Online Safety Policy

Reviewed by:	Teaching & Learning Committee
Reviewed when	January 2025
Next review	January 2026
Source and date of model policy, if applicable	The ICT Service
Added to website (if applicable)	Yes
Added to Google Drive – All Staff	Yes
Added to G Drive	Yes
Review date noted on schedule	Yes

Please note that references to the Headteacher can also be taken to mean Executive Headteacher or Head of School. References to the Chair of the Governing Body may refer to Co-Chairs of the Governing Body.

This policy takes into account guidance from:

- Teaching Online Safety in Schools guidance – DfE, June 2019
- Education for a Connected World – UKCIS, June 2020
- National Curriculum in England - Computing - DFE, Sept 2014
- Relationships and Health Education – DfE, July 2020

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 Federation and followed by the whole Federation 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
- Complaints Procedure
- Cambridgeshire Progression in Computing Capability Materials
- Whistleblowing Policy

This policy must be read alongside the Acceptable Use Policy (AUP). The AUP outlines the expectations which apply to staff use of technology.

- This policy may also be partly reviewed and/or adapted in response to specific online safety incidents or developments in the Federation's use of technology.

- All staff must be familiar with this policy and must sign the relevant Acceptable Use Policy before being allowed to access Federation's systems. As Online safety is an important part of our Federation's approach to safeguarding, all staff have a shared responsibility to ensure that the policy and practices are embedded.

Rationale

At The Trumpington Federation 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 misuse of technology can put young people at risk within and outside school.

The risks they may face can broadly be categorised into the '4 C's' **Contact**, **Content, Conduct** and **Commerce** (Livingston and Haddon) 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
- 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 Federation and this will be referenced in more detail later in this policy.

Technologies regularly used by pupils and staff include:

Staff:

- Staff laptops / iPads / Chromebooks / desktops - staff devices can also be used at home in accordance with the staff AUP, particularly with regard to GDPR.
- Staff / some staff have access to Federation systems beyond the school building (e.g. MIS systems, cloud platforms e.g. Microsoft 365 or Google Workspace).
- Class cameras and other peripherals such as visualisers and Interactive Whiteboards
- Staff level internet access
- Twitter and Instagram accounts
- Federation website

Pupils:

- Curriculum laptops / iPads / Chromebooks / desktops including filtered access to the Internet and pupil level access to areas of the Federation network
- Cameras and peripherals including programming resources
- Cloud platforms such as Google Classroom / online tools providing pupils with access within and beyond the school gates such as Accelerated Reader, Times Tables Rockstars

Where the Federation 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.

IMPLEMENTATION

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 The Trumpington Federation 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, so 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 Cambridgeshire PSHE Service Primary Personal Development Programme, with reference to UKCIS's Education for a Connected World. We also refer to the Computing And Schools Scheme in the development of our curriculum.

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.

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 Federation community. We regularly update our online safety curriculum to reflect developing national concerns (for example 'fake news', viral scares and generative AI).

Monitoring, and averting online safety incidents

The Federation 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 Federation's technology infrastructure is designed to minimise the risks associated with adult and pupil use of technology. This is provided and maintained by The ICT Service on behalf of the local authority. Safeguards built into the Federation's infrastructure include:

- Secure, private EastNet internet connection to each school with a direct link to the National Education Network.

- Managed firewalling running Unified threat management (UTM) that provides restrictions on download of software, apps and file types from known compromised sites.

- Foundation DDoS mitigation service, security analysts carefully monitor the patterns of traffic across the network.

- Enhanced web filtering provided to all EastNet sites as standard.

- Optional SSL decryption available on web traffic to allow for greater visibility of sites being accessed and requested.

- Antivirus package provided as part of EastNet Connection.

This will alter with changes to the school's broadband provision in March 2025; however, the same standard of filtering and monitoring will be continued.

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
- Use of additional reporting tools to monitor and investigate pupil use of the internet

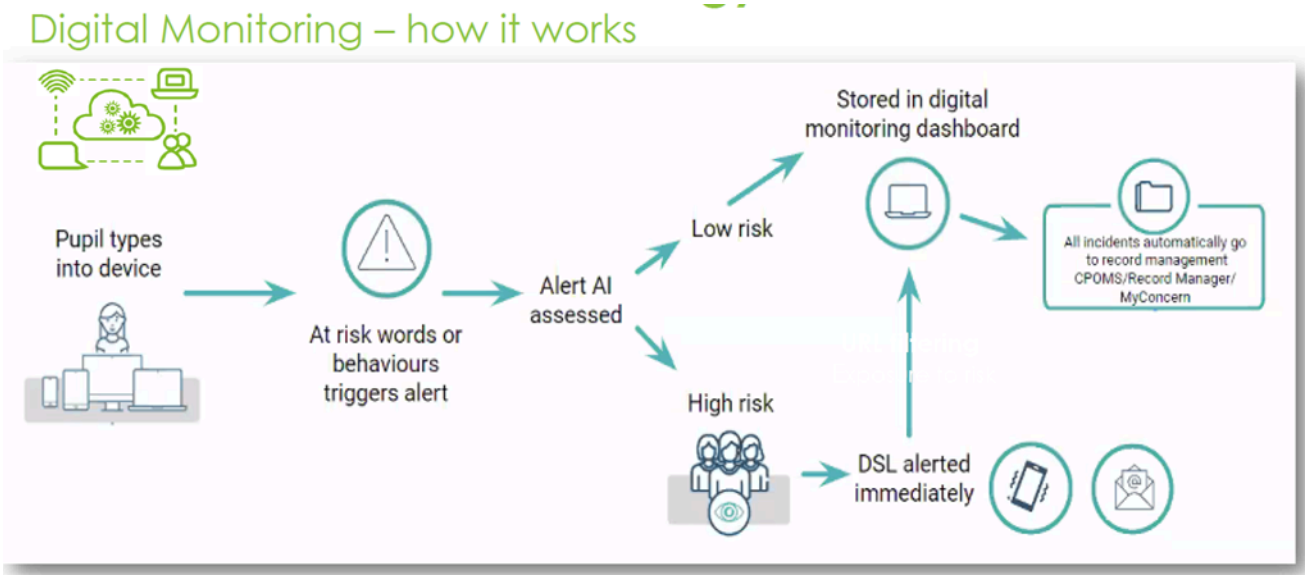
Staff use of the Federation's internet can also be monitored and investigated where needed.

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

- All members of staff have individual, password protected logins to the Federation network / cloud service / MIS systems.
- Visitors to the Federation, such as supply teachers, can access part of the Federation 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.
- Children have individual Google logins. Functions of the Google suite which are not appropriate for use by children are disabled for all pupils.

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

The ICT Service graphic below demonstrates how digital monitoring works within the Federation:



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, The Trumpington Federation 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 Federation'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 Federation community.

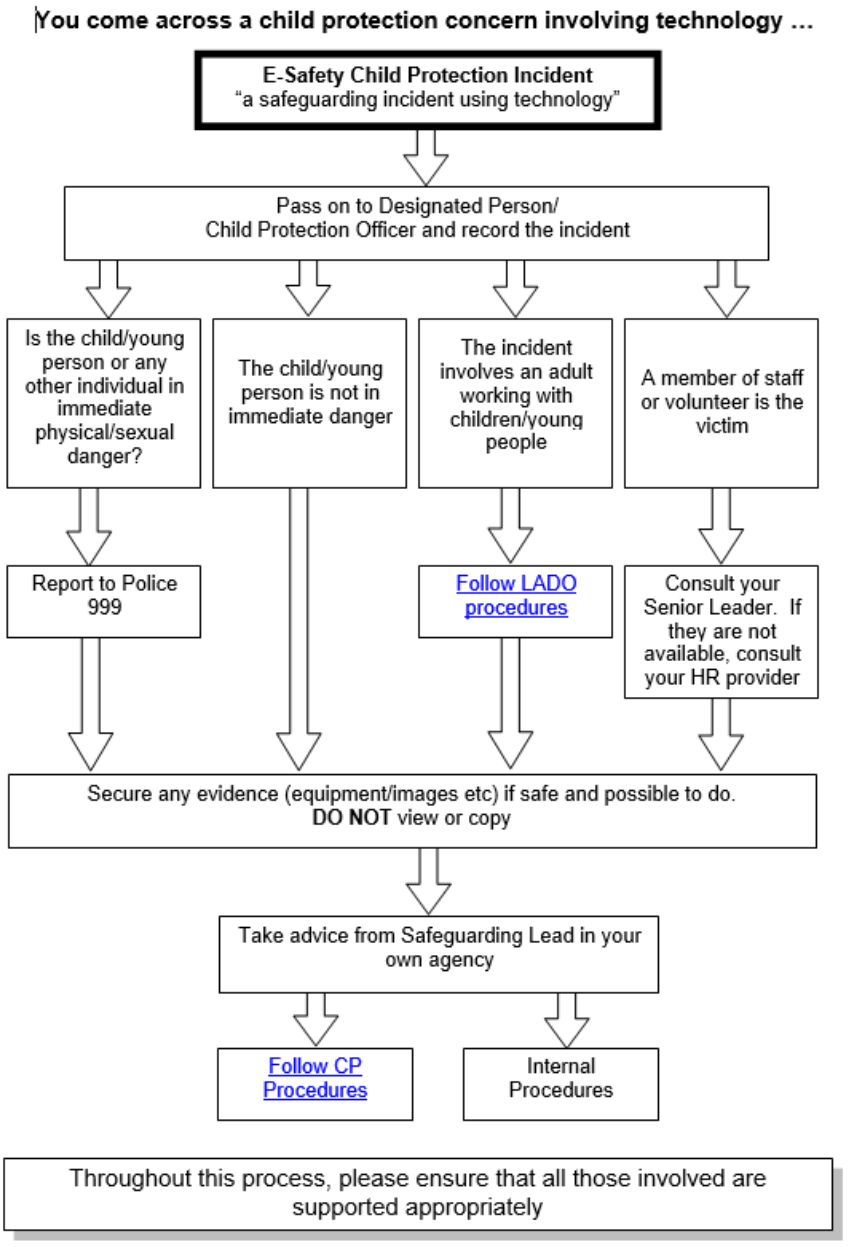
- With this in mind, the Headteacher may decide to apply the sanctions and / or procedures in the relevant AUP to incidents which occur outside of schools if s/he deems it appropriate.

The Education Act 2011 gives school staff the powers, in some circumstances, to search personal digital devices and decide whether or not 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 Federation will always seek to resolve areas of concern in line with safeguarding procedures, and with parents where appropriate, before taking any further action.

In our Federation, the likelihood of these types of instances occurring are already reduced as we do not allow pupils to use personal devices in school. Older children who can walk home alone are permitted to bring their device to school but this must be handed in at the start of the day and stored in the school office.

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



Radicalisation

Radicalisation is the process by which a person comes to support terrorism and extremist ideologies associated with terrorist groups. This process can occur through direct recruitment, e.g. individuals in extremist groups identifying, targeting and contacting young people with the intention of involving them in terrorist activity, or by exposure to violent ideological propaganda. Children who are targets for radicalisation are likely to be groomed by extremists online to the extent that they believe the extremist has their best interests at heart, making them more likely to adopt the same radical ideology.

Staff members will be aware of the factors which can place certain pupils at increased vulnerability to radicalisation, as outlined in the Prevent Duty Policy. Staff will be expected to exercise vigilance towards any pupils displaying indicators that they have been, or are being, radicalised.

Where staff have a concern about a pupil relating to radicalisation, they will report this to the DSL without delay.

This policy is to be read alongside the following policies:

- Anti Bullying
- Behaviour
- Safeguarding and Child Protection
- Supporting Children with Medical Conditions
- Code of Conduct for All Adults in School
- Equality Objectives
- Relationships and Sex Education