Grateley House School

Safeguarding - Filtering and Monitoring of Digital Technology Policy
2025-26

Policy Reviewed By	Jean North, DSL
Date of Review	February 2026
Date reviewed/approved by SLT	March 2026
Date of Next Review	March 2027

Jean North
Designated Safeguarding Lead

Eva Pereira
Deputy Designated Safeguarding Lead

Chris Bartel
Deputy Designated Safeguarding Lead

Melissa Morton
Deputy Designated Safeguarding Lead

Purpose

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

This policy ensures the senior 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.

The Governing body 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

- To ensure that risks linked to digital and technology equipment are assessed
- Staff are aware of the need to filter and monitor content
- Staff know how to use the filtering and monitoring equipment
- Individuals are protected from viewing inappropriate/harmful content
- Staff know how to report concerns to the DSL
- 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 our 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 2020[1]. 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.

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

- 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 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

What Filtering and Monitoring Systems are in place?

Grateley House School has Fortinet security. The filtering system is Fortigate and the monitoring system in place is Fastvue. Securus is the live monitoring system which provides screenshots when triggered against a library of word phrases and addressed. All filtering is centrally controlled by Cambian/Caretech and is regularly monitored.

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. Fastvue 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 safeguarding team and the ICT technician responsible for oversight of filtering and monitoring across the school. More information on Fastvue can be found at Fastvue 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 must remain vigilant. The school risk assesses the use of devices and digital technology, considering the:

- Vulnerability of each student

- Any known risks with individual students (risks of being exposed to radicalisation, CSE, CCE or being bullied)
- Whether there are 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 student to harmful content). Staff support students to access the internet safely and discuss the risks and measures. Staff inform students that they can report inappropriate content (including confidentially if required). Staff report any concerns regarding harmful/inappropriate content they have seen students' access, or suspect they have accessed, to the DSL immediately.

KCSiE categorises 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 students access to the internet.

The role of the DSL and other identified staff

The DSL ensures 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.

GHS 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 the above tasks are allocated to a nominated person who has the required knowledge, skills and experience to perform the role. 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 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 DSL liaises with the Group Head of IT Kate.Brogan@cambiangroup.com to ensure that risks to students are reduced, either with increased filter security or tighter monitoring.

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

Staff use of mobile phones/devices

Questions for the DSLs:

- Are staff permitted to have their phones on them during teaching time? If not, are they properly stored and locked away?
- Are Staff following the mobile phone/devices policy?
- Are staff 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.
    - Students should not use, move or remove IT equipment without the express permission of the ICT technician.
    - Should a staff member be concerned that their login details have been compromised they must change their password or contact the ICT technician to do so.
    - 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.
    - Students will not intentionally visit internet sites that contain obscene, violent, illegal, hateful or otherwise objectionable materials.
    - Students will be provided with e-safety training/education.
    - Uploading and downloading of non-approved software will not be permitted.
    - The school will regularly monitor student's computer usage.
    - CareTech 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. However, authorisation can be done at site level if authorised by the Principal who will then advise the ICT technician to apply policy. 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 student to use their personal phone or access data.
- Bluetooth is not switched on during working hours.
- 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 ICT technician who will take immediate action.

Visitor use of mobile phones/device

- Visitors are not to be left alone with students unless previously agreed by the principal.
- Staff at the school know visitor whereabouts at all times
- Visitors do not make direct contact with students met in school by phone, email, letter or by social network sites.
- Visitors do not take photographs of students.

Students use of mobile phones/devices at school

- Students do not use their mobile phone devices during the school day unless agreed with the principal as part of their support plan.
- Student laptops and tablets are not permitted.

Use of mobile phones/devices off site trips/activities

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

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

- Keeping children safe in education 2025 (publishing.service.gov.uk)
- 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.

- Safeguarding and Child Protection Policy
- Safeguarding - Role of the DSL Policy
- Safeguarding - Child on Child Abuse Policy
- Safeguarding - Filtering and Monitoring Policy
- Safeguarding - Managing Low Level Concerns Policy
- Missing from Education Policy
- Schools Safer Recruitment 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.

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.

Signed:

Eva Pereira
Principal

February 2026

Andrew Sutherland
Operations Director - Education Services, CareTech Group
February 2026