



Hummersea Primary School

Online Safety Policy

September 2026

Purpose

The purpose of this policy statement is to:

- ensure the safety and wellbeing of children and young people is paramount when adults, young people or children are using the internet, social media or mobile devices
- provide staff and volunteers with the overarching principles that guide our approach to online safety
- ensure that, as an organisation, we operate within the law in terms of how we use online devices.

The policy statement applies to all staff, volunteers, young people and anyone involved with Hummersea Primary School.

Legal framework

This policy has been drawn up on the basis of legislation, policy and guidance that seeks to protect children in England. Summaries of the key legislation and guidance are available on:

- online abuse
- bullying
- child protection.

We believe that:

- children and young people should never experience abuse of any kind
- children should be able to use the internet for education and personal development, however safeguards need to be in place to ensure they are kept safe at all times.

We recognise that:

- the online world provides everyone with many opportunities; however, it can also present risks and challenges.
- we have a duty to ensure that all children, young people and adults involved in our organisation are protected from potential harm online.
- we have a responsibility to help keep children and young people safe online, whether or not they are using Hummersea Primary's network and devices.
- working in partnership with children, young people, their parents, carers and other agencies is essential in promoting young people's welfare and in helping young people to be responsible in their approach to online safety.
- all children, regardless of age, disability, gender, race, religion or belief, sex or sexual orientation, have the right to equal protection from all types of harm or abuse.

We will seek to keep children and young people safe by:

- providing clear and specific directions to staff and volunteers on how to behave online through our Code of Conduct Policy.
- supporting and encouraging the young people using our service to use the internet, social media and mobile phones in a way that keeps them safe and shows respect for others
- supporting and encouraging parents and carers to do what they can to keep their children safe online
- developing an online safety agreement for use with young people and their parents or carers.
- developing clear and robust procedures to enable us to respond appropriately to any incidents of inappropriate online behaviour, whether by an adult or a child or young person
- reviewing and updating the security of our information systems regularly
- ensuring that usernames, logins, email accounts and passwords are used effectively.
- ensuring personal information about the adults and children who are involved in our organisation is held securely and shared only as appropriate, also ensuring we are GDPR compliant.
- ensuring that images of children, young people and families are used only after their written permission has been obtained, and only for the purpose for which consent has been given
- providing supervision, support and training for staff and volunteers about online safety
- examining and risk assessing any social media platforms and new technologies before they are used within the organisation.

Managing the Internet

All internet activity within school is monitored and filtered through Securly, a cloud-based filtering and monitoring system for the internet use withing our network.

Whenever any inappropriate use is detected, the IT Lead, Head Teacher and DSL are notified and the incident will be followed up in line with the school Acceptable Use Policy and Safeguarding reporting procedures.

Pupils will have supervised access to Internet resources (where reasonable) through the school's digital devices.

The school monitoring system is reviewed and tested annually.

Infrastructure

Our internet access is monitored by Securly, One IT Services and Solutions and the IT Coordinator, Head Teacher and DSL.

Alongside One IT Services and Solutions, the IT Manager manages the administrative devices throughout school and curriculum access.

Staff and pupils are aware that should they encounter or access anything unsuitable or damaging they must report it immediately to teachers, the DSL, the Head Teacher or the IT Manager.

Online Safety

Definition of Online Safety

Online safety is the collective approach to protecting pupils from harm, exploitation, and radicalisation while using digital technology. It involves identifying, understanding, and reducing the risks children may encounter when using the internet, digital devices, social media, online games, and other digital platforms.

Our approach to online safety focuses on four key areas of risk: **Content, Contact, Conduct, and Commerce**.

The Four Areas of Online Risk

- **Content:** Exposure to illegal, inappropriate, or harmful material. This may include pornography, fake news, radical or extremist content, conspiracy theories, misinformation, disinformation, and AI-generated deepfakes.
- **Contact:** Interaction with harmful or inappropriate individuals or automated systems. This can include grooming, peer-to-peer bullying, communication with unknown individuals, and interactions with generative AI chatbots.
- **Conduct:** Personal behaviour online that may cause harm to oneself or others. This includes cyberbullying, sharing explicit images, creating or sharing deepfakes, spreading misinformation, and engaging in harmful or inappropriate online behaviour.
- **Commerce:** Exposure to financial risks, commercial exploitation, and gambling. This can include in-app purchases, loot boxes, phishing scams, online fraud, and aggressive or targeted advertising.

School Responsibility

The school is committed to providing a safe and secure digital environment for all pupils. Robust web filtering and monitoring systems are maintained across school devices to help prevent pupils from accessing inappropriate or harmful content and to identify potential online safety concerns. However, technology alone cannot keep children safe. Staff proactively teach age-appropriate digital literacy and online safety skills so that pupils understand the risks they may encounter online, know how to make safe and responsible choices, and feel confident reporting concerns to a trusted adult.

Pupils are encouraged to report anything online that makes them feel uncomfortable, worried, threatened, or unsafe. Staff respond appropriately to concerns and follow the school's safeguarding procedures where necessary.

Online Safety in the Curriculum

Online safety education is embedded throughout the curriculum, with all year groups receiving dedicated internet safety teaching each year, as outlined in the **Computing Curriculum Intent**. Further opportunities to develop pupils' understanding of online safety are provided through **Computing and Relationships and Sex Education (RSE)** lessons.

Teaching is designed to help children:

- recognise inappropriate or harmful **content, contact, conduct, and commerce**;
- understand the potential risks associated with different digital platforms and technologies;
- identify inappropriate behaviour and know how to respond or report concerns;
- understand the importance of protecting personal information and maintaining appropriate boundaries online;
- recognise harmful or unreliable information, including conspiracy theories, misinformation, and disinformation;
- develop strategies for checking whether online information is reliable and trustworthy; and
- understand that digital content, including images and information generated or altered using artificial intelligence, may not always be authentic or accurate.

A key part of online safety education is helping pupils become critical and responsible users of digital technology. Children are taught not simply to avoid online risks, but to develop the knowledge, confidence, and critical thinking skills needed to navigate the digital world safely and responsibly.

Misinformation and Disinformation

As part of our online safety curriculum, pupils are taught about the difference between **misinformation** and **disinformation**.

Disinformation is the deliberate creation and spread of false or misleading content, such as deliberately fabricated or manipulated news stories.

Misinformation is the unintentional sharing or spread of false or misleading information. Pupils are taught to question information they encounter online, consider the reliability of the source, check information against trustworthy sources, and avoid sharing content before establishing whether it is accurate.

This approach reflects the definitions provided by the **Cabinet Office and Department for Science, Innovation and Technology (2023)**.

Online/Cyber Bullying

Pupils are made aware of the impact of online bullying and how to seek help if they are affected by these issues. Pupils are taught how to seek advice or help if they experience problems when using the internet and related technologies; i.e. parent/ carer, teacher/ trusted staff member, or an organisation such as Childline/ CEOP report abuse button.

If online abuse occurs, we will respond to it by:

- having clear and robust safeguarding procedures in place for responding to abuse (including online abuse)
- providing support and training for all staff and volunteers on dealing with all forms of abuse, including bullying or cyberbullying, emotional abuse, sexting, sexual abuse and sexual exploitation
- making sure our response takes the needs of the person experiencing abuse, any bystanders and our organisation as a whole into account
- reviewing the plan developed to address online abuse at regular intervals, in order to ensure that any problems have been resolved in the long term.
- This will also be documented on CPOMS so a clear record is kept to safeguard all

- Notifying the appropriate authorities where necessary e.g. police, social services.

Use of Artificial Intelligence (AI) in School

At Hummersea Primary, we recognise that new technologies, including generative Artificial Intelligence (AI), can support teaching, learning and school operations. In line with statutory guidance (*Keeping Children Safe in Education 2026*, the Online Safety Act 2023, and the DfE's Filtering and Monitoring Standards), we are committed to ensuring that any AI tools used within school are **safe, age-appropriate and secure**. AI products must include effective filtering and moderation to prevent access to harmful or inappropriate content and be sensitive to pupils' needs, including those with SEND.

AI systems used in school must maintain strong monitoring and reporting processes. This means that all pupil interactions are logged and reviewed where necessary, with real-time alerts in place if harmful or safeguarding-related content is searched for or disclosed. Where concerns arise, staff will follow school safeguarding procedures.

To ensure safe practice, all AI products used in school must comply with data protection law (UK GDPR and the Data Protection Act 2018), ensuring children's personal data is not collected, stored, or shared inappropriately, nor used for commercial purposes. Regular security updates, password protections, and permissions will be in place, and staff will review the effectiveness of AI tools as part of our wider online safety and safeguarding monitoring. Parents will be informed of how AI tools are used in school, and pupils will be taught how to use them responsibly if and when they are included as part of our computing and digital citizenship curriculum.

Mobile Phone Policy and Storage

The school is a mobile phone-free environment to safeguard children, minimise distractions, and protect the learning environment. Pupils are strictly prohibited from having mobile phones, smartwatches with cellular/camera capabilities, or any other personal internet-enabled devices in their possession during the school day. If a child must bring a mobile phone to school for safety during their journey to and from the premises, the device must be completely switched off before entering the school gates. Immediately upon arrival, the pupil must hand the device to their class teacher or designated staff member, who will place it in a secure storage area. The device will remain locked away and inaccessible to the child throughout the entire day, including during breaktimes and lunchtimes, and will be returned to the pupil only at the final dismissal. Any device found in a pupil's possession during the school day will be immediately confiscated, stored securely, and released only to a parent or legal guardian.

Related policies and procedures

This policy statement should be read alongside our organisational policies and procedures, including:

- Safeguarding Policy
- Child-on-Child Abuse Policy
- Staff Code of Conduct (including low level concerns) Policy
- Confidentiality and Whistle Blowing Policy
- Behaviour Policy

- Social Media Policy
- Safer Recruitment Policy (Redcar and Cleveland Council)

Monitoring and Review

This policy will be reviewed annually or in light of any updated guidance for online safety.