Addendum to ELT Safeguarding and Child Protection Policy

Filtering and Monitoring
September 2023

Contents

---

1. Aims

Education Learning Trust if committed to having robust filtering and monitoring systems and processes in place, to limit children's and adult's exposure to potentially harmful and inappropriate online material.

These systems are administered either by an external ICT provider or internally by the schools ICT Managers.

Regularly review filtering and monitoring systems and processes, at least annually, to ensure their effectiveness.

Establish clear mechanisms to identify, intervene and escalate an incident, where appropriate

2. Legislation and guidance

This policy is based on the Department for Education's (DfE's) statutory safeguarding guidance, Keeping Children Safe in Education

Filtering and Monitoring standards for Schools and Colleges

Cyber security standards for Schools and Colleges

3. Roles and responsibilities

3.1 The Trust Board

The Trust Board has overall responsibility for monitoring this online safety including filtering and monitoring and holding the headteacher to account for its implementation.

The Trust Board will make sure all staff undergo online safety training as part of child protection and safeguarding training, and ensure staff understand their expectations, roles and responsibilities around filtering and monitoring.

The Trust Board will co-ordinate regular meetings with appropriate staff to discuss online safety, requirements for training, and monitor online safety logs as provided by the designated safeguarding lead (DSL).

The Trust Board should ensure children are taught how to keep themselves and others safe, including keeping safe online.

The Trust Board must ensure the school has appropriate filtering and monitoring systems in place on school devices and school networks, and will regularly review their effectiveness. The board will review the DfE filtering and monitoring standards, and discuss with ICT staff and service providers what needs to be done to support the school in meeting those standards, which include:

- Identifying and assigning roles and responsibilities to manage filtering and monitoring systems;
- Reviewing filtering and monitoring provisions at least annually;
- Blocking harmful and inappropriate content without unreasonably impacting teaching and learning;
- Having effective monitoring strategies in place that meet their safeguarding needs.

The Trustee who oversees online safety is **Helen White** (Chair of Trustees).

All Trustees will:

- Ensure they have read and understand this policy
- Agree and adhere to the terms on acceptable use of the school's ICT systems contained in the ELT ICT Acceptable Use Policy and associated code of conduct.
- Ensure that online safety is a running and interrelated theme while devising and implementing their whole-trust approach to safeguarding and related policies and/or procedures
- Ensure that, where necessary, teaching about safeguarding, including online safety, is adapted for vulnerable children, victims of abuse and some pupils with special educational needs and/or disabilities (SEND). This is because of the importance of recognising that a 'one size fits all' approach may not be appropriate for all children in all situations, and a more personalised or contextualised approach may often be more suitable

3.2 The headteacher

The headteacher is responsible for ensuring that staff understand this policy, and that it is being implemented consistently throughout the school.

3.3 The designated safeguarding lead

Details of the school's designated safeguarding leads (DSL) deputies are set out in the Trust Safeguarding and Child Protection policy, as well as relevant job descriptions.

The DSL takes lead responsibility for online safety in school including filtering and monitoring, in particular:

- Taking the lead on understanding the filtering and monitoring systems and processes in place on school devices and school networks

- Working with the ICT manager to make sure the appropriate systems and processes are in place
- Working with the headteacher, ICT manager and other staff, as necessary, to address any online safety issues or incidents
- Managing all online safety issues and incidents in line with the school's child protection policy
- Ensuring that any online safety incidents are logged on CPOMS and dealt with appropriately in line with this policy
- Updating and delivering staff training on online safety and ensuring training includes up to date information of filtering and monitoring (appendix 1 contains a self-audit for staff on online safety training needs)
- Liaising with other agencies and/or external services if necessary
- Providing regular reports on online safety including filtering and monitoring in school to the headteacher and/or Trust Board
- Undertaking annual risk assessments that consider and reflect the risks children face
- Providing regular safeguarding and child protection updates, including online safety, to all staff, at least annually, in order to continue to provide them with relevant skills and knowledge to safeguard effectively

This list is not intended to be exhaustive.

3.4 The ICT manager

In this document, the ICT Manger relates to the school's ICT Manager or external provider of ICT where ICT management is contracted out. Where ICT management is contracted out, it is the responsibility of the DSL as lead for online safety, to oversee that the following responsibilities are carried out.

The ICT manager is responsible for:

- Putting in place an appropriate level of security protection procedures, such as filtering and monitoring systems on school devices and school networks, which are reviewed and updated at least annually to assess effectiveness and ensure pupils are kept safe from potentially harmful and inappropriate content and contact online while at school, including terrorist and extremist material
- Ensuring that the school's ICT systems are secure and protected against viruses and malware, and that such safety mechanisms are updated regularly
- Conducting a full security check and monitoring the school's ICT systems on a regular basis
- Blocking access to potentially dangerous sites and, where possible, preventing the downloading of potentially dangerous files
- Ensuring that any online safety incidents are logged and dealt with appropriately in line with this policy

This list is not intended to be exhaustive.

3.5 All staff and volunteers

All staff, including contractors and agency staff, and volunteers are responsible for:

- Knowing that the DSL is responsible for the filtering and monitoring systems and processes, and being aware of how to report any incidents of those systems or processes failing by [insert school specific action here]

- Ensuring annual online safety training is carried out and annual updates are read and understood.
- Following the correct procedures by [insert school specific action here] if they need to bypass the filtering and monitoring systems for educational purposes
- Working with the DSL to ensure that any online safety incidents are logged and dealt with appropriately in line with this policy

This list is not intended to be exhaustive.

3.6 Parents/carers

Parents/carers are expected to:

- Be kept informed of what filtering and monitoring systems are in use, so they can understand how the Trust works to keep children safe.
- What their children are being asked to do online, including the sites they will be asked to access and who from the school (if anyone) their child will be interacting with online
- If parents/carers have any queries or concerns in relation to online safety, these should be raised in the first instance with the headteacher and/or the DSL.

3.7 Visitors and members of the community

Visitors and members of the community who use the school's ICT systems or internet will be made aware of this policy, when relevant, and expected to read and follow it. If appropriate, they will be expected to agree to the terms on acceptable use contained in the ELT ICT Acceptable Use Policy and associated code of conduct.

Concerns or queries about this policy can be raised with any member of staff or the headteacher.

4. Monitoring arrangements

Schools will monitor the websites visited by pupils, staff, volunteers, governors and visitors (where relevant) to ensure they comply with the above and restrict access through filtering systems where appropriate.

This policy will be reviewed annually and will be shared with the Trust board.

The review will be supported by an annual risk assessment that considers and reflects the risks pupils face online. This is important because technology, and the risks and harms related to it, evolve and change rapidly.

5. Links with other policies

- This online safety policy is linked to the Trust's:
- Child protection and safeguarding policy
- Disciplinary policy and procedure
- Data protection policy and privacy notices
- Complaints procedure

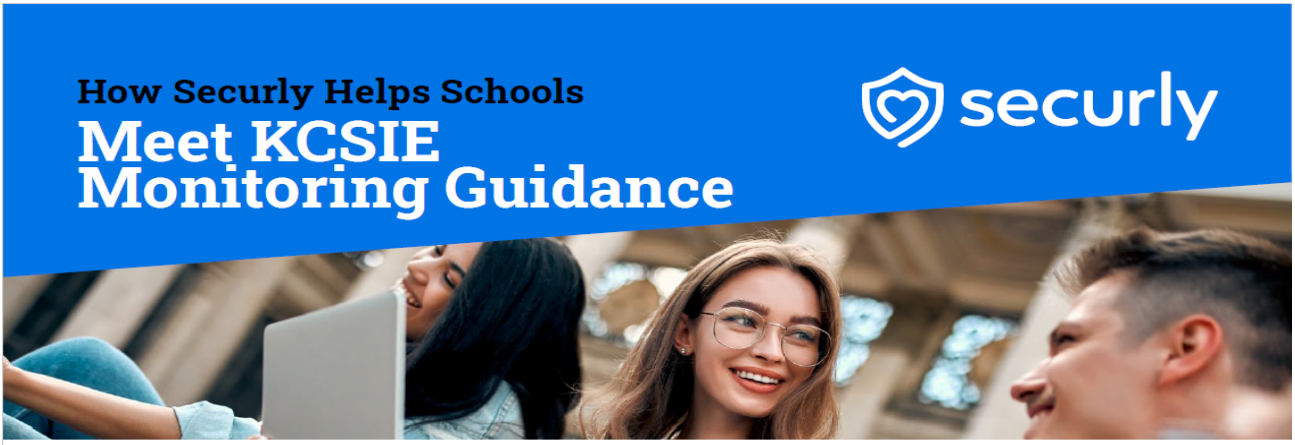
ICT Acceptable Use policy

[Add any other related policies and procedures that the school has here]

- School Behaviour policy

6. Filtering and Monitoring at all Trust Schools (except Werneth) - September 2023

ESItech provide IT support including filtering and monitoring for Bredbury Green Primary, Gatley Primary, Meadowbank Primary and The Kingsway School using **Securly** and **Securly Aware** security and wellness systems:



How Securly Helps Schools
Meet KCSIE Monitoring Guidance

securly

KCSIE guidance says that "monitoring user activity on school and college devices is an important part of providing a safe environment for children and staff. Unlike filtering, it does not stop users from accessing material through internet searches or software".

"A variety of monitoring strategies may be required to minimise safeguarding risks on internet connected devices and may include:"

- Physically monitoring by staff watching the 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.

Securly suite of safety and wellness solutions helps you meet these requirements.

Securly *Aware* is a student safety and wellness solution that provides unprecedented visibility into your students' mental health and wellness. The data provided by Aware can help you understand and meaningfully impact your students' wellness. With Aware, you can:

aware

- Know who's at risk of self-harm, suicide, depression, violence, and bullying.
- React quickly with AI generated instant alerts on student safety issues.
- Proactively support students who demonstrate concerning behaviours.
- Gain a clear picture of each student's current wellness level.
- Identify student behavioral trends to intervene before a crisis occurs.
- Respond effectively to student safety concerns.

Securly *Classroom* enables teachers to monitor all of the devices in their class at once by displaying a thumbnail of each screen on a teacher's device and enabling teachers to zoom in on any particular student.

classroom

Responses to KCSIE Monitoring Requirements

KCSIE GUIDANCE	SECURLY RESPONSE
Physical Monitoring Physical monitoring can contribute where circumstances and the risk assessment suggests low risk, with staff directly supervising children on a one-to-one ratio whilst using technology.	**Classroom** Physical monitoring of devices on a 1:1 basis is time consuming and can be counterproductive to teaching and learning. Securly offers Classroom, a system that enables teachers to monitor all the devices in their class at once by displaying a thumbnail of each screen on a teacher's device and enabling teachers to zoom in on any particular student.
Internet and web access Some Internet Service Providers or filtering providers provide logfile information that details and attributes websites access and search term usage against individuals. Through regular monitoring, this information could enable schools to identify and intervene with issues concerning access or searches.	**Filter. Delegated Admin.** Securly Filter offers delegated administration enabling teachers and student safety staff to access filter logs and reports on students in their care. The interface is simple and non-technical. Reports can be customised, accessed at any time, or scheduled.
Monitoring Content Recognising that no monitoring can guarantee to be 100% effective, schools should be satisfied that their monitoring strategy or system (including keywords if using technical monitoring services) at least covers the following content.	**Aware** Aware helps schools monitor search, web browsing, and web based social media. And email, documents, drives, messaging, in Google and Microsoft environments. A sophisticated AI engine uses keywords and sentiment analysis to identify and categorise harmful activity. All categories identified in the technical guidance are covered.
Active monitoring where a system generates alerts for the school to act upon.	Aware generates real time alerts which are sent to the appropriate staff. Alerts may be tuned to minimise staff workload.
Pro-active monitoring where alerts are managed or supported by a specialist third-party provider and may offer support with intervention. Proactive monitoring is most effective where?	**On-Call** On-Call is a proactive monitoring service which utilises Securly's trained student safety team to analyse alerts and respond by logging cases and managing appropriate escalations.

7. Filtering and Monitoring at Werneth School - September 2023

Smoothwall

Smoothwall is used as the Internet filtering and firewall solution at Werneth School.

Filtering is divided into 2 main categories, Staff and Students, allowing websites to be unblocked/blocked in either category.

Smoothwall provides and updates a daily list of blocked websites that they deem unsafe, this is automatically applied to Werneth 's system to ensure it is always up to date.

Internet filtering logs are checked daily by the Network Manager with detailed testing to the filtering policies completed every half term or when changes are made, The safeguarding team are made aware that these tests are being made and which usernames are making them, as the tests will trigger CPOMS alerts.

Visigo (Owned by Smoothwall)

Visigo is the active monitoring system, Visigo actively monitors everything Staff or Students type on their PCs and reports back any concerns directly into CPOMS, the safeguarding team then action each CPOMS alert and update CPOMS with any action taken.

If Visigo determines an alert is of the highest category, they will also ring the Network Manager and Safeguarding team along with automatically logging it with CPOMS.

Net Support DNA

Net Support DNA is still being rolled out across the school, it is used as the passive monitoring system, it monitors and records everything typed and accessed by Staff and Students.

Currently this system is only accessed by the Network Manager but will shortly be rolled out to the Safeguarding team, in the meantime the Safeguarding team can request data and reports from the Network Manager.

This system is our backup to Visigo (should we ever have an issue with Visigo).

Net Support School

Net Support School is installed in all ICT suites, this software allows the teacher of each room to see a live view of each students PC screen and activity and they have the ability to temporary block access to the internet or certain websites, or even disable the student account should they have the need to.

Appendix 1: online safety training needs – self-audit for staff

ONLINE SAFETY TRAINING NEEDS AUDIT	
Name of staff member/volunteer:	**Date**:
Question	**Yes/No (add comments if necessary)**
Do you know the name of the person who has lead responsibility for online safety in school?	
Are you aware of the ways pupils can abuse their peers online?	
Do you know what you must do if a pupil approaches you with a concern or issue?	
Are you familiar with the school's acceptable use agreement for staff, volunteers, governors and visitors?	
Are you familiar with the school's acceptable use agreement for pupils and parents/carers?	
Are you familiar with the filtering and monitoring systems on the school's devices and networks?	
Do you understand your role and responsibilities in relation to filtering and monitoring?	
Do you regularly change your password for accessing the school's ICT systems?	
Are you familiar with the school's approach to tackling cyber-bullying?	
Are there any areas of online safety in which you would like training/further training?	