community are categorised under four pillars:

- **Content:** Exposure to illegal, inappropriate, or harmful content (e.g., pornography, violence, hate speech, radicalisation/extremism, age-inappropriate gaming, or fake news).
- **Contact:** Harmful interaction with adults or peers (e.g., grooming, illegal contact, or identity theft).
- **Conduct:** Personal online behavior that causes harm (e.g., cyberbullying, sharing illegal/inappropriate images, poor digital footprint, copyright infringement).
- **Commerce:** Risks associated with commercial exploitation (e.g., in-app purchases, age-restricted online marketing, scams, or phishing).

Roles and Responsibilities

Role	Key Responsibilities
Headteacher	Has overall responsibility for online safety provision and data security compliance. Ensures the school uses filtered Internet services complying with DfE Standards. Ensures suitable staff training and maintains oversight of serious online safety incidents.
Designated Safeguarding Lead (DSL) (<i>Lucy McNeil</i>)	Takes lead day-to-day responsibility for online safety and safeguarding risks. Oversees filtering and monitoring logs, ensures incident reporting systems are maintained, liaises with local agencies, and keeps up to date with KCSIE guidelines.
Online Safety / Computing Lead	Promotes online safety education across the curriculum (EYFS–KS1). Works with the DSL and technical team to review policies, incident logs, and curriculum delivery.
Governing Body	Approves the Online Safety Policy annually and evaluates its effectiveness. Ensures the school meets DfE Filtering and Monitoring Standards and appoints a Governor responsible for Online Safety/Safeguarding.
IT Managed Service Provider (<i>Turn It On</i>)	Maintains network security, firewall rules, and virus protection. Implements and audits user-level filtering in line with DfE standards. Reports system alerts, security breaches, or filtering failures immediately to the DSL and Headteacher.

Data Protection Lead / DPO	Ensures compliance with UK GDPR and Data Protection Act 2018. Oversees access controls, data breach logging, and ICO reporting if required.
All Staff	Embed online safety in teaching, model safe behaviors, enforce Acceptable Use Agreements (AUAs), and report all online safeguarding concerns immediately to the DSL via the school's reporting system.

2. Education and Curriculum

Pupil Curriculum

- The school delivers a progressive online safety curriculum embedded within Computing and PSHE, utilizing **Purple Mash** and national age-appropriate frameworks for EYFS to Key Stage 1.
- Key learning strands include:
 - Knowing to **STOP, THINK, and ASK** a trusted adult before clicking or sharing.
 - Recognizing age-appropriate content and online safety rules.
 - Understanding online politeness, privacy, and keeping personal data safe.
 - Understanding that online "friends" or characters may not be who they seem.
 - Knowing how to report worries, abuse, or uncomfortable content to a parent, teacher, or trusted adult (or services such as Childline / CEOP).

Staff and Governor Training

- All staff and governors receive annual safeguarding training (including online safety, filtering and monitoring responsibilities, and UK GDPR).
- Regular updates are provided during staff meetings and induction processes for new hires or placement staff.

3. Expected Conduct and Incident Management

- **Acceptable Use Agreements (AUAs):** All staff, governors, parents, and visitors must sign an AUA prior to system access. At EYFS/KS1, parents sign on behalf of pupils.
- **Incident Escalation:**
 - Online safety or filtering alerts are immediately reported to the DSL (Lucy McNeil) or Deputy DSL (Beckie Lewis).
 - Data protection breaches are escalated to the Data Protection Lead (Carly Busby) and DPO (*Turn It On*).
 - Cases involving illegal content, serious harassment, or law-breaking are escalated to the Police and Local Authority Safeguarding teams.
- **Photography at School Events:** Parents/carers are permitted to take photos of their own children during designated times (e.g., end of assemblies) for personal use only.

Photos/videos containing other children must never be uploaded to social media platforms (e.g., Facebook, WhatsApp, Instagram, TikTok).

4. Managing the Technical Infrastructure (Filtering & Monitoring)

- **DfE Filtering and Monitoring Standards Compliance:**
 - The school works with *Turn It On* to ensure active, managed filtering.
 - Illegal content (including child sexual abuse material) is blocked via the Internet Watch Foundation (IWF) CAIC list.
 - Filtering rules block terrorist, extremist, radicalisation, and adult content in line with the Prevent Duty.
 - The DSL reviews filtering logs and system overrides regularly.
- **Search Engine Controls:** Raw image searches are strictly restricted. Approved, child-friendly search tools (e.g., Google SafeSearch) are implemented for pupil use.
- **User Access:**
 - Pupils use class/year group logins or unique personal logins where appropriate.
 - Staff access systems using individual, strong passwords with multi-factor authentication (MFA) enabled where available.
 - Shared or pupil use of teacher accounts is strictly prohibited.

5. Data Security (UK GDPR Compliance)

- **Data Storage:** Personal data must be stored on secure, encrypted school cloud platforms (e.g., Google Workspace for Education). Unencrypted USB memory sticks are prohibited.
- **Email Use:** Staff must only use official [@haddenhaminfant](#) email addresses for school business and pupil communication. Transfer of personal data via personal email accounts is strictly forbidden.
- **Data Audits:** Staff conduct annual housekeeping to securely delete or archive files in accordance with the Data Retention Policy.

6. Equipment and Digital Content

- **Asset Management & Disposal:** All hardware and software assets are logged. Disposal of redundant storage media is managed by authorized agencies providing forensic wiping guarantees in compliance with WEEE regulations.
- **Device Handling:** Devices provided to staff remain school property, require up-to-date security measures, and must be presented for regular maintenance checks.