WHINFELL SCHOOL

Safeguarding Policy -

(4) Filtering and Monitoring of Digital Technology

Jennifer Carradus – DSL

Paddy Sandham – DDSL

Emma Brown - DDSL

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

- Keeping children safe in education 2023 (publishing.service.gov.uk)
- Meeting digital and technology standards in schools and colleges - Filtering and monitoring standards for schools and colleges - Guidance - GOV.UK (www.gov.uk) Meeting digital and technology standards in schools and colleges updated March 2023.
- Appropriate Filtering and Monitoring - UK Safer Internet Centre

Wider Policies support this Child Protection 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. Absent from Education Policy
7. Schools Safer Recruitment Policy
8. Managing Contextual Risks to Children

Purpose

Our schools / colleges are committed to safeguard and promote the welfare of children and provide them with a safe environment in which to learn. The purpose of this policy is to ensure that school staff are doing all that they reasonably can to limit children's exposure to the above risks from the school's / college's IT system.

This policy is written to ensure that the leadership team and relevant staff have an awareness and understanding of the provisions in place and manage them effectively and know how to escalate concerns when identified.

Governing bodies and proprietors should 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. Children 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/colleges can monitor children's 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's 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.
- 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 are becoming more digitally articulate, 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 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 abuse pressures to share youth produced sexual imagery

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

What Filtering and Monitoring Systems are in place?

All schools / colleges 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 and alert the nominated person. More information on Fastvue Fastvue Reporter for Education. Student online safety, safeguarding and wellbeing. Fastvue also collects all searches into a report which can be monitored by the nominated person.

Dilsten College has a separate filtering and monitoring system in place via Smoothwall Digital Safeguarding Solutions | Smoothwall for Education. Smoothwall is able to filter and alert the nominated person of any searches that it deems to be harmful or inappropriate. Smoothwall also tracks all searches and produces a report.

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

The role of staff

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

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

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

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

Staff are required to report any concerns regarding harmful/inappropriate content they have seen children access, or suspect children 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 must have these in mind when considering pupil/students are accessing the internet.

The role of the DSL

KCSiE 2023 is explicitly clear that it is the appropriateness of any filtering and monitoring systems are be informed by the risk assessment required by the Prevent Duty. The DSL is required to ensure that these systems are included in the local risk assessment. Templates can be found Prevent duty: risk assessment templates - GOV.UK (www.gov.uk).

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
- review filtering and monitoring provision at least annually
- block harmful and inappropriate content without unreasonably impacting teaching and learning
- have effective monitoring strategies in place that meet their safeguarding needs.

It is the role of the DSL to ensure the above roles are allocated to a nominated person who has the required knowledge, skills and experience to perform the role. In addition, it is essential that the DSL monitors the checks at least termly to satisfy themselves that they are aware of patterns and trends of searches.

If this monitoring raises concerns about gaps in filtering, the DSL must liaise with Kate Brogan – Group Head of IT Kate.Brogan@cambiangroup.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 Abuse (such as youth produced sexual imagery, cyberbullying, harmful sexual content), the DSL is required to refer to the policy and if a child protection concern emerges, then to refer to the child protection policy.

Staff use of mobile phones/devices

Questions for the Safeguarding Champions – are staff permitted to have their phones on them during teaching time? If not are they properly stored and locked away?

Staff mobile phone/device policy –

Individuals should complete an Internet access and use agreement form Policy 40.06 (Internet access and use agreement) that outlines:

- 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 expressly forbidden.
- Network access must be made via the user's authorised account and password, which must not be given to any other person.
- The location will regularly monitor individuals' computer usage.
- 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 should be provided with e-safety training/education.
- Uploading and downloading of non-approved software will not be permitted.
- Individuals will not intentionally visit Internet sites that contain obscene, violent, illegal, hateful or otherwise objectionable materials.
- Cambian 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 it is essential for staff members to adhere to the following:

- Staff members should not carry personal mobile telephones on them when they are on duty. Mobile telephones should not be left on office desk. They should be kept in a safe location and kept on silent mode.
- Staff members should never allow a child to use their personal phone or access data
- Bluetooth should not be switched on during this time
- Staff smart watches with built-in technology that provides internet access, text messaging, phone calls and/or have built-in cameras are not to be worn by staff, young people are not to be given access to staff smart watches.
- No photographs or young people should be taken on staff mobile telephones
- No sharing of staff personal mobile phone WIFI (Hotspot) to any individual
- Staff to ensure previous calls are erased for data protection and safeguarding purposes
- 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/devices

- Visitors are not to be left alone with children unless previously agreed by the headteacher / DSL.
- Ensure that staff at the school know your whereabouts at all times
- Do not make direct contact with children met in school by phone, email, letter or by social network sites.
- Do not take photographs of children

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

- Children are not permitted to use their mobile phone devices during the school day unless agreed with the headteacher.

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

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

Use of mobile phones/devices off site excursions

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

Review

This Policy was written on 08 November 2023. A review will be 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.

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, 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.