Hummersea Primary School

Online Safety Policy

September 2025

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.

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 in the Curriculum

All year groups receive internet safety lessons yearly as laid out in the Computing Curriculum intent. The school provides opportunities within RSE and Computing lessons to teach about online safety. The teaching of online safety focuses on helping children to recognise inappropriate content, conduct, contact and commerce and helps them learn how to respond or react appropriately. They are also made aware of untrustworthy content available on the internet such as conspiracy theories, dis information and misinformation and how to look for reliable, trustworthy sources when accessing the internet.

Disinformation is the deliberate creation and spread of false or misleading content, such as fake news.

Misinformation is the unintentional spread of this false or misleading content

(Cabinet Office, 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*, 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.

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.