



Growing and Learning Together

Online Safety Policy

Please note that 'Headteacher' may refer to the Executive Headteacher or Head of School. 'Chair of Governing Body' may refer to Co-Chairs of the Governing Body.

Reviewed by:	Teaching & Learning Committee
Reviewed when	June 2026
Next review	June 2028
Source and date of model policy, if applicable	The ICT Service v.July 2024
Added to website (if applicable)	Yes
Added to Google Drive – All Staff	Yes
Review date noted on schedule	Yes

Contents

Background to this policy	4
Rationale	6
The online safety curriculum	8
Continued professional development	9
Mobile phones and use of mobile data in school	10
Monitoring and averting online safety incidents	11
Responding to online safety incidents	13
Appendix 1: Cambridgeshire & Peterborough Safeguarding Partnership Board Procedure	14

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 schools 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
- Complaints Procedure
- Cambridgeshire Progression in Computing Capability Materials
- Whistle Blowing Policy
- Artificial Intelligence policy

This policy considers guidance from:

- Meeting digital and technology standards in schools and colleges DfE March 2023
 - Teaching Online Safety in Schools guidance – DfE, January 2023
 - Education for a Connected World – UKCIS, June 2020
 - National Curriculum in England - Computing - DfE, Sept 2013
 - Relationships and Health Education – DfE, July 2020
-

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

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

- 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 the 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 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 2025) 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 / iPads / Chromebooks / desktops - staff devices can also be used at home in accordance with the staff AUP, particularly with regard to data protection.
- Some staff have access to school 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
- Instagram account

- Federation website

Pupils:

- Curriculum laptops / iPads / Chromebooks / desktops including filtered access to the Internet and pupil level access to areas of the school network
- Cameras and peripherals including programming resources
- Cloud platforms / online tools providing pupils with access within and beyond the school gates
- 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
- Year 5 and 6 bringing phones into school

Where the Federation 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 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 by doing 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 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.

Continued professional development

In accordance with KCSiE guidance, staff at the Trumpington Federation receive safeguarding and child protection training at induction. This training covers online safety which, amongst other things, includes an understanding of the expectations, applicable roles and responsibilities in relation to filtering and monitoring. Safeguarding, child protection and online safety training is regularly updated during staff meetings and through updates from the school's online safety and Designated Safeguarding Leads, as well as training from external providers where appropriate.

The Trumpington Federation will identify a member of the senior leadership team and a safeguarding governor, to be responsible for ensuring the DfE filtering and monitoring standards are met. These identified individuals will receive more in-depth online safety training to support them in keeping up to date and reviewing the Federation's approach, policies and practice.

New staff receive information on the Federation'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 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"*. Please see our Mobile Phones policy for more information.

Artificial intelligence (AI)

Generative AI tools are now widespread and easy to access. Staff, pupils and parents/carers may be familiar with generative chatbots such as ChatGPT and Google Gemini.

The Trumpington Federation recognises that AI has many uses to help pupils learn, but may also have the potential to be used to bully others. For example, in the form of 'deepfakes', where AI is used to create images, audio or video hoaxes that look real. This includes deepfake pornography: pornographic content created using AI to include someone's likeness.

The Trumpington Federation will treat any use of AI to bully pupils very seriously, in line with our anti-bullying/behaviour policy.

Staff should be aware of the risks of using AI tools while they are still being developed and should carry out a risk assessment where new AI tools are being used by the Federation, and where existing

AI tools are used in cases which may pose a risk to all individuals that may be affected by them, including, but not limited to, pupils and staff.

Any use of artificial intelligence should be carried out in accordance with our AI usage policy.

Please see our Mobile Phones and Smart Devices policy [here](#)

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 school's technology infrastructure is designed to minimise the risks associated with adult and pupil use of technology. We provide a secure internet connection, firewalling and filtering. Staff also monitor pupils' use of technology and, specifically, their activity online. This is achieved through a combination of appropriate levels of supervision, auto-generated alerts which flag up activity in specific safeguarding categories which may raise child protection concerns in conjunction with appropriate reporting tools where necessary.

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

- All members of staff have individual, password protected logins to the school network / cloud service / MIS systems.
- All pupils have individual, password protected logins to the school network
- 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.
- 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 totally 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, we will follow 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 1: Cambridgeshire & Peterborough Safeguarding Partnership Board Procedure).

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. When incidents such as these may occur we refer to our behaviour policy: 'The Federation also considers the behaviour of children online to be the responsibility of parents. However, the Federation may sanction pupils where their online behaviour poses a threat or causes harm to another pupil, where their behaviour could have repercussions for the orderly running of the school, where the pupil is identifiable as a member of the school or where their behaviour could adversely affect the reputation of the school.'

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 and 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.

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.

Appendix 1: Cambridgeshire & Peterborough Safeguarding Partnership Board Procedure

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

If you think that a child or young person is at risk of serious harm contact Children Social Care
<https://safeguardingcambspeterborough.org.uk/concerned/>

Out of hours emergencies 01733 234724.