Cottenham Primary School

E-safety Policy

Dated:	Spring 1 2026
Reviewed by:	Personnel sub-committee
Next Review date:	Spring 1 2027
Equality Review Checklist	In reviewing this policy due consideration must be given to the impact that changes may have on issues of equality for the protected groups: Age Disability Religion or belief Race Pregnancy and Maternity Sex Sexual orientation Gender reassignment Marriage/civil partnerships If the equality of a protected group is likely to be compromised by changes to the policy then please complete an equality risk assessment, tick in the box and circle the characteristics affected: ☐

Cottenham Primary School
E-safety Policy

Contents

- The background to this policy
- Rationale
- The e-safety curriculum
- Continued Professional Development
- Monitoring and preventing e-safety incidents
- Responding to e-safety incidents
- Appendices (including AUPs)

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 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 monitoring and preventing and responding to e-safety incidents
- A progressive, age-appropriate e-safety curriculum for all pupils

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

- Safeguarding and Child Protection Policy
- Personal Social and Health Education (PSHE)
- Safer Working Practices
- Data Protection Policy
- Anti-Bullying Policy
- Complaints Policy
- Whistleblowing Policy

This policy must be read alongside the CPS **ICT Acceptable Use Policy**, the **Device and Technology Acceptable Use Guidance for Pupils** and the **Device and Technology Acceptable Use Agreement for Staff**. These acceptable use documents outline the expectations and sanctions which apply to staff and pupils using technology.

- The development of our e-safety policy involves:
  - The Headteacher
  - The Designated Safeguarding team
  - The Computing Senior Curriculum Lead and the Computing Curriculum Co-ordinator
  - Cambridgeshire Local Authority Advisor (Cambridgeshire Education ICT Service)
  - The Governor(s) responsible for Safeguarding

- This policy may also be partly reviewed and/or adapted in response to specific e-safety incidents or developments in the school's use of technology. It is shared with all staff and is readily available on the school network and website.

- All staff must be familiar with this policy, and all staff must sign the relevant **Device and Technology Acceptable Use Agreement for Staff** before being allowed to access the school's systems. All staff should also re-sign the Staff Declaration Form (Appendix A of the **ICT Acceptable Use Policy**) annually. The **Device and Technology Acceptable Use Guidance for Pupils** will be shared with all parents and carers annually. As e-safety is an important part of strategic leadership within the school, 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.

Rationale:

- At Cottenham Primary School we believe that the use of technology in schools 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 these 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 use of these new technologies can put young people at risk within and outside the school.
The risks they may face can broadly be categorised into the '3 C's', **Contact**, **Content** and **Conduct** 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
- 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 of music or video files
- The potential for excessive use 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. E-safety issues can also affect adults who work at 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 computers including staff level internet access, server access and access to MIS systems.
- Some staff have access to MIS systems from home via multi-factor authentication (MFA), a multi-step account login process that requires users to enter more information than just a password. Staff laptops can also be used at home in accordance with the **ICT Acceptable Use Policy**.
- Curriculum iPads for preparing and delivering pupil activities
- Class cameras and other peripherals such as visualisers and interactive whiteboards

Pupils:

- Curriculum iPads and laptops, including filtered access to the internet and pupil-level access to areas of the school network
- Cameras and peripherals including programming resources (Beebots, control equipment, class cameras etc.)

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

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

- **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.

At Cottenham Primary School we believe that a comprehensive programme of 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, they will learn safe life-long online behaviours by accessing and using a range of online services including the world wide web.
This is achieved using a combination of:

- Discrete and embedded activities drawn from a selection of appropriate materials.
- Our programme for e-safety education is evidenced in teachers' planning either as discrete or embedded activities.
- Key e-safety messages are delivered and reinforced through cross-curricular opportunities, such as researching and podcasting.

Continued Professional Development:

- Staff at Cottenham Primary School receive up-to-date information and training on e-safety issues in the form of staff meetings and updates from the Computing Senior Curriculum Lead and Curriculum Co-ordinator, as well as training from external providers, where appropriate.
- New staff receive information on the school's **ICT Acceptable Use Policy** as part of their induction.
- All staff have been made aware of their individual responsibilities relating to the safeguarding of children within the context of e-safety and know what to do in the event of the misuse of technology by any member of the school community.
- All e-safety incidents will be logged by the school.

School website:
The main purpose of our school website is to provide information. Our school website will not only tell the world that our school exists, but it will provide information to our pupils and parents, promote the school to prospective parents 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.

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 apply to its physical surroundings. The Headteacher and the Governing Body therefore take on the responsibility

of ensuring that no individual child can be identified or contacted either via, or because of, a visitor using the school website.
The school should establish clear policies to ensure that its website is maintained, is effective, and does not compromise the safety of pupils or staff.

Monitoring, and averting e-safety incidents:
The school keeps children safe when using online technologies through a combination of e-safety education, filtering and monitoring children's online activity and reporting incidents, including following Child Protection procedures, where appropriate.
The school's technology infrastructure is designed to minimise the risks associated with adult and pupil use of technology. This is provided and maintained by Jisc and the Local Authority's Education ICT Service. Safeguards built into the school's infrastructure include:

- A secure, private internet connection provided to the school through Jisc's JANET network and The ICT Service's wraparound services
- A Palo Alto PA-440 firewall.
- Baseline and enhanced filtering provided by the approved Netsweeper filtering system.
- CPSN-provided Sophos antivirus package.
- Email system for all school staff protected with MFA and Acronis email security (powered by Perception Point) helping prevent all email-borne threats.
- Restrictions on download of software, apps and file types from known compromised sites.

Staff also monitor pupils' use of technology and, specifically, the internet:

- Pupils' use of online services (including the world wide web) is supervised in school at all times.
- Pupils are not permitted to bring in their own devices. In the exceptional circumstance of them bringing in their own device they are to be handed into the School Office and collected at the end of the school day.

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

- All staff and pupils from Y3 upwards have individual, password-protected logins to the school network.
- The school's network can either be accessed using a wired or wireless connection. However, 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 generally not permitted to connect personal devices to the school's main wireless network and a guest wireless key is issued to staff and visitors on a case-by-case basis to access the school's secondary wireless network.

Whilst we recognise that it is impossible to completely eliminate the risks associated with the use of technology, these safeguards are in place to help minimise these risks as much as possible.

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

Staff responses to e-safety incidents must be consistent with responses to other incidents in school. This may mean that serious actions must be taken in some circumstances.

If an e-safety incident occurs, Cottenham Primary School will follow its agreed procedures for responding, including internal sanctions and involvement of parents. This may include the deactivation of accounts or restricted access to systems.

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 away from 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 e-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 sanctions and/or procedures to incidents which occur outside of school, if they deem 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 with parents (where appropriate) before taking any further action.

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 child protection issue, the usual child protection procedures will be followed. This process is illustrated in **Appendix A**.

APPENDIX A

You come across a child protection concern involving technology …

