Ely St. John's Primary School

Online E-Safety Policy

(September 2023)

Ely St. John's Primary School - Online E-Safety 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 e-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
- Personal Social and Health Education (PSHE)
- Safer Working Practices
- Data Protection / GDPR Policy
- Anti-Bullying Policy
- School Complaints Procedure
- Whistle Blowing Policy

This policy must be read alongside the staff and pupil Acceptable Use Policies (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 in September 2023 and will be formally reviewed by September 2025.

Ely St. John's Primary School - Online E-Safety Policy

- 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 and is readily available on the school network, website, and has also been made available to parents.

- All staff must be familiar with this policy and all staff and pupils must sign the relevant Acceptable Use Policy before being allowed to access school's systems (see appendices). 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.

Rationale

At Ely St. John's, 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, 2023)* 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 and desktops in the office and ICT Suite including staff level internet access, server access and access to MIS systems.

Ely St. John's Primary School - Online E-Safety Policy

- Some staff have access to MIS systems from home via a secure logon and key fob. Staff laptops can also be used at home in accordance with the staff AUP.
- Curriculum iPads for preparing and delivering pupil activities
- Class cameras and other peripherals such as visualisers and Interactive Whiteboards

Pupils:

- Curriculum iPads and desktops in the ICT Suite including filtered access to the Internet and pupil level access to areas of the school network
- Cameras and peripherals including programming resources (Beebots, Makey Makeys, control equipment, class cameras etc.)
- School website
- School YouTube account

Parents:

- School website
- School Twitter/'X' account
- School YouTube account
- Zoom

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 Ely St. John's, we believe that a comprehensive programme of online e-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 so they will learn safe life-long online behaviours by accessing and using a range of online services including the World Wide Web.

- **At KS1:** use technology safely and respectfully, keeping personal information private; identify where to go for help and support when they have concerns about content or contact on the internet or other online technologies.
- **At KS2:** use technology safely, respectfully and responsibly; recognise acceptable/unacceptable behaviour; identify a range of ways to report concerns about content and contact.

Our online safety curriculum is based on the Cambridgeshire Progression in Computing Capability Materials, 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 platform.
- 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.

Parents:

- We expect our parents to be aware of e-safety for their children and to regularly monitor the sites children are using. We also expect parents to behave responsibly on social media with regards to our Consent Form For Photography/videos and Images of Children;

When responding to school news and communication on school media sites;

- Parents should not bring the school into disrepute or undermine the reputation of the school on social media
- Parents should not write defamatory or knowingly false information about the school
- Parents should not discuss other children in a public forum
- Parents must respond positively or constructively on school social media sites

School website:

Schools are required to publish certain information online – which in practice means you must have a school website. You are not however required to develop a website policy but sometimes the boundaries of responsibility for setting up, maintaining and ownership of the content are blurred and this can lead to difficulty.

The main purpose of our school website is to provide information and to provide a forum to celebrate learning and achievement. Our school website will not only tell the world that our school exists, but it will provide information our pupils and parents, promote the school to prospective ones and publish the statutory information required by the Department for Education.

In conjunction with a range of online services, a school website can be used to showcase examples of pupils' work - in words, pictures, sound or movie clips - and can share resources for teaching and learning both within the school and with colleagues elsewhere.

School social media:

The purpose of school social media accounts are to

- Provide additional learning platforms for pupils
- Modernise communication with parents
- Make relevant links with the wider community
- Celebrate / showcase pupil achievement
- Linked to positive mental health in sharing successes and reaching out or signposting to parents

Under safeguarding responsibilities, it is the duty of a school to ensure that every child in their care is safe, and the same principles should apply to the virtual presence of a school as it would apply to its physical surroundings. Head teachers and the Governing Body should therefore take on the responsibility to ensure

Ely St. John's Primary School - Online E-Safety Policy

that no individual child can be identified or contacted either via, or as a result of, a visitor using the school website.

The school should establish clear policies to ensure that its website and media sites are maintained and effective, and do not compromise the safety of the pupils or staff.

The website is audited by Govenors to ensure all statutory aspects are there. Twitter is monitored by staff regularly and governors have overall monitoring responsibility. Key stage leaders to monitor blogs written by their team members to ensure quality and correct safeguarding is in place. The ICT Service provides technical support for the website.

Continued Professional Development

Staff at Ely St. John's 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 (the DSL Team) receive more in-depth online safety training to support them in keeping up to date and reviewing the school's approach, policies and practice.

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 Ely St. John's, pupils are not permitted to use mobile devices on school premises during the school day and such devices are only allowed on the school site in limited and clearly defined circumstance as stated in the 'Mobile Phone Use' section of the school website.

Staff (and other adults) use of mobile phones is made clear in the school 'Acceptable Use Policies' and 'Staff Code of Conduct'.

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:

Ely St. John's Primary School - Online E-Safety Policy

- Secure, private EastNet internet connection with a direct link to the National Education Network. This is provided and maintained 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.

- Smoothwall notification system for filtering and monitoring (pupils and staff)

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 (Smoothwall Notifications)
- Use of additional reporting tools to monitor and investigate pupil use of the Internet.

Staff use of the schools' internet can also be monitored and 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 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 and DSL (the Headteacher).
- 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, Ely St. John's will follow its agreed procedures for responding including internal sanctions and involvement of parents (this 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.

Where the school suspects that an incident may constitute a Safeguarding issue, the usual Safeguarding procedures will be followed.

Where the school suspects that an incident may constitute a Child Protection issue, the usual Child Protection procedures will be followed. This process is illustrated in the diagram below.
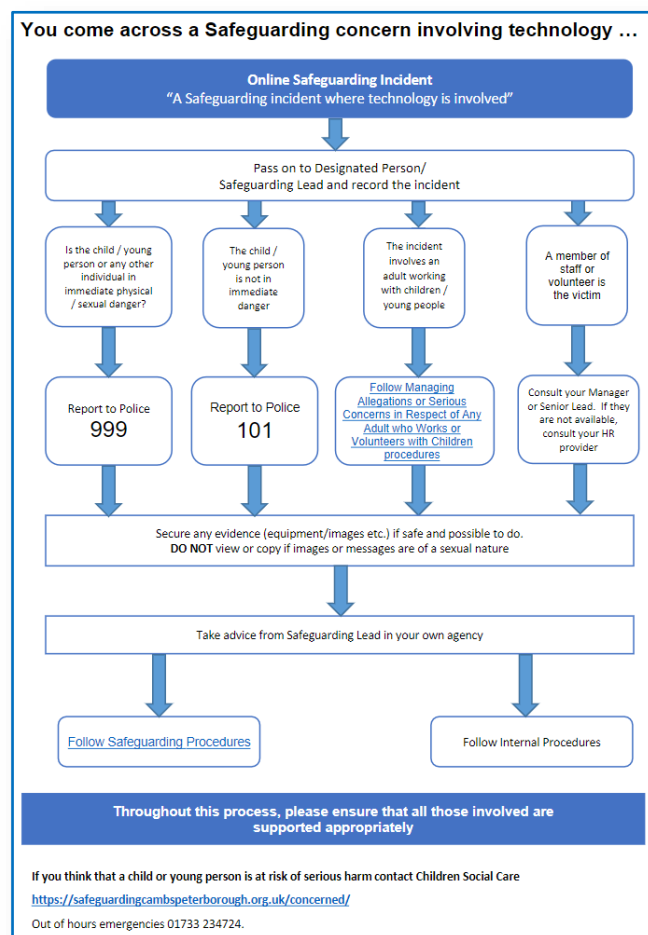
This policy will be reviewed on a yearly basis and in accordance with the following on an as and when required basis:

- Legislative changes
- Good practice guidance
- Case law
- Significant incidents reported
- KICKSIE document

This process is illustrated below.

Ely St. John's Primary School - Online E-Safety Policy

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

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