

Cambian Spring Hill School

Safeguarding Policy -

(4) Filtering and Monitoring of Digital Technology



Christine Sherman DSL



Samantha Price - Deputy DSL

This policy is written in line with the following legislation and guidance:

- [Keeping children safe in education 2024 \(publishing.service.gov.uk\)](https://www.gov.uk/guidance/keeping-children-safe-in-education-2024)
- <https://www.gov.uk/guidance/meeting-digital-and-technology-standards-in-schools-and-colleges/filtering-and-monitoring-standards-for-schools-and-colleges>
- Meeting digital and technology standards in schools and colleges updated May 2024.
- [Appropriate Filtering and Monitoring - UK Safer Internet Centre](#)

Wider Policies support this Safeguarding Policy. All are numbered and sit alongside to create the school safeguarding policy.

1. Child Protection Policy
2. The Role of the DSL Policy
3. Child on Child Abuse Policy
4. Filtering and Monitoring Policy
5. Managing Low Level Concerns Policy

6. Missing from Education Policy
7. Schools Safer Recruitment Policy
8. Managing Contextual Risks to Children
9. Adult Safeguarding Policy

We also provide education to those over the age of 18 years. This policy is therefore written in line with the Care Act 2014, Mental Capacity Act 2005 and Education Act. Those over the age of 18 are referred to as Students.

Purpose

Our schools are committed to safeguarding and promoting the welfare of children and students by providing a safe environment in which to learn. This policy ensures school staff are doing all they reasonably can to limit children/students exposure to the above risks from the school's/college's IT system.

This policy ensures the leadership team and relevant staff have an awareness and understanding of the provisions in place and manage them effectively, knowing how to escalate concerns when identified.

Governing bodies and proprietors also consider the number of and age range of their children, those who are potentially at greater risk of harm and how often they access the IT system along with the proportionality of costs versus safeguarding risks.

Aims of the policy

1. To ensure that risks linked to digital and technology equipment are assessed
2. Staff are aware of the need to filter and monitor content
3. Staff know how to use the filtering and monitoring equipment
4. Individuals are protected from viewing inappropriate/harmful content
5. Staff know how to report concerns to the DSL
6. The DSL is clear on how to escalate concerns and has clear monitoring checks in place.

What is Filtering?

Filtering by dictionary definition, is 'to remove impurities'. Applied to digital and technology equipment, filtering is a way of allowing people to access some content but block other types of content. The guidance from Meeting digital and technology standards states that your school filtering system 'should block harmful and inappropriate content, without unreasonably impacting teaching and learning'.

What is Monitoring?

Monitoring is to 'observe and check the progress or quality of (something) over a period of time; keep under systematic review'. The guidance from Meeting digital and technology standards states that schools can monitor devices in a number of ways such as:

- physically monitoring by staff watching screens of users

- live supervision by staff on a console with device management software
- network monitoring using log files of internet traffic and web access
- individual device monitoring through software or third-party services

What are the risks?

The office for national statistics (ONS) completed a survey on Children and teenagers online behaviour in England and Wales in 2020¹. The findings of the survey were:

- Almost 9 in 10 children (89%) aged 10 to 15 years said they went online every day.
- Around one in six children (17%) aged 10 to 15 years spoke with someone they had never met before (equivalent to 682,000 children) in the previous 12 months.
- An estimated 1 in 50 children (2%) said that they spoke to or messaged someone online in the previous 12 months who they thought was their age but later found out were much older.
- An estimated 5% of children aged 10 to 15 years met up in person with someone they had only spoken to online (equivalent to 212,000 children) in the previous 12 months.
- Around 1 in 10 children (11%) aged 13 to 15 years reported receiving a sexual message, while 1 in 100 reported sending a sexual message, in the previous 12 months.
- Girls aged 13 to 15 years were significantly more likely to report receiving sexual messages than boys (16% compared with 6%) in the previous 12 months.
- The majority of parents or guardians of children aged 10 to 15 years (64%) had some sort of rules about the length of time and when their children can go online.

Digital media and technology have become embedded in society and is a useful aid to extend children's learning. However, this does come with attached risks. Children/students are becoming more digitally articulate whilst younger children are better able to navigate devices and access online content. It is difficult for staff to keep updated and refreshed on online content and devices. Staff are required to complete regular training and test their knowledge with school leaders as often as possible.

The risks children/students face online include access to:

- pornography or inappropriate sexualised content
- violent pranks or harm caused to others
- radical content ideologies that differ from traditional British values
- content relating to harm to self or suicidal ideologies
- online/cyberbullying
- exploitation and grooming linked to radicalisation, CSE, CCE or modern slavery
- child on child/student on student abuse pressures to share youth produced sexual imagery

¹ [Children's online behaviour in England and Wales - Office for National Statistics \(ons.gov.uk\)](https://ons.gov.uk)

What Filtering and Monitoring Systems are in place?

All schools have Fortinet security. The filtering system is Fortigate and the monitoring system in place is Fastvue.

Fortigate is able to filter harmful content and protect users from Spam or malware attacks. More information about the filtering system can be found [Fortinet Security Solutions for Education](#).

Fast Vue is a tool that alerts the nominated person of online searches being completed by children. The software is able to highlight searches that it may consider harmful or inappropriate whilst sending live alerts to the nominated person responsible for oversight of filtering and monitoring across the school/college. More information on Fastvue; [Fast Vue Reporter for Education. Student online safety, safeguarding and wellbeing](#).

The filtering systems can be tested to give staff an overview of the filtering by accessing the link while on the school system [Test Your Internet Filter | SWGfL Test Filtering](#).

We ensure filtering is tested at least termly on both staff and student accounts to ascertain effectiveness.

The role of staff

When using IT equipment, staff remain vigilant. School/colleges risk assess the use of devices and digital technology, considering the:

- Vulnerability of each pupil/student
- Any known risks with individual children/students (risks of being exposed to radicalisation, CSE, CCE or being bullied)
- Are there individuals within the group who can be easily influenced by others?

When using digital technology, staff consider the purpose of doing so (will the advantage of learning outweigh the potential of exposing a child/student to harmful content).

Staff support children/students to access the internet safely and discuss the risks and measures. Staff inform children/students that they can report inappropriate content (including confidentially if required).

Staff report any concerns regarding harmful/inappropriate content they have seen children/students access, or suspect they have accessed, to the DSL immediately.

KCSiE groups online safety risks into four areas: content, contact, conduct and commerce (sometimes referred to as contract), known as the 4 C's. Staff have these in mind when considering pupil/students are accessing the internet.

The role of the DSL and other identified staff

The DSL works alongside the Principal to ensure processes are in place to enable effective filtering and monitoring practices.

To support schools and colleges to meet this duty, the Department for Education has published filtering and monitoring standards which set out that schools and colleges should:

- identify and assign roles and responsibilities to manage filtering and monitoring systems – this can be a staff member from the Senior Leadership Team who works closely with the DSL to ensure Filtering and Monitoring Standards are met
- review filtering and monitoring provision at least annually. Reviews include the identification of gaps and technical limitations, detailed assessments of vulnerable student groups, such as those with SEND or EAL in addition to the impact of new technologies, particularly generative artificial intelligence (AI)
- block harmful and inappropriate content without unreasonably impacting teaching and learning as in line with recommended blocklists
- have effective monitoring strategies in place that meet their safeguarding needs

Our school/college also has a locality risk assessment in place which takes account of risks relating to Prevent alongside having a Prevent action plan in place.

The DSL ensures that staff undertake filtering and monitoring training to enable them to undertake appropriate action should Fortiguard identify unusual/concerning access, or attempted access to websites of concern. In addition, the DSL monitors immediate alerts to keep abreast of patterns and trends of searches in addition to passing on concerns for actioning.

The Principal and DSL works closely with the IT department. This collaboration is critical to ensure that systems not only function technically but also align with broader safeguarding strategies. If monitoring raises concerns about gaps in filtering, the Principal and/or DSL liaises with the Group Head of IT Kate.Brogan@cambianguroup.com to ensure that risks to pupils/students are reduced, either with increased filter security or tighter monitoring.

When incidents occur, which could relate to Child on Child/Student on Student Abuse (such as youth produced sexual imagery, cyberbullying, harmful sexual content), the DSL refers to the Child on Child/Student on Student policy and where necessary the Child Protection/Adult Safeguarding Policy.

Staff use of mobile phones/devices

Staff are also aware of the following expectations:

- Business internet Filtering and Monitoring systems will be used in order to minimise the risk of exposure to inappropriate material.
- Individuals should not use, move or remove IT equipment without the express permission of staff.
- Removal of system covers e.g. computer cases is forbidden



- Network access must be made via the user's authorised account and password, which must not be given to any other person.
- IT system security must be respected; it is a criminal offence to use a computer for a purpose not permitted by the system owner.
- Individuals will not intentionally visit Internet sites that contain obscene, violent, illegal, hateful or otherwise objectionable materials.
- Individuals will be provided with e-safety training/education.
- Uploading and downloading of non-approved software will not be permitted.
- The location will regularly monitor individuals' computer usage.
- Care Tech reserves the right to check a service user's personal technology – if applicable (including; Desktop computer, Laptop, Tablet, Smartphone and portable media devices (to include USB Media Device, portable HDD, CD, DVD) for inappropriate or malicious content. This information is to be expressly made known to both Individual and relevant persons/professionals.
- Corporate WIFI will be restricted in some locations for individuals and will only be authorised by IT service desk, any access to Corporate WIFI should be appropriately risk assessed and reviewed on a regular basis.

In order to provide appropriate protection to the young people in our services staff members adhere to the following:

- Staff members do not carry personal mobile telephones on them when they are on duty. Mobile telephones are not left on any office desk and are kept in a safe location on silent mode.
- Staff members never allow a child/student to use their personal phone or access data
- Bluetooth is not switched on during shifts
- No photographs of young people are taken on staff mobile telephones
- Staff do not share their personal mobile phone WIFI (Hotspot) to any individual
- Safeguarding and monitoring of the use of IT systems
- Completion of risk assessments and monitoring of corporate WIFI
- Misuse of computer, mobile phones and other IT Technology may result in restriction of services and confiscation.
- Any infringement, misuse or inappropriate content to be reported immediately to the IT service desk and line manager.

Visitor use of mobile phones/device

Visitors are not to be left alone with children unless previously agreed by the Principal / DSL.

- Staff at the school know visitor whereabouts at all times
- Visitors do not make direct contact with children/students met in school by phone, email, letter or by social network sites.
- Visitors do not take photographs of children/students

Children/Students use of mobile phones/devices on school sites (during the school day)

- Children/Students do not use their mobile phone devices during the school/college day unless agreed with the Head Teacher/Principal as part of their support plan.

Children/Students use of mobile phones/devices on school/college sites (outside of education hours)

- Children/Students use their phones outside of educational hours
- Children/Students are encouraged to use the school wifi to use their phones so that content can be monitored.
- Staff remain vigilant around children's/student's use of devices and those with a history of known risks have an up to date risk assessment which remains under review.
- If concerns regarding the content a child/student accesses emerges, staff inform the DSL.
- If there is a change in the child's/student's presentation, staff refer to the child on child abuse/student on student abuse policy in addition to the child protection/adult safeguarding policy for further guidance.

Use of mobile phones/devices off site excursions

- Please refer to the school/college risk assessment/off site activities policy.

Review History

A review will be undertaken annually as a minimum.

However, subject to a significant safeguarding concern this policy and all other attached policies will be reviewed and monitored as part of a lessons learned review.

Reviewed – December 2024 by Laura Dickie, Head of Policy Children's Services with input from Pottersbury Lodge School, Spring Hill School and Lufton College.

Next Review – December 2025

Written by:

This policy was written by Matt Nicholls – Head of Policy Children's Services. It was reviewed by Christina Leath – Group Safeguarding Director, Kate Brogan – Group Head of IT and Russell Edge – Group Data Protection Officer. This policy has been reviewed by the DSL of the School and agreed by the head of the Governance Board.