The Forge Trust Filtering and Monitoring Technical requirements checklist

This checklist was completed on 4th September 2024

- Designated safeguarding lead (DSL)- Jo Knapp
- Atom IT
- ESLT- Carl Braithwaite/ Jamie Macintyre
- Sue Trentini- Chair of Trustees
- Linda Sargisson- Trustee

REQUIREMENT FILTERING SYSTEM	✓
Is it a member of the Internet Watch Foundation (IWF)?	✓
Is it signed up to Counter-Terrorism Internet Referral Unit list (CTIRU)?	✓
Does it block access to illegal content including child sexual abuse material (CSAM)?	✓
Are you satisfied that the system manages the following content: › Discrimination › Drugs/substance abuse › Extremism › Gambling › Malware/hacking › Pornography › Piracy and copyright theft › Self harm › Violence	✓

REQUIREMENT FILTERING SYSTEM	✓

Is the filtering system:
› Operational
› Up to date
› Applied to all:
  ○ Users, including guest accounts
  ○ School-owned devices
  ○ Devices using the school broadband connection
	✓

Does the filtering system: › Filter all internet feeds, including any backup connections › Handle multilingual web content, images, common misspellings and abbreviations › Identify technologies and techniques that allow users to get around the filtering, such as VPNs and proxy services, and block them › Provide alerts when any web content has been blocked It is: › Age and ability appropriate for the users, and suitable for educational settings	✓
Does the filtering system allow you to identify: › Device name or ID, IP address, and where possible, the individual › The time and date of attempted access › The search term or content being blocked	✓

REQUIREMENT FILTERING SYSTEM	✓
Are you clear on how long logfile information (internet history) is retained and how it’s stored?	✓
Are you clear on how the system does not over block access so it doesn’t lead to unreasonable restrictions?	✓

REQUIREMENT FILTERING SYSTEM	✓
Does the filtering system meet the following principles? › Context appropriate differentiated filtering, based on age, vulnerability and risk of harm o Can you vary the filtering strength? E.g. for staff? › Circumvention o Can you identify and manage technologies used to circumvent the system, e.g. virtual personal networks (VPNs), proxy services and domain name system (DNS) over Hypertext Transfer Protocol Secure (HTTPS) › Control o Can you control the filter yourselves to permit or deny specific content? o Can you log any changes as part of an audit trail? › Contextual content filters o In addition to URL or IP-based filtering, the extent to which (http and https) content is analysed as it is streamed to the user and blocked, this would include artificial intelligence (AI) generated content. For example, being able to contextually analyse text on a page and dynamically filter › Filtering Policy o Does your provider detail its approach to filtering, as well as over blocking? › Group/multi-site management o Can your system be deployed centrally, with a central policy and dashboard? › Identification o Does the system allow you to identify users? › Multiple language support o Does the system manage relevant languages? › Network level o Is the filtering provided at ‘network level’, i.e. it doesn’t reply on software on user devices while at school	✓

REQUIREMENT FILTERING SYSTEM	✓

› Remote devices
  o Can the system filter devices where staff and/or pupils are working remotely?
› Reporting
  o Can you report inappropriate content?
  o Does the system provide clear historical information on the websites users have accessed or tried to access?
› Safe Search
  o Does the system have the ability to enforce ‘safe search’?
	✓

If users access content via mobile or through apps: Get confirmation that your provider can provide filtering on mobile or app technologies. They should also apply a technical monitoring system to devices using mobile and app content to reduce the risk of harm.	✓
If your filtering provision is procured with a broadband service: Make sure it meets the needs of your school or college	✓

REQUIREMENT MONITORING SYSTEM	✓
Are incidents urgently picked up, acted on and the outcomes recorded?	✓
Are all staff clear on: › How to deal with these incidents › Who should lead on any actions	✓
Is device monitoring managed? (this could be by your IT staff or a third-party provider) Whoever is manging device monitoring will need to: › Make sure monitoring systems are working as expected › Provide reports on pupil device activity › Receive safeguarding training including online safety › Record and report safeguarding concerns to the DSL	✓
Is your monitoring data received in a format that your staff can understand?	✓
Are users identifiable to your school or college, so you can trace concerns to an individual, including guest accounts?	✓

REQUIREMENT MONITORING SYSTEM	✓
Does your monitoring system alert you to behaviours associated with: › Content o Being exposed to illegal, inappropriate, or harmful content, for example: pornography, fake news, racism, misogyny, self-harm, suicide, anti-Semitism, radicalisation and extremism › Contact o 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 o 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 › Commerce o Risks such as online gambling, inappropriate advertising, phishing and/or financial scams	✓

REQUIREMENT MONITORING SYSTEM	✓
Does the monitoring system meet the following principles: › Age appropriate o Can you vary your strategy to take age, vulnerability, or specific situations (e.g. boarding schools) into account › Audit trail o Are any changes to the strategy logged so no one can make changes on their own? › Bring your own device (BYOD) o If your system can monitor staff and pupils' personal devices, make sure this is done according to your data management policies. For example, will your system monitor devices out of school hours? › Data retention o Be clear on what data is stored, where and for how long (including any backup data) › Devices o Make sure your system is clear about which devices it covers › Flexibility o Make it clear how keywords can be added or removed › Group/multi-site management o Can your strategy be deployed centrally, with a central policy and dashboard? › Harmful image detection o To what extent is visual content monitored and analysed? › Impact o How do monitoring results impact your policy and practice?	✓

REQUIREMENT MONITORING SYSTEM	✓
› Monitoring policy o How do you tell all users that you're monitoring their online access? o How do you communicate your expectations on appropriate use to pupils and staff? › Multiple language support o Can the system manage relevant languages to your school? › Prioritisation o How are alerts prioritised? o What procedures do you have in place to allow staff to respond to alerts rapidly? › Remote monitoring o Can the system monitor devices where staff and/or pupils are working remotely? o Are users aware of this? Are you clear if these devices are only monitored during school hours? › Reporting o How are alerts recorded, communicated and escalated?	✓
Do your staff: › Provide effective supervision › Take steps to maintain awareness of how devices are being used by pupils › Report any safeguarding concerns to the DSL	✓
If users access content via mobile or through apps: Have you applied a technical monitoring system to these devices?	✓

Your school:

- Will need to carry out your own data protection impact assessment (DPIA) and review the privacy notice of third-party providers. Use this template from the ICO
- Will need to reflect your monitoring procedures in your acceptable use policy
- May decide to enforce Safe Search or another child-friendly search engine/tool