|  |  |  |
| --- | --- | --- |
| Hambleton Primary Academy  2025-2026 | A close up of a logo  Description automatically generated | Online Safety Policy |

**Context**

Online safety is an essential part of the school’s safeguarding responsibilities. This policy aligns with the latest statutory guidance, **Keeping Children Safe in Education (KCSIE)**, which explicitly defines online safety as covering three main areas: **Content** (exposure to inappropriate material), **Contact** (harmful interactions with others), and **Conduct** (personal online behaviour and the risk of cyberbullying).

The internet and related technologies are powerful educational tools. It is the duty of the school to ensure that every pupil in our care is safe, and the same principles of safeguarding apply to the ‘virtual’ or digital world as would be applied to the school’s physical buildings.

This Policy document is drawn up to protect all parties – the **pupils**, the **staff**, and the **school** – and aims to provide clear advice and guidance on how to minimise risks and how to deal with any infringements.

**Effective Practice in Online Safety**

**Online Safety** (replacing 'e-Safety') depends on effective practice in each of the following areas:

* Education for responsible ICT use by staff and pupils.
* A comprehensive, agreed, and implemented **Online Safety Policy** (including the **Acceptable Use Policy - AUP**).
* Secure, filtered broadband, and a monitored school network.

**1. The Technologies**

ICT in the 21st Century has an all-encompassing role. Current and emerging technologies used in school and outside of school by pupils include:

* The Internet and e-mail
* Instant messaging (often using simple webcams)
* Blogs, Podcasting, and Social networking sites
* Video broadcasting sites, Chat Rooms, and Gaming Sites
* Mobile phones, smart devices, and tablets (including through **Bring Your Own Device - BYOD**).

**2. Whole School Approach to the Safe Use of ICT**

Creating a safe ICT learning environment includes three main elements at this school:

* An effective range of technological tools (**including filtering and monitoring**).
* Policies and procedures, with clear roles and responsibilities.
* A comprehensive **Online Safety** education programme for pupils, staff, and parents.

**3. Roles and Responsibilities**

**Online Safety** is recognised as an essential aspect of strategic leadership. The Headteacher, with the support of Governors, ensures the Policy is implemented and compliance is monitored. The responsibility for Online Safety has been designated to the Senior Management Team (SMT).

* The SMT ensures they keep up to date with **Online Safety** issues and guidance through liaison with the Local Authority and organisations such as the **Child Exploitation and Online Protection (CEOP) Command**.
* All teachers are responsible for promoting and supporting safe behaviours and fostering a **‘No Blame’ culture** so pupils feel able to report any bullying, abuse, or inappropriate materials.
* All staff are updated about **Online Safety** matters at least once a year, with specific training on professional conduct and appropriate online professional boundaries with pupils.

**4. Teaching and Learning - Why the Internet and Digital Communications are Important**

1. The Internet is an essential element in 21st-century life. The school has a duty to provide pupils with quality Internet access as part of their learning experience.
2. Internet use is part of the statutory curriculum and a necessary tool for staff and pupils.
3. Pupils will be taught what Internet use is acceptable and what is not, through clear objectives and the annual **Acceptable Use Policy (AUP)**.
4. Pupils will be educated in the effective use of the Internet in research and taught how to evaluate Internet content and how to report unpleasant material.

**5. Managing Internet Access**

**Information System Security**

* School ICT systems security will be reviewed regularly.
* Virus protection will be updated regularly.

**E-mail**

* Pupils may only use approved e-mail accounts on the school system.
* Pupils must immediately tell a teacher if they receive offensive e-mail.
* Pupils must not reveal personal details or those of others, or arrange to meet anyone without specific permission.

**Published Content and the School Web Site**

* Staff or pupil personal contact information will not generally be published.
* The Headteacher will take overall editorial responsibility and ensure that content is accurate and appropriate.

**Publishing Pupils’ Images and Work**

* Photographs will be selected carefully, using group shots where possible.
* Pupils’ full names will not be used in association with photographs.
* **Written permission from parents or carers will be obtained before photographs of pupils are published.**

**Social Networking and Personal Publishing**

* The school will educate pupils in the safe use of social networking sites.
* Pupils and parents will be advised that the use of social network spaces outside school brings a range of dangers for primary-aged pupils.

**Managing Filtering and Monitoring**

* The school uses **Senso** (or insert your provider name) for web filtering and monitoring across all devices, including BYOD.
* If staff or pupils come across unsuitable on-line materials, the site must be reported to the SMT.

**Managing Emerging Technologies (Including BYOD)**

* **Pupil-owned devices (BYOD) are permitted only under the strict conditions laid out in the signed Acceptable Use Policy (AUP).**
* The school reserves the right to conduct **unannounced spot checks** on pupil-owned devices to ensure compliance, particularly those not managed by the school's device management system.
* Mobile phones will **not** be used during lessons or formal school time, unless explicitly for a teacher-led activity. The sending of abusive or inappropriate text messages or files is forbidden.

**6. Protecting Personal Data**

Personal data will be recorded, processed, transferred, and made available according to the **GDPR** and the **Data Protection Act 2018**. The school adheres to the principles of the **Information Commissioner's Office (ICO)** guidance, particularly regarding children's data.

**7. Policy Decisions**

**Authorising Internet Access**

* All staff and pupils must read and sign the **Acceptable Use Policy Agreement (AUP)** before using any school ICT resource.
* Parents will be asked to sign and return a consent form at the start of each academic year.

**Sanctions and Consequences for Misuse (The Three-Strike Policy)**

The school operates a clear, three-stage policy for misuse of any device or network access in school:

* **Strike One (Verbal Warning):** Recorded conversation with the class teacher.
* **Strike Two (Written Warning):** Letter home, recorded by SMT, potential temporary loss of device use.
* **Strike Three (Device Confiscation):** Device is immediately removed from the pupil. **The device can only be collected by a parent or guardian** to ensure a mandatory conversation about the breach of the AUP and the safety concerns.

**Assessing Risks**

* The school will take all reasonable precautions to ensure **Online Safety**. However, due to the international scale and linked nature of Internet content, it is not possible to guarantee that unsuitable material will never appear. The school cannot accept liability for any material accessed outside of our managed network.

**8. Communications Policy**

**Introducing the Online Safety Policy to Pupils**

* **Online Safety** rules will be displayed clearly in school.
* Pupils will be informed that network and Internet use will be **monitored and appropriately followed up**.
* **Online Safety** training will be embedded within the ICT scheme of work or the Personal, Social, Health and Economic (PSHE) curriculum.

**Enlisting Parents’ and Carers’ Support**

* Parents’ and carers’ attention will be drawn to the School **Online Safety Policy** and the **AUP** in newsletters and on the school Web site.
* The school will ask all parents to sign the parent/pupil agreement when they register their child and annually thereafter.

**9. Writing and Reviewing the Online Safety Policy**

The **Online Safety Policy** relates to other policies including those for ICT, GDPR, anti-bullying, and child protection. It has been agreed by SLT and approved by Governors and will be reviewed annually.

|  |  |  |
| --- | --- | --- |
| Approved by: | Holly Wood - Headteacher | Date: September 2025 |
| Last reviewed on: | September 2025 | |
| Next review due by: | September 2026 | |