Online Safety Policy

Autumn Term 2025

Purpose

At Elloughton Primary School we fully recognise and embrace the opportunities that digital technologies and connectivity bring to teaching, learning, communication, and school life. Access to the online world enables limitless opportunities for creativity, collaboration, and knowledge-sharing, and is therefore integral to everyday learning.

We are also mindful that technology brings potential risks, including exposure to inappropriate material, contact from strangers, online bullying, radicalisation, grooming, exploitation, misinformation, and identity theft. The role of the school is not only to reduce these risks but also to equip pupils with the knowledge, skills and resilience to become safe, responsible, and respectful online citizens.

This policy sets out our approach to online safety in line with statutory guidance including:

- *Keeping Children Safe in Education* (DfE, 2025)
- *Working Together to Safeguard Children* (DfE, 2023)
- *UKCIS Education for a Connected World Framework* (2020, updated)
- The *Data Protection Act 2018* and *UK GDPR*

Responsibilities of the school community

Online safety is a shared responsibility across the school community. Everyone has a role to play in ensuring children and adults are safe, confident, and responsible users of digital technologies.

Leadership Team

- Develop and promote a positive culture of online safety across the school.
- Support the E-Safety Coordinator in their role.
- Provide resources, training and support for staff and pupils.
- Receive and regularly review online safety incident logs recorded on CPOMS.
- Ensure compliance with all relevant legislation and guidance.
- Take ultimate responsibility for online safety within the school community.

E-Safety Coordinator

- Act as the school lead on online safety, staying up to date with legislation and risks.
- Be the first point of contact for online safety concerns.
- Maintain, update and monitor implementation of this policy.
- Embed online safety across the computing and PSHE curriculum.
- Deliver and/or coordinate regular staff training.
- Engage parents/carers through workshops, newsletters, and online resources.
- Liaise with external agencies (e.g. LA, UK Safer Internet Centre, CEOP, police) where necessary.
- Report to SLT and governors on online safety issues and incidents.

All Staff

- Read, understand and implement this policy and the Staff Acceptable Use Policy (AUP).
- Model safe, respectful and responsible online behaviour.
- Embed online safety into teaching and learning activities.
- Know how to recognise and respond to online safety concerns.
- Maintain professional conduct in personal use of technology (see Staff Code of Conduct).
- Report concerns promptly to the DSL.

ICT Support (Primary Tech)

- Provide and maintain a secure, filtered and monitored ICT infrastructure.
- Ensure timely updates to systems, security and filtering.
- Report any breaches, vulnerabilities or risks to the DSL.
- Liaise with the LA and external agencies on technical and safeguarding issues.
- Maintain professional conduct in personal use of technology.

Pupils

- Read, understand and follow the Pupil Acceptable Use Policy.
- Use technology respectfully, responsibly and safely.
- Report concerns, inappropriate content, or unsafe behaviour to staff.
- Support peers in making safe choices online.
- Respect the rights, feelings and intellectual property of others.

Parents and Carers

- Support the school's approach to online safety.
- Read, discuss and reinforce the Pupil AUP at home.
- Stay informed about the risks and opportunities of children's online use.
- Model positive and safe behaviour when using technology.
- Raise any online safety concerns with the school promptly.

Governing Body

- Understand statutory duties around online safety.
- Ensure the school has effective filtering and monitoring systems in place (in line with DfE filtering and monitoring standards, 2023).
- Ensure online safety is integrated into safeguarding and curriculum policies.
- Monitor and evaluate the school's approach to online safety.
- Support funding and resources for staff training and safe infrastructure.

Teaching and Learning

Online safety is taught through computing, PSHE, RSE, assemblies and cross-curricular opportunities. Pupils are taught about the four key risk areas (Content, Contact, Conduct, Commerce).

Pupils learn to:

- Protect personal information
- Evaluate online sources and misinformation
- Manage online relationships
- Understand consent, digital footprints, and privacy
- Report concerns appropriately

Online safety education is age-appropriate, progressive, and adapted to pupil needs (including SEND). The school participates in **Safer Internet Day** and other national awareness campaigns. Staff routinely highlight relevant online safety issues during lessons and weekly e-safety questions.

Working with Parents and Carers

We will:

- Share regular updates, advice and resources via newsletters, Reach More Parents, Class Dojo and the school website.
- Hold online safety workshops and information sessions.
- Promote National Online Safety materials.
- Provide guidance on filtering, parental controls and supporting children at home.

Managing ICT Systems and Access

- Access to ICT systems is restricted to authorised users with unique login details.
- Staff and pupils must not share passwords.
- Staff logins must not be used by pupils.
- Filtering and monitoring is provided through **Securly** and Primary Tech in line with DfE standards.
- Logs of activity are maintained and monitored regularly.
- Internet use by pupils is closely supervised.
- Use of personal data is compliant with UK GDPR and the Data Protection Act 2018.

Filtering and Monitoring

- The school uses a filtered internet service. The filtering is provided through Securly and Primary Tech.
- If users discover a website with inappropriate content this will be reported immediately to the E-safety Coordinator.
- Incidents of inappropriate or illegal online content are reported immediately to the DSL, filtering provider, and (where necessary) external agencies such as CEOP or the police.
- The school will regularly review the filtering and the security systems to ensure they meet the needs of all users.

To address this and in light of the 4 categories of risk outlined below, we will adopt a whole school approach involving a number of measures and approaches with the aim of:

- Having robust processes (including filtering and monitoring systems) in place to ensure the online safety of pupils, staff, volunteers and governors
- Protecting and educating the whole school community in safe and responsible use of technology, including mobile and smart technology
- Setting clear guidelines for the use of mobile phones for the whole school community
- Establishing clear mechanisms to identify, intervene and escalate any incidents or concerns, where appropriate.

The approach to online safety is based on addressing the following 4 categories of Risk:

- **Content** – Being exposed to illegal, inappropriate or harmful content, such as pornography, fake news, racism, misogyny, self-harm, suicide, antisemitism, radicalisation and extremism.
- **Contact** – Being subjected to harmful online interaction with other users, such as peer-to-peer pressure, commercial advertising and adults posing as children or young adults with the intention to groom or exploit them for sexual, criminal, financial or other purposes.

- **Conduct** – Personal online behaviour that increases the likelihood of, or causes, harm, such as making, sending and receiving explicit images (e.g. consensual and non-consensual sharing of nudes and semi-nudes and/or pornography), sharing other explicit images and online bullying.
- **Commerce** – Risks such as online gambling, inappropriate advertising, phishing and/or financial scams.

Use of Digital Devices and Mobile Phones

- Pupils may not use personal mobile phones or other digital devices such as smart phones or Airtags in school. KS2 pupils who bring a phone for travel safety must hand it to staff during the day.
- Staff may only use personal phones outside of teaching time and not in the presence of pupils.
- Staff should not use personal devices to capture or share images of pupils unless permission has been given for a specific purpose. Once the image has been uploaded to Google Drive and/or added to social media it should be deleted from the personal device.
- School devices must be used for recording and storing images in line with GDPR and safeguarding guidance.

Using New Technology

- As a school we will keep abreast of new technologies and consider both the benefits for learning and teaching and also the risks from a safety point of view.
- We regularly amend the E-safety policy to reflect any new technology that we use, or to reflect the use of new technology by pupils which may cause an E-safety risk.

Using Email

- Pupils should use approved email accounts allocated to them by the school and be aware that their use of the email system will be monitored and checked.
- Pupils will be reminded when using email about the need to send polite and responsible messages, about the dangers of revealing personal information, opening emails from an unknown sender and viewing/opening attachments.
- Pupils are not permitted to access personal email accounts during school.
- Communication between staff and pupils or members of the wider school community should be professional and related to school matters only. It should be via their school email account and not a personal email account.

Any inappropriate use of the school email system or the receipt of any inappropriate messages by the user should be reported to a member of staff immediately.

Use of Images, Video and Sound

- Parental consent is obtained before publishing pupil images/videos.
- Pupils are taught safe and responsible creation and use of digital media.
- Full names will never be used alongside pupil images.
- Staff must follow the Staff AUP when using school equipment.

Using Video Conferencing and Other Online Video Meetings and/or Blogs

On occasion we use blogs or websites to enhance our teaching and learning by publishing content online. However we will ensure that staff and pupils take part in these activities in a safe and responsible manner.

There are also times where we use video conferencing to enhance the curriculum by providing learning and teaching activities that allow pupils to link up with people in their locations and see and hear them. We ensure that staff and pupils take part in these opportunities in a safe and responsible manner.

- All video conferencing activity is supervised by a suitable member of staff.
- Pupils will not operate video conferencing equipment, or answer calls, without the permission from the supervising member of staff.
- Video conferencing equipment will be switched off and secured when not in use / online meeting rooms will be closed and logged off when not in use.
- Pupils will be given appropriate user rights when taking part in an online meeting room. They will not have host rights or the ability to create meeting rooms.
- Video conferencing should not take place off school premises without the permission of the Headteacher.
- Parental permission will be sought before taking part in video conferences.
- Permission will be sought from all participants before a video conference is recorded. Video conferences should only be recorded where there is a valid educational purpose for reviewing the recording. Such recordings will not be available outside of the school.

Personal Data

- We will ensure personal data is processed and stored securely in line with the Data Protection Act 2018 and UK GDPR.
- We will ensure personal data is recorded, processed, transferred, stored and managed in accordance with the General Data Protection Regulation 2018.
- Staff will ensure they properly log off from a computer terminal after accessing personal data.
- Staff will not remove personal or sensitive material from the school premises without permission from the Headteacher. Any data, which is impractical to ensure is kept in school, (e.g. reports) will be removed in password / encrypted format.

School Website and Other Online Content Published by the School

The school website will not include the personal details, including individual email addresses of staff and pupils.

- A generic contact email address will be used for all enquiries received through the school website.
- All content included on a school website will be approved by the Headteacher before publication.
- Photographs of children will only appear on the website with parental permission.
- Staff and pupils should not post school related content on the school website or social network platforms without seeking parental permission first.

Monitoring and review

The effectiveness of the school's e-safety provision is monitored and reviewed regularly by senior leaders and the designated safeguarding lead to ensure pupils are kept safe online. Monitoring includes review of online safety incidents, filtering and monitoring systems, staff training, and pupil and parent feedback. Findings are used to strengthen practice and inform safeguarding procedures. This policy is reviewed every three years, or sooner if required, to reflect current guidance and emerging online risks.

Learning Technologies in School

	Pupils	Staff
Personal mobile phones in school	Yes (stored safely)	Yes
Mobile phones used in lessons	No	No
Mobile phones used outside of lessons	No	Yes *
Taking photographs or videos on personal equipment	No	No
Taking photographs or videos on school devices.	Yes	Yes
Use of handheld devices such as iPads, recording devices.	Yes	Yes
Use of personal emails addresses in school	Yes- provided by school	Yes
Use of online chat rooms	No	No
Use of blogs, wikis, podcasts or social networking sites.	Yes as controlled by filtering	Yes as controlled by filtering
Use of video conferencing / online video meetings	Supervised	Yes

NB. Phones are only to be used by staff to make/receive calls and text messages when children are not present. The phone should be on silent and stored away during lessons. Staff are not allowed to show photos/play music from their personal phone to pupils.

Adoption, Approval, Sign Off

Signed	**Louise Hurwood/Rachel Callaghan**
On behalf of	**Headteacher**
Date	**Autumn Term 2025**

Document Control

Title of Document	**Online Safety Policy**
Revision number	**1**
Review frequency	**Annually**
Next review date	**Autumn Term 2026**
Type or status	**Policy**