Cambridge Nursery Federation

Brunswick | Colleges | The Fields

Online Safety Policy

School Name	Cambridge Nursery Federation
Date Approved	September 2025
Review Date	October 2026
Agreed and Signed by Headteacher	
Name	Ruth Holman
Agreed and Signed by Chair of Governors	Carolyn Purser
Name	Carolyn Purser

"An effective whole Federation approach to online safety empowers an individual Nursery school, within the Federation, I to protect and educate pupils, students, and staff in their use of technology"

(Keeping Children Safe in Education 2023)

It is essential that your Online Safety Policy shows your school's ability to:

- protect and educate pupils and staff in their use of technology
- have the appropriate mechanisms to intervene and support any incident where appropriate.

(Inspecting online safety in Schools, Ofsted 2014)

___

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

___

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
- Data Protection / GDPR Policy
- Whistle Blowing Policy

This policy must be read alongside the staff Acceptable Use Policy (Appendix 1). This AUP outline the expectations and sanctions which apply to staff and pupil use of technology.

The development of our online safety policy involved:

- The Executive Headteacher
- The Designated Safeguarding Lead
- Cambridgeshire Local Authority Advisor (The ICT Service)
- The governor responsible for Safeguarding

It was presented to the governing body in September and will be ratified at the Full Governing Body meeting in October 2025 and will be formally reviewed in October 2026

- 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 email and a staff meeting and is readily available on the school website and has 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 Executive Headteacher, the Designated Safeguarding Lead and governors as appropriate.

Rationale

At **Cambridge Nursery 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. See Appendix 2 for AI Policy.

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.

Online safety issues 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, desktops - staff devices can also be used at home in accordance with the staff AUP, particularly regarding GDPR.
- Some staff have access to school systems beyond the school building (e.g. MIS systems, cloud platforms e.g. Microsoft 365 or Google Workspace).
- Staff level internet access
- Some staff have access to Nursery Social media platforms
- Third-party applications integrated with school accounts such as Learning Journals

Pupils:

- **Staff iPads, including filtered access to the Internet.**

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 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.

At **Cambridge Nursery 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 Department for Education Help for Years website:

https://help-for-early-years-providers.education.gov.uk/health-and-wellbeing/internet-safety

This is achieved using a combination of:

- Focus events to raise the profile of online safety for our pupils and school community
- A flexible curriculum which can respond to new challenges as they arise.

Continued professional development

In accordance with KCSiE guidance, staff at **Cambridge Nursery Federation,** receive safeguarding and child protection training at induction and annually thereafter. 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.

Cambridge Nursery Federation will identify a member of the senior leadership team and a 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 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 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 Appendix 3 for the mobile phones and other devices policy.

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 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 sites as standard.
- Antivirus package provided as part of Connection.

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.
- 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, governors, visitors, parents and pupils are not permitted to connect personal devices to the school's wireless network

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, **Cambridge Nursery 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 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.

- 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.

NB: In our federation, the likelihood of these types of instances occurring are already reduced as we do not allow pupils or their families to use personal devices in the nursery schools.

Appendix 1: Acceptable Use Policy
Appendix 2: AI Policy
Appendix 3: Mobile phones and other devices Policy