Girls' Learning Trust

ONLINE SAFETY POLICY

Approved By: Trust Board
Approval Date: October 2025

Contents

1. Policy statement 3
2. Roles and responsibilities 3
   Trust Board 3
   Local Governing Bodies 3
   CEO 3
   Chief Infrastructure Officer (CIO) 4
   Headteachers 4
   Designated Safeguarding Leads (DSLs) 4
   Head of IT 4
   IT Staff 4
   Individual Staff 5
   Students 5
3. Legislation and guidance 5
4. Key categories of risk 6
5. Online safety in the curriculum 6
6. Use of technology in the classroom 7
7. Use of personal mobile and digital devices 7
8. Use of email 8
9. Filtering and Monitoring 8
10. Network security 9
11. Generative artificial intelligence (AI) and emerging technologies 9
12. Handling online safety concerns 10
13. Reviewing online safety 11
14. Further information and support 11
15. Appendix A – Filtering & Monitoring system and Procedure 12

1. POLICY STATEMENT

The Girls' Learning Trust (the Trust) takes seriously its duty to safeguard and promote the physical, mental and emotional welfare of every child and young person, both inside and outside of the school premises, including online, and we expect everyone who works in our schools to share this commitment.

This policy sets out the Trust's approach to ensuring that all students and staff are safe, responsible, and digitally literate in their use of technology, in line with safeguarding legislation and statutory guidance. This policy should be read in conjunction with Keeping Children Safe in Education (2025) (KCSIE).

The aims of this policy are to:

- Ensure a whole school approach to online safety, empowering schools to protect, educate and safeguard the entire community against online risks, misuse of digital platforms, and harmful content.
- Implement robust and proactive systems to ensure the online safety of students, staff, and governors.
- Deliver proactive and responsive education and intervention relating to online safety.
- Promote digital resilience by ensuring students are equipped to identify and manage online risks themselves.
- Encourage a culture of open dialogue and safe reporting of online concerns.
- Maintain clear procedures to identify, intervene, escalate, and manage online incidents swiftly and appropriately.

2. ROLES AND RESPONSIBILITIES

Trust Board

The Trust Board has strategic leadership accountability for each school's safeguarding arrangements and must ensure that they comply with their duties under legislation. It will ensure that policies, procedures and training across the Trust is effective and complies with the law.

Local Governing Bodies

The Local Governing Bodies (LGBs) are responsible for determining any local procedures for safeguarding and for ensuring a safe environment for students to learn. This includes ensuring that children are taught about how to keep themselves and others safe, including online, and ensuring that the school has appropriate filtering and monitoring systems in place to help limit students' exposure to risk from the school's IT system.

The LGB should ensure that:

- The DSL takes responsibility for understanding the filtering and monitoring systems and processes in place within the school as part of their role.
- All staff understand their expectations, roles and responsibilities around filtering and monitoring as part of safeguarding training.

CEO

The CEO is responsible for the strategic leadership and oversight of safeguarding across the Trust. This includes ensuring that schools are well-supported and held to account for compliance in this area. The

CEO leads on cross-Trust priorities, commissions external reviews where needed, and ensures a safeguarding culture is embedded within each school.

Chief Infrastructure Officer (CIO)

The CIO is the "Digital Lead" as per the DfE standards and is responsible for operational delivery of IT systems and services. This includes supporting compliance as it relates to this policy, working closely with the Head of IT and each school as appropriate. The CIO will annually review the DfE's filtering and monitoring standards, discussing with IT staff what needs to be done to support the schools in meeting the standards.

Headteachers

Headteachers, working closely with the DSLs, have overall responsibility for ensuring that online safety is a running and interrelated theme throughout the school's policies and procedures, including those related to the curriculum, teacher training and safeguarding. Headteachers will:

- Ensure a whole-school approach to online safety.
- Support the DSL and DDSL by ensuring they have enough time and resources to fulfill their responsibilities in relation to online safety.
- Ensure staff receive regular, up to date and appropriate online safety training and information as part of their induction and safeguarding training.
- Ensure online safety practices are annually audited and evaluated.
- Maintain oversight of online incidents and report patterns to governors.
- Seek assurance from the CIO that internet filtering meets safeguarding standards.
- Lead on response strategies to serious online safety incidents.

Designated Safeguarding Leads (DSLs)

The DSL has a responsibility for day-to-day safeguarding and child protection in their school, including online safety, and understanding the filtering, and monitoring systems and processes in place. They will be responsible for:

- Taking the lead responsibility for online safety in their school.
- Reviewing the filtering and monitoring reports and taking appropriate action.
- Ensuring concerns are logged on CPOMS and followed up appropriately.
- Liaising with Local Authority safeguarding partners, Police, and Prevent leads.
- Ensuring that online safety training for all staff is delivered, which includes an understanding of the expectations, applicable roles and responsibilities in relation to filtering and monitoring, and for delivering annual updates to staff.

Head of IT

The Head of IT provides technical leadership across the Trust, ensuring IT systems are secure, reliable, and aligned with Trust policy and national standards. Working closely with the Chief Infrastructure Officer and school-based IT staff, the Head of IT is responsible for supporting the requirements of this policy and ensuring compliance with IT support requirements.

IT Staff

IT staff will be responsible for:

- Providing technical support in the development and implementation of this policy and related school procedures.
- Implementing appropriate security measures as directed by the Headteacher and / or DSL.
- Ensuring that the school's filtering and monitoring systems are updated as appropriate.
- Working with the DSL and Headteacher to conduct light touch reviews of the online safety protocols.

Individual Staff

All staff will be responsible for:

- Taking responsibility for the security of ICT systems and electronic data, they use or have access to and using platforms appropriately.
- Adhering to the Acceptable Use requirements outlined in the Information Technology (IT) Policy.
- Modelling safe and appropriate use of technology in and out of school.
- Ensuring they are familiar with, and understand, the indicators that students may be unsafe online.
- Following procedures for reporting concerns and incidents.
- Maintaining a professional level of conduct in their personal use of technology and avoiding personal communication with students via private channels.
- Understanding the expectations, applicable roles and responsibilities in relation to filtering and monitoring.
- Attending and undertaking all training, which will include raising awareness of emerging technologies and associated risks.
- Where relevant to their role, ensuring online safety is embedded in their teaching of the curriculum.
- Reporting any digital boundary breaches or safeguarding risks.

Students

Students will be responsible for:

- Adhering to rules outlined in Acceptable Use Agreements and other relevant policies.
- Engaging with curriculum content around online safety and digital citizenship.
- Understanding the impact of their digital behaviour on others and themselves.
- Seeking help from staff if they are concerned about something they or a peer have experienced online.
- Reporting online safety incidents and concerns in line with procedures within this policy.

3. LEGISLATION AND GUIDANCE

This policy has been developed in accordance with the principles established by the Department for Education's (DfE's) statutory guidance, Keeping Children Safe in Education (2025) (KCSIE) and Working Together to Safeguard Children (2023).

This policy also has due regard to all relevant legislation and statutory guidance including but not limited to:

- Online Safety Act 2023
- Cyber Security Standards for Schools and Colleges (2025)
- Filtering and Monitoring Standards for Schools and Colleges (2025)
- Relationships Education, Relationships and Sex Education (RSE) and Health Education (2025)

This policy should be read alongside other relevant school and Trust policies, including but not limited to:

- Safeguarding and Child Protection Policy
- IT Policy
- Photographs and Media Policy
- Data Protection and Freedom of Information Policy
- Staff Code of Conduct

4. KEY CATEGORIES OF RISK

The Trust recognises that the breadth of issues classified within online safety is considerable and ever evolving, but can be categorised into four areas of risk, as outlined in KCSIE:

- Content: being exposed to illegal, inappropriate, or harmful content, for example: pornography, fake news, racism, misogyny, self-harm, suicide, anti-Semitism, radicalisation, extremism, misinformation, disinformation (including fake news) and conspiracy theories.

- Contact: being subjected to harmful online interaction with other users; for example, peer-to-peer pressure, commercial advertising and adults posing as children or young adults with the intention to groom or exploit them for sexual, criminal, financial or other purposes.

- Conduct: online behaviour that increases the likelihood of, or causes, harm; for example, making, sending and receiving explicit images (e.g. consensual and non-consensual sharing of nudes and semi-nudes and / or pornography, sharing other explicit images and online bullying; and

- Commerce: risks such as online gambling, inappropriate advertising, phishing and or financial scams. If staff are concerned that any students or staff are at risk, please report this to spam@girlslearningtrust.org. All reports will be reviewed and reported to the Anti-Phishing Working Group as required (https://apwg.org/).

5. ONLINE SAFETY IN THE CURRICULUM

As part of a broad and balanced curriculum, all students will be made aware of risks and taught how to stay safe online. Each school's approach to teaching online safety in the curriculum will reflect the Relationships Education, Relationships and Sex Education (RSE) and Health Education statutory guidance. It will also reflect the ever-evolving nature of online risks, ensuring students develop the knowledge and resilience to navigate digital spaces safely and responsibly.

With support from the DSL in the development of the school's online safety curriculum, teaching is always appropriate to the students' ages and developmental stages and integrated across computer science, PSHE, RSE and tutorial programmes. Students are taught the underpinning knowledge and behaviours that can help them navigate the online world safely and confidently regardless of the device, platform or app they are using.

Each school shall determine their curriculum sequence, ensuring that programmes are proactively and responsively planned to meet the needs of their students. Online safety education will address the four key categories of risk: content, contact, conduct and commerce.

Schools will work in partnership with parents to ensure students stay safe online at school and at home. Parents will be provided with information about the school's approach to online safety and their role in protecting their children.

6. USE OF TECHNOLOGY IN THE CLASSROOM

A wide range of technology will be used during lessons, including the following:

- Computers
- Laptops
- Tablets
- Smartphones
- Intranet
- Email
- Cameras

Prior to using any websites, tools, apps or other online platforms in the classroom, or recommending that pupils use these platforms at home, the class teacher will review and evaluate the resource. Class teachers will ensure that any internet-derived materials are used in line with copyright law.

Students will be supervised when using online materials during lesson time – this supervision is suitable to their age and ability. Outside of timetabled lessons student access to devices are subject to filtering and monitoring platforms and any attempted misuse will be followed up.

7. USE OF PERSONAL MOBILE AND DIGITAL DEVICES

The Trust accepts that staff will bring their own devices into the workplace and may use them during the day. However, staff should not have such devices out or in use in front of students or in classrooms.

Staff are not permitted to use their personal mobile phone or other digital device to take pictures or videos of students at any time. If there is a requirement for a staff member's role to take photographs or videos of students for school purposes, this must be carefully planned before any activity and carried out using school equipment.

Where photographs and videos will involve pupils who are children looked after (CLA), adopted pupils, or pupils for whom there are security concerns, the Headteacher will liaise with the DSL to determine the steps involved. The DSL will, in known cases of pupils who are CLA or who have been adopted, liaise with the pupils' social workers, carers or adoptive parents to assess the needs and risks associated with the pupils.

Staff should refer to the Staff Code of Conduct, the Photographs and Media Policy and the Data Protection and Freedom of Information Policy for more detail.

Staff will report any concerns about pupils' or other staff members' use of personal electronic devices to the DSL, following the appropriate procedures.

8. USE OF EMAIL

Access to and the use of emails will be managed in line with the Data Protection & Freedom of Information Policy and the Acceptable Use Agreement. Staff should also refer to the Staff Code of Conduct.

Staff and students will be given approved school email accounts and will only be able to use these accounts at school and when doing school-related work outside of school hours. By using the school's network and IT equipment, staff and students agree to the Acceptable Use Agreement, which can be found in the Staff and Student Handbooks, the Information and Technology (IT) Policy, and in the IT section of the GLT Knowledge Base. Communication between staff and students will only be permitted between Trust sanctioned platforms. Any email that contains sensitive or personal information should only be sent using secure and encrypted email.

Staff members and students will be required to block spam and junk mail and report the matter to IT colleagues. Guidance on this can be found in the Trust's Knowledge Base. The school's monitoring system can detect inappropriate links, malware and profanity within emails – staff and students will be made aware of this. Chain letters, spam and all other emails from unknown sources will be deleted without being opened.

9. FILTERING AND MONITORING

The Trust will ensure that the school's ICT network has appropriate filtering and monitoring systems in place and that it meets the DfE's 'Filtering and monitoring standards for schools and colleges'.

The LGB will ensure 'over blocking' does not lead to unreasonable restrictions as to what students can be taught with regards to online teaching and safeguarding.

The DSL in each school is responsible for overseeing the filtering and monitoring systems in their school and the IT team is responsible for the management and administration of the platforms to ensure they meet the school's safeguarding needs.

The DSL and Head of IT will undertake an annual audit and risk assessment to determine what filtering and monitoring systems are required. These systems will be scaled appropriately to meet the safeguarding needs of all students, in line with KCSIE guidance. The DSL and Head of IT will undertake regular checks on the filtering and monitoring systems to ensure they are effective and appropriate. Staff and students are expected to report any inappropriate content that may have been accessed to the DSLs and / or Head of IT.

Requests regarding making changes to the filtering system will be directed to the DSL via an MS Form, who will undertake a risk assessment. Before the DSL agrees to the request, they will first check with the DSLs from the Trust's other schools and, where they are unanimous in their agreement, the request will be sent to IT to unblock the site across all schools. Any changes made to the system will be recorded by IT colleagues to ensure a robust audit trail is in place.

The schools' network and school-owned devices will be appropriately monitored. All users of the network and school-owned devices will be informed about how and why they are monitored. Concerns identified through monitoring will be reported to the DSL who will manage the situation in line with the

Safeguarding and Child Protection Policy. If a student has deliberately breached the filtering system, this will be dealt with by the school's Behaviour Policy. If a member of staff has deliberately breached the filtering system, this will be dealt with by the staff Disciplinary Policy.

If material that is believed to be illegal is accessed, inadvertently or deliberately, this material will be reported to the appropriate agency immediately, e.g. the Internet Watch Foundation (IWF), CEOP and / or the police.

Personal devices connected to the school's network will be subject to the same filtering standards to ensure consistent safeguarding measures. This applies to any device that is connected to the school's network.

Please see Appendix A for further information on the filtering and monitoring system and procedure in use within the Trust.

10. NETWORK SECURITY

Technical security features, such as anti-virus software and firewalls, will be kept up-to-date and managed by IT. Firewalls will be switched on at all times. IT colleagues will review the security features on a regular basis to ensure they are running correctly, and to carry out any required updates.

Staff and students will be directed not to download unapproved software or open unfamiliar email attachments and will be expected to report all malware and virus attacks to IT.

All members of staff will have their own unique usernames and private passwords to access the school's systems. Students will be provided with their own unique username and private passwords. Staff and students will be responsible for keeping their passwords private.

Users will inform IT if they forget their login details, who will take appropriate action to ensure access is securely restored. Users will not be permitted to share their login details with others and will not be allowed to log in as another user at any time. If a user is found to be sharing their login details or otherwise mistreating the password system, a member of the senior leadership team will be informed and will decide the necessary action to take.

Users will be required to lock access to devices and systems when they are not in use.

11. GENERATIVE ARTIFICIAL INTELLIGENCE (AI) AND EMERGING TECHNOLOGIES

The Trust recognises the growing influence of emerging technologies, including artificial intelligence (AI), on education and student wellbeing and safety. The Trust will monitor developments in AI and update training and curriculum content accordingly.

When deciding whether to use generative AI, safety will be the top priority. Any use of AI tools by staff and pupils will be carefully considered and assessed, evaluating the benefits and risks of its use in the school.

AI tools will only be used in situations where there are specified clear benefits that outweigh the risks, e.g. where it can reduce teacher workload, and the school will ensure that any use of AI tools comply with wider statutory obligations, including those outlined in KCSIE.

Each school will carry out an AI Risk Assessment, which includes plans for mitigating against unauthorised use cases.

Pupils will only be permitted to use generative AI in the school with appropriate safeguards in place, e.g. close supervision and the use of tools with appropriate filtering and monitoring features in place.

For any use of AI, the school will:

- Comply with age restrictions set by AI tools and open access large language models (LLMs).
- Consider online safety, including AI, when creating and implementing the school's approach to safeguarding and related policies and procedures.
- Consult KCSIE to ensure all statutory safeguarding obligations and AI tools are used safely and appropriately.
- Refer to the DfE's generative AI product safety expectations and filtering and monitoring standards.

Each school will take steps to prepare students for changing and emerging technologies, e.g. generative AI and how to use them safely and appropriately with consideration given to pupils' age.

Each school will ensure:

- Its IT systems include appropriate filtering and monitoring systems to limit pupils' ability to access or create harmful or inappropriate content through generative AI.
- That students are not accessing or creating harmful or inappropriate content, including through generative AI.
- It take steps to ensure that personal and sensitive data is not entered into generative AI tools and that it is not identifiable.
- Staff and students are aware of the risks associated with AI tools, such as misinformation, bias, and inappropriate content generation.

12. HANDLING ONLINE SAFETY CONCERNS

Any disclosures made by students to staff members about online abuse, harassment or exploitation, whether they are the victim or disclosing on behalf of another child, will be handled in line with the Safeguarding and Child Protection Policy.

Staff will be aware that harmful online sexual behaviour can progress on a continuum, and appropriate and early intervention can prevent abusive behaviour in the future. Staff will also acknowledge that students displaying this type of behaviour are often victims of abuse themselves and should be suitably supported.

The victim of online harmful sexual behaviour may ask for no one to be told about the abuse. The DSL will consider whether sharing details of the abuse would put the victim in a more harmful position, or whether it is necessary in order to protect them from further harm. Ultimately the DSL will balance the victim's wishes against their duty to protect the victim and other young people. The Headteacher and DSL will meet with the victim's parents to discuss the safeguarding measures that are being put in place to support their child and how the report will progress.

Confidentiality will not be promised, and information may be still shared lawfully, for example, if the Headteacher decides that there is a legal basis under UK GDPR such as the public task basis whereby it is

in the public interest to share the information. If the decision is made to report abuse to children's social care or the police against the victim's wishes, this must be handled extremely carefully – the reasons for sharing the information should be explained to the victim and appropriate specialised support should be offered.

Concerns regarding a staff member's online behaviour should be recorded on Staff Safe and reported to the Headteacher or appropriate senior leader (for shared professional services), who decides on the best course of action in line with the relevant policies. If the concern is about the Headteacher, it is reported to the CEO. If the concern is about the CEO it should be reported to the Chair of Trust Board.

Concerns regarding a student's online behaviour should be recorded on CPOMs. The DSL will investigate concerns with relevant staff members.

Where there is a concern that illegal activity has taken place, the Headteacher will inform the CEO and contact the police. The school will avoid unnecessarily criminalising students, e.g. calling the police, where criminal behaviour is thought to be inadvertent and as a result of ignorance or normal developmental curiosity, e.g. a student has taken and distributed indecent imagery of themselves. The DSL will decide in which cases this response is appropriate and will manage such cases in line with the Safeguarding and Child Protection Policy.

13. REVIEWING ONLINE SAFETY

The DSL in each school and the Head of IT will carry out an annual review of the school's approach to online safety (using the LGfL online safety audit), including filtering and monitoring, supported by an annual risk assessment that considers and reflects the risks the students face.

14. FURTHER INFORMATION AND SUPPORT

There is a wealth of additional information available to support staff, schools and parents to keep children safe online. Staff should refer to Annex B in KCSIE.

15. APPENDIX A – FILTERING & MONITORING SYSTEM AND PROCEDURE

Web Filtering - NetSweeper

This is the name of the current solution deployed across all Trust schools. NetSweeper is used to filter billions of categorised URLs, text and images to ensure education-specific safe searches in over 40 languages. For any sites that are not in their database, they use AI to analyse and categorise in real time. It is compliant with:

- PREVENT
- Home Office terrorism block list
- Internet Watch Foundation (IWF) block list and Image Hash List
- KCSIE
- UK Safer Internet Centre
- Meeting digital and technology standards in schools and colleges

We use NetSweeper to help protect our students and staff from:

- Online bullying
- Child sexual exploitation
- Self-harm content
- Radicalisation
- Drug abuse
- Misinformation
- Disinformation (including fake news)

In general, filtering is split into three groups differentiated according to age, vulnerability and risk of harm. Each group is configured with internet access policies depending on the required access to various internet site categories:

- Staff
- Students (Years 7-11)
- Students (Years 12-13)

Splitting the filtering in this way allows us to better manage and fine-tune access as staff require less restricted access than students. Similarly, Sixth-Form students require access to some internet resources that lower-year groups do not.

In addition, the Trust subscribes to Sophos Endpoint Protection which helps to keep everyone safe online by providing an additional layer of strong web filtering and application control across the schools' networks. It allows the schools to manage which websites can be accessed, ensuring that students and staff only reach safe, appropriate, and educational content. Websites are checked and categorised in real time, and filters are applied based on the school's safeguarding policies, whether users are on-site or working remotely on Trust issued devices. Sophos also helps prevent the use of certain apps or programmes that may be unsafe or disruptive to learning. By using this system, the schools can maintain a secure and focused digital environment that supports education while protecting all users from online risks.

Monitoring - Smoothwall Monitor (Formerly Visigo)

This is an additional layer of monitoring GLT has implemented to help us keep our staff and students safe while using our IT systems. It provides real-time monitoring of all GLT student access PCs and laptops. Digital monitoring in this way has helped us spot students at serious risk online. Students who may otherwise have gone unnoticed. The software offers:

- Proactive real-time monitoring which captures user activity as it happens, automatically sending potential risks through to the Monitor portal, which the DSL teams have access to.
- Online and offline monitoring which captures activity that may indicate a risk, even outside of the regular web browser such as in a Word document, messaging app, or encrypted "dark web" browsers.
- Smoothwall have a 24/7 in-house team of moderators who review captures to minimise false positives and contact us by phone for any urgent risks.
- Alerts are sent in real-time by phone, email, and stored within the intuitive portal for the DSL teams to review.

While NetSweeper and Smoothwall Monitor work together to provide a robust and manageable filtering and monitoring solution, these systems do have their limitations and will not provide filtering or monitoring on personal devices outside of the GLT networks.

Location	Device	Filtering (NetSweeper)	Monitoring (Smoothwall)
In school	School Device	Yes*	Yes
	Personal Device (Using school Wi-Fi not mobile data)	Yes	No
At home	School Device	Yes (via Sophos)	Yes
	Personal Device	No	No
	Personal Device (Remoting in)	Yes	Yes

*Student and staff accounts are set up with different levels of filtering.

Web filtering & monitoring reports

NetSweeper can be configured to provide many different reports which can be run manually as needed or scheduled to provide the DSL teams with regular updates. As of September 2023, a daily report, which will show websites that students have attempted to access but have been blocked by our filtering policies, will be sent directly from NetSweeper to the DSLs. This report will be sent at the end of the school day at 4pm.

An annual review of all manually unblocked sites will be carried out. A report will be scheduled to list all manually unblocked websites which the school has agreed to allow through the filtering which would otherwise be blocked by NetSweeper. This report will then be reviewed by the DSL team to determine if the sites are still appropriate or if they should be added back to the blocked list.

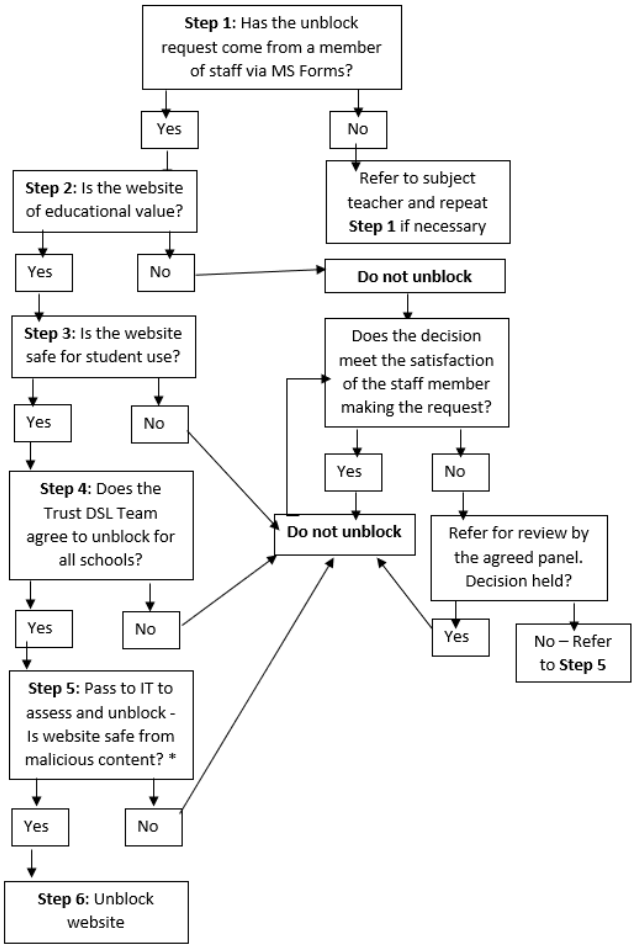
Smoothwall Monitor sends real-time reports to the DSL teams for critical alerts, it also records and logs less critical alerts in the portal for the DLS teams to review. These should be reviewed daily.

Unblocked websites and management.

It is important that we do not unblock websites unnecessarily; only sites that are of educational value and have been assessed by the DLS team for any potential safeguarding issues be allowed to bypass the NetSweeper filtering for students.

The DSL team is responsible for using their professional judgment when agreeing to unblock a website for student use. If a member of staff requires a website to be unblocked, the request should be passed to the DSL to assess the safeguarding risk. After careful consideration, the DSL will instruct the IT team to unblock, if necessary. Staff in school should be aware that a website request will take time to assess and should not expect an immediate resolution.

Should the DSL team decide that a website will not be unblocked, and this decision is disputed by the requesting member of staff, the decision should be reviewed by the Chief People Officer and Head of IT. The panel will access the educational value of the website, the safeguarding reasons for the site to be initially flagged as blocked by NetSweeper and any technical vulnerabilities the site may introduce.



*Malicious Content means viruses, worms, time bombs, Trojan horses and other harmful or malicious code, files, scripts, agents, or programs.

Annual review.

On an annual basis, in the summer term, a report from NetSweeper will be issued to the DSLs which will list all websites that have been manually unblocked using the above process. This list is to be reviewed and a decision made as to whether the unblocked sites are still necessary. If any sites are to be added back to the student filtering policy, using the decision process above, inform IT to remove the website from the unblocked list.

All staff receive appropriate safeguarding and child protection training (including online safety which, amongst other things, includes an understanding of the expectations, applicable roles, and responsibilities in relation to filtering and monitoring at induction. The training is regularly updated. In addition, all staff receive safeguarding and child protection (including online safety) updates (for example, via email, e-bulletins, and staff meetings), as required, and at least annually, to continue to provide them with relevant skills and knowledge to safeguard children effectively.

We fully adhere to the government guidance 'Meeting digital and technology standards in schools and colleges'.