E-Safety Policy

Autumn Term 2023

Purpose

At Elloughton Primary School we fully recognise, acknowledge and embrace the importance and benefits of a connected world. The opportunities for learning created by providing access to such a world are limitless and must therefore become part of day to day teaching and learning in school.

Being part of the internet community, as well as providing the aforementioned opportunities, also opens up the possibilities of exposure to dangers which would otherwise not be present, for example: access to inappropriate materials, contact with potentially dangerous strangers, "cyber" bullying and identity theft. It must therefore be the role of the school to ensure that such risks are minimised, and, more importantly, that children are provided with the knowledge, skills and attitude necessary to become positive, safe and healthy on-line citizens.

Responsibilities of the school community

We believe that E-safety is the responsibility of the whole school community, and everyone has their part to play in ensuring all members of the community are able to benefit from the opportunities that technology provides for learning and teaching. The following responsibilities demonstrate how each member of the community will contribute.

Responsibilities of Leadership Team
- Develop and promote an E-safety culture within the school community.
- Support the E-safety Coordinator in their work.
- Make appropriate resources, training and support available to members of the school community to ensure they are able to carry out their roles with regard to E-safety effectively.
- Receive and regularly review e-safety incident logs on CPOMs and be aware of the procedure to be followed should an E-safety incident occur in school.
- Take ultimate responsibility for the E-safety of the school community.

Responsibilities of the E-safety Coordinator
- Promote awareness and commitment to E-safety throughout the school.
- Be the first point of contact in school on all E-safety matters.
- Create and maintain e-safety policies and procedures.
- Develop an understanding of current e-safety issues, guidance and appropriate legislation.
- Ensure all members of staff receive an appropriate level of training in E-safety issues.
- Ensure that E-safety education is embedded across the curriculum.
- Ensure that E-safety is promoted to parents and carers.
- Liaise with the Local Authority, the local safeguarding children's board and other relevant agencies as appropriate.
- Monitor and report on e-safety issues to the E-safety group and SLT as appropriate.

Responsibilities of Staff
- Read, understand and help promote the school's E-safety policies and guidance.
- Read, understand and adhere to the school staff Acceptable Use Policy.

● Develop and maintain and awareness of current E-safety issues and guidance.

● Model safe and responsible behaviour in your own use of technology.
● Embed E-safety messages in learning activities involving technology.
● Be aware of what to do if an e-safety incident occurs.
● Maintain a professional level of conduct in their personal use of technology at all times.

Responsibilities of ICT Support (Primary Tech)
● Read, understand, contribute and help promote the school's E-safety policies and guidance.
● Read, understand and adhere to the school staff Acceptable Use Policy.
● Support the school in providing a safe technical infrastructure to support learning and teaching.
● Take responsibility for the security of the school ICT system.
● Report any E-safety related issues that come to your attention to the E-safety Coordinator.
● Develop and maintain an awareness of current E-safety issues, legislation and guidance relevant to your work.
● Liaise with the Local Authority and others on technical issues.
● Maintain a professional level of conduct in their personal use of technology at all times.

Responsibilities of Pupils
● Read, understand and adhere to the school pupil Acceptable Use Policy.
● Help and support the school in creating E-safety policies and practices; and adhere to any policies and procedures the school creates.
● Take responsibility for learning about the benefits and risks of using the internet and other technologies in school and at home.
● Take responsibility for your own and each other's' safe and responsible use of technology in school and at home,
● Ensure you respect the feelings, rights, values and intellectual property of others in your use of technology in school and at home.
● Understand what action you should take if you feel worried, uncomfortable, vulnerable or at risk whilst using technology in school and at home, or if you know of someone who this is happening to.
● Discuss E-safety issues with family and friends in an open and honest way.

Responsibilities of Parents and Carers
● Help and support your school in promoting E-safety.
● Read, understand and promote the school pupil Acceptable Use Policy with your children.
● Take responsibility for learning about the benefits and risks of using the internet and other technologies that your children use in school and at home.
● To take responsibility for their own awareness and learning in relation to the opportunities and risks posed by new and emerging technologies.
● Discuss e-safety concerns with your children, show an interest in how they are using technology and encourage them to behave safely and responsible when using technology.
● Model safe and responsible behaviours in your own use of technology.
● Consult with the school if you have any concerns about your children's use of technology.

Responsibilities of Governing Body
● Read, understand, contribute to and help promote the school's E-safety policies and guidance.
● Develop an overview of the benefits and risks of the internet and common technologies used by pupils.

● Develop an overview of how the school ICT infrastructure provides safe access to the internet.

● Develop an overview of how the school encourages pupils to adopt safe and responsible behaviours in their use of technology in and out of school.
● Support the work of the E-safety group in promoting and ensuring safe and responsible use of technology in and out of school, including encouraging parents to become engaged in E-safety activities.
● Ensure appropriate funding and resources are available for the school to implement their E-safety strategy.

Learning and Teaching

● We believe that the key to developing safe and responsible behaviours online, not only for pupils but everyone within our school community, lies in effective education. We know that the internet and other technologies are embedded in pupil's lives not just in school but outside as well, and we believe we have a duty to help prepare our children to safely benefit from the opportunities the internet brings.
● We will provide a series of specific E-safety related lessons in every year group as part of the computing curriculum/ PSHE curriculum and other lessons.
● We will celebrate and promote E-safety through Safer Internet Day each year and celebration of our learning on the school website.
● We will discuss, remind or raise relevant e-safety messages with pupils routinely wherever suitable opportunities arise during all lessons; including the need to protect personal information, consider the consequences their actions may have on others, the need to check the accuracy and validity of information they use, and the need for respect and acknowledge ownership of digital materials.
● We will remind pupils about their responsibilities through the Acceptable Use Policy which every pupil will sign and will be displayed throughout the school.
● Staff will model safe and responsible behaviour in their own use of technology during lessons.

How parents and carers will be involved

We believe that it is important to help all our parents develop sufficient knowledge, skills and understanding to be able to help keep themselves and their children safe. To achieve this we will:
● Share via Class Dojo the weekly e-safety circle question, and information from National Online Safety, so the same key messages about E-safety can be reinforced at home.
● Hold parent workshops on E-safety.
● Include useful links and advice on E-safety regularly in newsletters and on the website.

Managing ICT systems and access

The school will be responsible for ensuring that access to the ICT systems is as safe and secure as possible.

● Servers and other key hardware or infrastructure will be located securely with only appropriate staff permitted access.
● Servers, workstations and other hardware and software will be kept updated as appropriate.

- Virus protection is installed on all appropriate hardware and will be kept updated as appropriate.

- The school will agree which users should and should not have internet access, and the appropriate level of access and supervision they should receive.
- All users will sign the summary of the Acceptable Use Policy (AUP) provided by the school, appropriate to their age and access. Users will be made aware that they must take responsibility for their use of, and behaviour whilst using, the school ICT systems, and that such activity will be monitored and checked.
- In Foundation Stage/ Key Stage One / Key Stage Two pupils will access the internet using an individual log on which will be their Wonde code or email address and password. Internet access will be supervised AT ALL TIMES by a member of staff.
- Members of staff will access the internet using an individual log on. They will ensure they log out after each session, and not allow pupils to access the internet through their log on. They will abide by the school AUP at all times.
- Any administrator or master passwords for school ICT systems should be kept secure and available to at least two members of staff, e.g. Headteacher and member of technical support.
- The wireless network in school is encrypted to reduce the risk of unauthorised access.
- The school will take all reasonable precautions to ensure that users do not access inappropriate material. However it is not possible to guarantee that access to unsuitable material will occur.
- The school will regularly audit ICT use to establish if the e-safety policy is adequate and that implementation of the E-safety policy is appropriate. We will regularly review our internet access provision

Filtering internet access

- 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 should be reported immediately to the E-safety Coordinator.
- If users discover a website with potentially illegal content, this should be reported immediately to the E-safety Coordinator. The school will report this to appropriate agencies including the filtering provider.
- 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 in 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.

Learning technologies in school

	Pupils	Staff
Personal mobile phones in school	No	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

* Phones are to be used by staff to make and receive calls and text messages when there are no children around. The phone is to be on silent and in a bag during lessons. Staff are not allowed to show photos/play music from their phone to pupils.

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.
- Any communication will be forwarded to school email only.
- 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 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.

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.

Using images, videos and sound

We remind pupils of safe and responsible behaviours when creating, using and storing digital images, videos and sound. We remind them of the risks of inappropriate use of digital images, video and sound on their online activities both at school and at home.

- Digital images, video and sound will be created using equipment provided by the school or by staff who have signed the staff AUP; images of children will not be stored on personally owned computer equipment.

- Staff and pupils will follow the school policy on creating, using and storing digital resources.
- In particular, digital images, video and sound will not be taken without the permission of participants: images and video will be of appropriate activities and participants will be in appropriate dress: full names of participants will not be used either within the resource itself, within the file name or in accompanying text online; such resources will not be published online without the permission of the staff / pupils involved.
- If pupils are involved, relevant parental permission will also be sought before resources are published online.

Using video conferencing and other online video meetings and 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.
- On occasion 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.

Using mobile phones

- Pupils' personal mobile phones are not allowed in classrooms. (Older children who have them for safety going to and from school must hand them in to the class teacher before registration.)
- Staff usually prefer to carry their own mobile phones on school visits, rather than a "school mobile". Staff will not be expected to use personal mobile phones in any situation where their mobile phone number or personal details may be revealed to a parent or pupil.

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 will 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.

Personal Data

- We will ensure personal data personal data is recorded, processed, transferred and made available to the Data Protection Act 2020.
- 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.

Adoption, Approval, Sign Off

Signed	**Louise Hurwood/Rachel Callaghan**
On behalf of	**Headteacher**
Date	**Autumn Term 2023**

Document Control

Title of Document	**E-Safety Policy**
Revision number	**1**
Review frequency	**1 Year**

| Next review date | **Autumn Term 2024** |
| Type or status | **Policy** |