Online Safety Policy

Fenstanton and Hilton Primary School

Reviewed By : The Full Governing Body

Date of Review : September 2025

Date of Next Review : September 2027

Policy adopted from the ICT Service Model Policy

Contents

Background to this policy

The purpose of this policy is to describe the safeguarding measures in place for adults and children in school in relation to online safety, including:

- The policies and practice embedded in our school and followed by the whole school community
- The infrastructure and how it is set up to keep pupils safe online, including filtering, monitoring, and preventing and responding to online safety incidents
- A progressive, relevant age appropriate online safety curriculum for all pupils which (as a minimum) meets the requirements of the National Curriculum for Computing and the statutory Relationships and Health Education

Online safety in schools is primarily a safeguarding concern and not a technology one. Therefore, this policy should be viewed alongside other safeguarding policies and approaches including, but not limited to:

- Safeguarding and Child Protection
- Keeping Children Safe in Education
- Safer Working Practices
- Data Protection / GDPR Policy
- Anti-Bullying Policy
- School Complaints Procedure
- Whistle Blowing Policy
- Cambridgeshire Progression in Computing Capability Materials

This policy must be read alongside the staff and pupil Acceptable Use Policies and Agreement (AUPs).

These AUPs outline the expectations and sanctions which apply to staff and pupil use of technology.

The development of our online safety policy involved:

- The Headteacher
- The Designated Safeguarding Lead
- The Computing Subject Leader
- Cambridgeshire Local Authority Advisor (Cambridgeshire Education ICT Service)
- The governor responsible for Safeguarding

It was presented to the governing body on and ratified on 10th July 2025 and will be formally reviewed in July 2027.

- This policy may also be partly reviewed and / or adapted in response to specific online safety incidents or developments in the school's use of technology. It has been shared with all staff via our internal communications, is readily available on the school network, My Concern safeguarding-reporting tool, school website, and has also been made available to parents.

- All staff must be familiar with this policy and sign the relevant Acceptable Use Policy before being allowed to access the school's systems. As online safety is an important part of our school's approach to safeguarding, all staff have a shared responsibility to ensure that the policy and practices are embedded. This will be monitored by the Headteacher, the Designated Safeguarding Lead and governors as appropriate. Pupils and parents/carers have an Acceptable Use Agreement shared with them annually (see appendices).

Rationale

At Fenstanton and Hilton Primary School, we believe that the use of technology in education brings great benefits. To live, learn and work successfully in an increasingly complex and information-rich society, our children must be able to use technology effectively.

The use of exciting and innovative technology tools in school and at home has been shown to support learning and promote pupil achievement. Yet at the same time, we recognise that the misuse of technology can put users of technology at risk within and outside the school.

The risks they may face can broadly be categorised into the 4 C's; **Contact**, **Content**, **Conduct, and Commerce** *(Keeping Children Safe in Education)* and may include:

- Access to harmful, illegal or otherwise unsuitable content including gaming, gambling sites, sexually explicit material and websites with extremist ideologies and images
- Unauthorised access to / loss of / sharing of personal information
- The risk of being subject to grooming by those with whom they make contact on the internet, including the sharing of Self-Generated Indecent Images
- The sharing / distribution of personal images without an individual's consent or knowledge
- Inappropriate communication / contact with others
- Cyber-bullying
- An inability to evaluate the quality, accuracy and relevance of information on the Internet
- Plagiarism and copyright infringement
- Illegal downloading or streaming of music or video files
- Phishing or financial scams
- The potential for excessive use which may impact on the social and emotional development and learning of the young person.

While children and young people need support to keep them safe online, the risks associated with the use of technology are not restricted to just them. Online safety issues can also affect adults who work or are associated with the school and this will be referenced in more detail later in this policy.

Technologies regularly used by pupils and staff include:

Staff:

- Staff laptops, classroom iPads and Chromebooks. Staff devices can also be used at home in accordance with the staff AUP, particularly with regard to GDPR.
- Staff have access to school systems beyond the school building, including Google Workspace.
- Class cameras and other peripherals such as visualisers and interactive whiteboards
- Staff level internet access

Pupils:

- Curriculum Chromebooks, including filtered access to the Internet and pupil level access to areas of the school network
- Cameras and peripherals including programming resources
- Google Classroom accounts, providing pupils with access within and beyond the school gates
- Purple Mash accounts; Times Tables Rock Stars accounts.

Where the school changes the use of existing technology or introduces new technologies which may pose risks to users' safety, a risk assessment will be completed to show how the risk is being mitigated and reduced to an acceptable level.

The Online Safety Curriculum

When using online technologies, it is essential that children understand how to behave in a safe and responsible manner and also how to react when faced with inappropriate content or situations which make them feel uncomfortable. The need for a progressive, age appropriate online safety curriculum is clearly documented in the National Curriculum for Computing (England) and the statutory Relationship and Health Education.

At Fenstanton and Hilton Primary School, we believe that a comprehensive programme of online safety education is vital for developing our pupils' ability to use technologies safely. We believe that just as children learn how to swim by going to a swimming pool, they will learn safe life-long online behaviours by accessing and using a range of online services including the World Wide Web.

Our online safety curriculum is based on the Purple Mash and online Safety units of work and the Cambridgeshire PSHE Service Primary Personal Development Programme, with reference to UKCIS's Education for a Connected World.

This is achieved using a combination of:

- Discrete and embedded activities, drawn from a selection of appropriate materials and is linked to demonstrating safe practice in our online learning platforms.
- Key online safety messages are delivered and reinforced through cross curricular opportunities such as emailing, researching, blogging and communicating in appropriate online environments.
- Focus events to raise the profile of online safety for our pupils and school community.
- A flexible curriculum which is able to respond to new challenges as they arise.

Continued Professional Development

Staff at Fenstanton and Hilton Primary School receive up-to-date information and training on online safety in the form of staff meetings and updates from the school's online safety and Designated Safeguarding Leads, as well as training from external providers where appropriate.

Nominated members of staff receive more in-depth online safety training to support them in keeping up to date and reviewing the school's approach, policies and practice. This nominated member of staff is also a Designated Safeguarding Lead.

New staff receive information on the school's acceptable use policy as part of their induction, including advice on Protecting their Professional Reputation Online.

All staff have been made aware of individual responsibilities relating to the safeguarding of children within the context of online safety and know what to do in the event of misuse of technology by any member of the school community.

Mobile Phones and Use of Mobile Data in School

Keeping Children Safe in Education (September 2023) acknowledges that "many children have unlimited and unrestricted access to the internet via mobile phone networks (i.e. 3G, 4G and 5G)." It highlights the need for schools to have a clear policy statement on, and carefully consider *"how this is managed on their premises and reflect this in their mobile and smart technology policy and their child protection policy."*.

At Fenstanton and Hilton Primary School, our Mobile Phones in School Policy states the following:
Where a pupil does bring a mobile phone to school, the phone must remain switched off and handed to the school office for safekeeping during the school day. Phones may not be used for any purpose on school

premises or during off-site activities, such as swimming or sports. Under no circumstances should there be access to phones during the school day. Phones may not be taken on school trips, including residential trips.

Monitoring, and Averting Online Safety Incidents

The school keeps children safe when using online technologies through a combination of online safety education, filtering and monitoring children's online activity and reporting incidents, including following Safeguarding procedures where appropriate.

The school's technology infrastructure is designed to minimise the risks associated with adult and pupil use of technology. Safeguards built into the school's infrastructure include:

- Secure, private EastNet internet connection with a direct link to the National Education Network. This is provided and maintained by The ICT Service on behalf of the local authority.
- Managed firewalling running Unified threat management (UTM) that provides restrictions on download of software, apps and file types from known compromised sites.
- Enhanced web filtering provided to all EastNet sites as standard.
- Antivirus package provided as part of EastNet Connection.

Staff also monitor pupils' use of technology and, specifically, their activity online. This is achieved through a combination of:

- Appropriate levels of supervision when pupils are using online technologies.
- Auto-generated alerts which flag up activity in specific safeguarding categories which may raise child protection concerns.

Staff use of the schools' internet is also monitored and can be investigated where needed.

A system of staff and pupil passwords is in place to enable appropriate access to the school network.

- All members of staff have individual, password protected logins to the school network / cloud service / MIS systems.
- Visitors to the school (e.g. supply teaching staff) can access part of the school systems using a generic visitor login and password.
- The wireless network is encrypted to the standards advised by the Local Authority and the wireless key is kept securely by the school office.
- School staff and pupils are not permitted to connect personal devices to the school's wireless network and a guest wireless key is issued to visitors on a case by case basis.

Whilst we recognise that it is impossible to eliminate the risks associated with the use of technology, these safeguards are in place to help minimise these risks to an acceptable level.

Responding to Online Safety Incidents

It is important that all members of staff – teaching and non-teaching – are aware of how to respond if an online safety incident occurs or they suspect a child is at risk through their use of technology.

- Staff responses to online safety incidents must be consistent with responses to other incidents in school. This may mean that serious actions have to be taken in some circumstances.
- If an online safety incident occurs, Fenstanton and Hilton Primary School will follow its agreed procedures for responding. This will include: support for the pupil/s and gaining pupil voice to understand context; internal sanctions, including protective and educational consequences as necessary; and involvement of parents/carers. This process may include the deactivation of

accounts, restricted access to systems as per the school's AUPs or reporting incidents to the police and other authorities– see appendix.

In addition, the Education and Inspections Act 2006 empowers headteachers to such extent as is reasonable, to regulate the behaviour of pupils when they are off the school site and empowers members of staff to impose disciplinary penalties for inappropriate behaviour. This is pertinent to incidents of cyber-bullying, or other online safety incidents which may take place outside of the school but has an impact within the school community.

- With this in mind, the Headteacher may decide to apply the sanctions and / or procedures in the relevant AUP to incidents which occur outside of schools if s/he deems it appropriate.

The Education Act 2011 gives school staff the powers, in some circumstances, to search personal digital devices and decide whether to delete data or files if the person thinks there is good reason to do so.

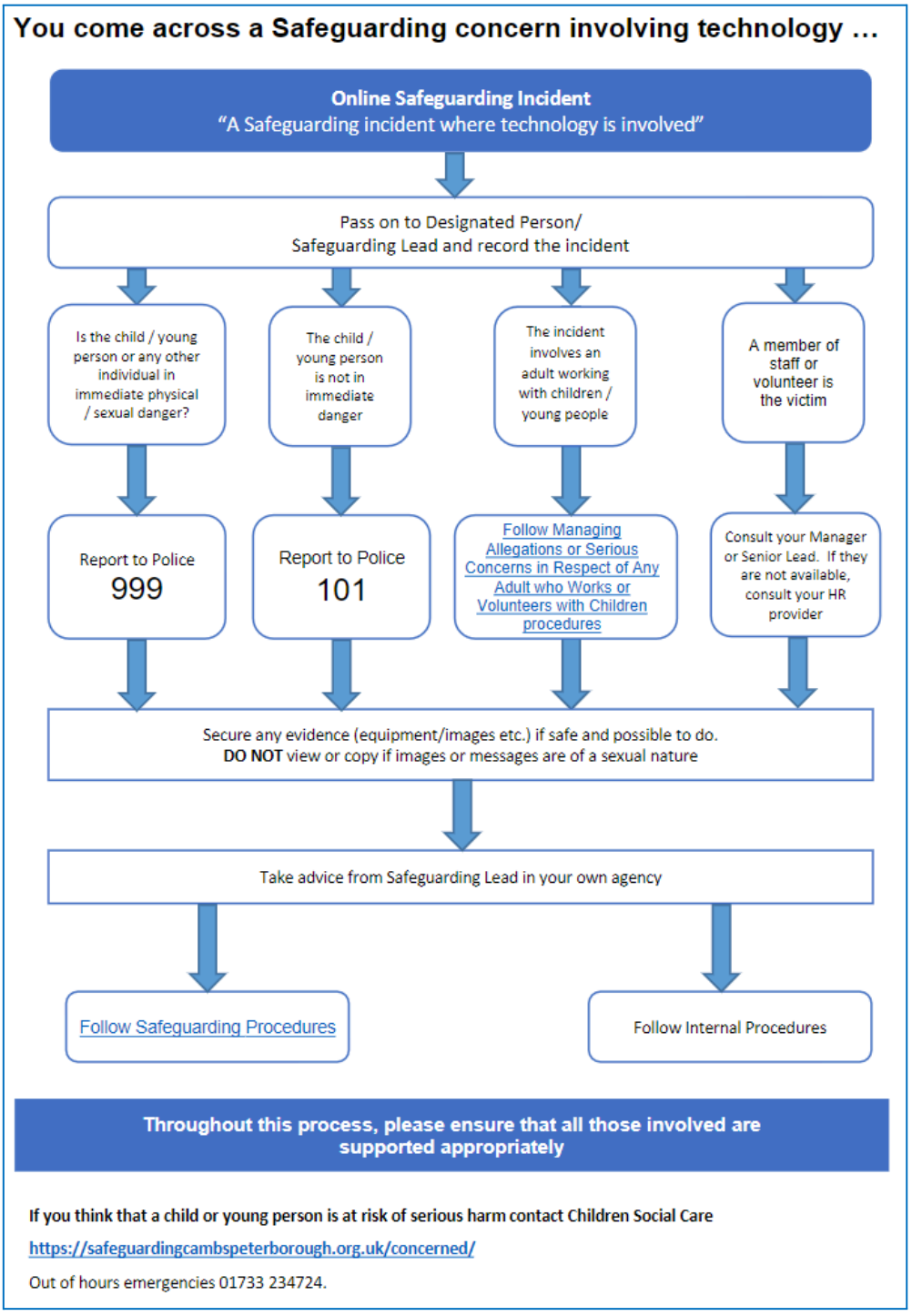
However, there is a risk that this could conflict with guidance about dealing with incidents where a child may be at risk where it may be inadvisable to delete, save or share content. The school will always seek to resolve areas of concern in line with safeguarding procedures, and with parents where appropriate, before taking any further action.

NB: In our school, the likelihood of these types of instances occurring are already reduced as we don't allow pupils to use personal devices in school.

Appendix A: Flowchart of safeguarding procedures following

Where the school suspects that an incident may constitute a Safeguarding issue, the usual Safeguarding procedures will be followed. This process is illustrated below.

Figure 1. Responding to a Safeguarding Incident where Technology is Involved



New Children Board Procedures | Cambridgeshire and Peterborough Safeguarding Partnership Board (safeguardingcambspeterborough.org.uk)

Appendix B: Pupil Acceptable Use Agreement

Fenstanton and Hilton Primary School

Acceptable Use Agreement

- ✓ I will only access computing equipment when a trusted adult has given me permission and is present.
- ✓ I will not deliberately look for, save or send anything that could make others upset.
- ✓ I will immediately inform an adult if I see something that worries me, or I know is inappropriate.
- ✓ I will keep my username and password secure; this includes not sharing it with others.
- ✓ I understand what personal information is and will never share my own or others' personal information such as phone numbers, home addresses and names.
- ✓ I will always use my own username and password to access the school network and subscription services such as Purple Mash.
- ✓ In order to help keep me and others safe, I know that the school checks my files and the online sites I visit. They will contact my parents/carers if an adult at school is concerned about me.
- ✓ I will respect computing equipment and will immediately notify an adult if I notice something isn't working correctly or is damaged.
- ✓ I will use all communication tools such as email and blogs carefully. I will notify an adult immediately if I notice that someone who isn't approved by the teacher is messaging.
- ✓ Before I share, post or reply to anything online, I will T.H.I.N.K.

  T = is it true?
  H = is it helpful?
  I = is it inspiring?
  N = is it necessary?
  K = is it kind?

- ✓ I understand that if I behave negatively whilst using technology towards other members of the school, my parents/carers will be informed and appropriate actions taken.

I understand this agreement and know the consequences if I don't follow it.

My Name: Class:

Parent/Carer Signed: Today's Date:

Appendix C: Parent Carer Acceptable Use Agreement

Fenstanton and Hilton Primary School

Acceptable Use Agreement

(For Parents/Carers)

Background and purpose

With access to rich dynamic content, connectivity across the globe, a platform for creativity and a place to engage in debate, digital technologies provide a powerful tool for learning. It is therefore essential that children are fully equipped to have the skills and knowledge to safely access and use digital technologies.

This Parent/Carer Acceptable Use Agreement is intended to help share the importance that the school places on keeping children safe with particular regard to online safety. It additionally intends to encourage parents/carers to be actively involved in their child's online safety education, including encouraging transparent behaviour, critical thinking and reporting.

The school will aim to provide every child with the best access it can to online technologies. Filtering, monitoring and alert systems will be in place to help protect children from unnecessary risks. The school will actively encourage children to think critically about content and communication from others and develop strategies for recognising inappropriate content/behaviours and how to deal with them. In return, the school expects the children to demonstrate that they are responsible users of digital technologies at all times.

Parents/Carers

We ask parents and carers to support us by:

- ✓ Sharing good online behaviours with your child.
- ✓ Emphasising the importance of the Acceptable Use Statements/School's rules your child has agreed to.
- ✓ Highlighting the importance of accessing only age-appropriate content and sites along with the pitfalls of social media.
- ✓ Explaining how to keep an appropriate digital footprint.
- ✓ Discussing what is and isn't appropriate to share online.
- ✓ Emphasising never to meet anyone online nor trust that everyone has good intentions.
- ✓ Reporting any concerns you have whether home or school based.
- ✓ Stressing the importance of openness when being online and that no one should ever be too ashamed or embarrassed to tell a trusted adult if they have seen/shared anything concerning or have had inappropriate online contact.
- ✓ Drawing up an agreement of online safety rules for outside of school that are applicable even when your child is at a friend's home.
- ✓ Avoiding posting or replying to any comments about the school to social media that may have a negative impact. Any concerns or worries should be reported to the school in the first instance.

Permission Access

By signing below, you agree to allowing your child access to the school's internet and ICT systems. This also includes any educational subscription services. You are also aware that your child has signed/agreed to the school's Acceptable Use Agreement for pupils.

Your Child's Name: _____ **Class:** _____

Parent's/Carer's Signature: _____ **Date:** _____

*The school aims to comply with GDPR regulations at all times and as such follows strict protocol about how we use personal data and keep it safe, including the information on this form. It is important that you refer to the school's data protection policy or contact the school if you have any questions about data.