Online Safety & Social Media Policy

Sponsorship & Review

1 Sponsor

Assistant Vice Principal for Safeguarding & IT Communications

2 Reviewed

September 2025

3 Next review due

December 2028

Overview

1. Aims

Protect pupils and staff from online harms across content, contact, conduct and commerce. Align with Keeping Children Safe in Education (KCSIE) 2025 and the DfE Filtering & Monitoring Standards, and consolidate our E-Safety and Social Media policies into one current policy.

2. Scope

Applies to all pupils, staff, governors, volunteers, visitors and contractors. Covers school-managed and personal devices on site, off site and in remote learning; school platforms (email, MIS, Teams/SharePoint/VLE), the school website and official social media accounts; and personal social media where any association with the school exists.

3. Legislation & Guidance

- Keeping Children Safe in Education (KCSIE) 2025 (Parts 1 & 2—including online safety, DSL duties and filtering & monitoring expectations).

- DfE Filtering & Monitoring Standards (updated Nov 17, 2025): roles & responsibilities; annual reviews; balanced filtering; effective monitoring strategies.

- UK Safer Internet Centre—Appropriate Filtering & Monitoring: definitions; avoiding over-blocking; contextual analysis including AI-generated content.

- Prevent Duty / CTIRU unlawful terrorist content lists; IWF child sexual abuse URLs (must be actively blocked by filtering systems).

4. Roles & Responsibilities

Governing Body / Proprietor

Provide strategic oversight and assurance that appropriate filtering and monitoring are in place, effective, and reviewed at least annually. Assign a governor and SLT lead for filtering/monitoring oversight; approve policy and resourcing.

Senior Leadership Team (SLT)

Procure and oversee filtering & monitoring; document decisions on what is blocked/allowed; ensure staff training; authorise official social media accounts; oversee incident escalation.

Designated Safeguarding Lead (DSL) & Deputy DSLs

DSL: Angela Bithell—leads online safety and safeguarding; liaises with IT on filtering/monitoring; triages alerts; ensures staff/student education; reports to governors; coordinates referrals (CEOP/Police/LA).

Deputy DSLs: Mrs Ceri Kinsey, manage cases and act when DSL is unavailable.

Principal & Chair of Governors

Principal: Mrs Sarah Barton—manages staff allegations. Chair of Governors: Mark Brown—manages any allegation against the Principal.

IT Services / Network Manager

Implement and maintain filtering/monitoring; test effectiveness; manage user identification; support investigations; maintain logs in line with data protection; patch systems; enable classroom monitoring and remote protections.

Staff & Students

Staff: model professional online behaviour; follow Acceptable Use Agreements (AUAs); use official channels for pupil/parent communication; report concerns immediately to DSL; complete annual training; comply with social media rules. Students: follow AUAs; respect others; protect personal information; report concerns; comply with mobile device expectations.

5. Education & Curriculum

Online safety is taught through Computing, PSHE/RSHE and across the curriculum, including misinformation/disinformation, extremism, fraud, privacy, AI literacy, respectful behaviour, digital footprint and image-sharing risks. Parents/carers are engaged via workshops, web resources and clear reporting routes (DSL, CEOP, UKSIC, Childline).

6. Acceptable Use Agreements (AUA)

AUAs are issued on induction and annually for students (by phase) and staff/governors/volunteers. Breaches are managed under the Behaviour or Staff Disciplinary Policy.

7. Mobile Devices & Personal Equipment

Students follow phase-specific rules; no recording in changing rooms/toilets; camera use only with permission. Staff secure devices (PIN/MFA), avoid local storage of sensitive data, and use school accounts/apps.

8. Technical Infrastructure, Filtering & Monitoring

Charlton uses LA-provided Lightspeed for web filtering and Senso for safeguarding/monitoring, aligned to UKSIC definitions. Illegal content (IWF, CTIRU) is blocked; categories include

pornography, extremism, hate speech, self-harm, violence, malware, piracy and discrimination. Filtering applies on-site and, where possible, to managed remote devices. Monitoring is proportionate (classroom/device/Teams chat), with alerts triaged by DSL/SLT and evidence retained per data protection. Annual self-assessment using the DfE tool; termly effectiveness tests; documented decisions/change logs; an incident response playbook is maintained.

Over-blocking is avoided to enable teaching and learning, in line with UKSIC guidance and Ofsted findings on "managed" versus "locked-down" systems.

9. Data Protection & Privacy

Personal data is processed lawfully, fairly and securely; role-based access; encryption; retention schedules; secure deletion. Monitoring data is minimised and retained only as necessary; access is controlled; subject rights are respected.

10. Social Media (Integrated Policy)

Professional communications occur via official channels only. Official school social media accounts require SLT approval, at least two moderators, secure credential storage and MFA, and daily monitoring. Tone is engaging, informative and professional; images follow parental consent; student images must never be posted via personal accounts; responses within one working day.

Staff (personal use): do not friend/follow current or prior students; do not discuss school business; use a disclaimer if referencing the school; maintain privacy settings; avoid excessive use during work time. Parents/carers: use official channels for complaints/concerns; do not post images of other children; avoid defamatory comments; school may request takedown and follow the Complaints Policy.

11. Responding to Misuse, Cyberbullying & Harm

All concerns are recorded and investigated promptly; evidence may include logs/screenshots/device checks. The school may contact platforms for takedown; Police/CEOP are involved where illegal content is suspected; support is provided to victims; sanctions are proportionate to severity.

12. Emerging Technologies, AI & Remote Learning

New tools undergo risk assessment and, where necessary, a DPIA. Generative AI use is guided by curriculum aims, age appropriateness, bias/accuracy and safeguarding (no harmful content; no uploading personal data). Remote learning platforms follow safeguarding and data protection expectations; live sessions use approved platforms and protocols.

13. Training

All staff receive induction and annual refresher training; DSL/DDSLs receive advanced training; governors receive oversight training for filtering/monitoring and policy assurance.

14. Monitoring & Review

Policy review annually (or sooner after updates/incidents). Filtering/monitoring: annual self-assessment (DfE "Plan technology for your school"), termly tests, governor oversight; KPIs include incident response times, training completion and test outcomes.

15. Reporting Routes & External Support

Internal: DSL (Angela Bithell); DDSLs (Mrs Ceri Kinsey;Miss Katie Littleford);

school@charlton.uk.com 01952 951409

External: NSPCC (0808 800 5000), CEOP Safety Centre, Action Fraud (0300 123 2040), West Mercia Police (999/101), NCSC (suspicious website reporting), Childline "Report Remove".

16. Links with Other Policies

Child Protection & Safeguarding; Behaviour; Child-on-Child/Anti-bullying; RSHE; Data Protection; Mobile Devices; Staff Code of Conduct; Remote Learning; Digital/Video Images; Complaints.

Appendix A: Acceptable Use Agreement – Students (KS3/KS4)

By using school devices, networks and accounts, I will:

- Respect others online; no bullying, harassment or discriminatory language.

- Protect my personal information and that of others; never share passwords.

- Use school platforms (Teams/VLE/email) responsibly and for learning purposes.

- Report anything that makes me feel unsafe or is inappropriate to a trusted adult/DSL.

- Not attempt to bypass filters or access blocked/inappropriate content.

- Not record or share images in changing rooms/toilets; only use cameras with permission.

I understand breaches may lead to sanctions under the Behaviour Policy and that illegal activity may be referred to the Police/CEOP.

Appendix B: Acceptable Use Agreement – Staff/Governors/Volunteers

I will:

- Use official channels and school accounts for all pupil/parent communications.

- Maintain professional boundaries online and on social media; never friend/follow pupils.

- Protect confidential information and personal data; follow GDPR and data protection policy.

- Use devices securely (PIN/MFA); report losses/incidents immediately.

- Uphold safeguarding responsibilities; report any concerns to DSL/DDSLs without delay.

I understand breaches may lead to disciplinary action and, where appropriate, referral to external agencies.

Appendix C: Filtering & Monitoring Annual Self-Assessment Checklist (DfE Standards)

Standard 1 – Roles & Responsibilities:

• Owners: SLT lead (DSL), IT Services Lead, Named Governor. Evidence: policy statement; assignment letter; minutes of governor oversight; training records. Review: annual (Sept).

Standard 2 – Annual Review:

• Owners: DSL/IT Services. Evidence: DfE self-assessment ("Plan technology for your school"), termly test results, incident log, change log. Review: annual (Sept).

Standard 3 – Balanced Filtering:

• Owners: IT Services (with DSL). Evidence: category lists (Lightspeed), whitelists/blacklists, curriculum access exceptions, UKSIC alignment note. Review: termly checks + annual audit.

Standard 4 – Effective Monitoring:

• Owners: DSL/SLT. Evidence: Senso alert workflow, triage records, escalation to CPOMS/CEOP/Police, classroom monitoring SOP. Review: termly + annual.

Social Media Policy

Social media (e.g. Facebook, X, LinkedIn, Instagram) is a broad term for any kind of online platform which enables people to directly interact with each other. However, some games, for example Minecraft or World of Warcraft and video sharing platforms such as You Tube have social media elements to them.

Charlton School recognises the numerous benefits and opportunities which a social media presence offers. Staff, parents/carers and students are actively encouraged to find creative ways to use social media. However, there are some risks associated with social media use, especially around the issues of safeguarding, bullying and personal reputation. This policy aims to encourage the safe use of social media by Charlton School, its staff, parents, carers and children.

Scope

This policy is subject to the school's Codes of Conduct and Acceptable Use Agreements.
This policy:

- Applies to all staff and to all online communications which directly or indirectly, represent the school.
- Applies to such online communications posted at any time and from anywhere.
- Encourages the safe and responsible use of social media through training and education
- Defines the monitoring of public social media activity pertaining to the school

The school respects privacy and understands that staff and students may use social media forums in their private lives. However, personal communications likely to have a negative impact on professional standards and/or the school's reputation are within the scope of this policy.

Professional communications are those made through official channels, posted on a school account or using the school name. All professional communications are within the scope of this policy.

Personal communications are those made via a personal social media accounts. In all cases, where a personal account is used which associates itself with the school or impacts on the school, it must be made clear that the member of staff is not communicating on behalf of the school with an appropriate disclaimer. Such personal communications are within the scope of this policy.
Personal communications which do not refer to or impact upon the school are outside the scope of this policy.

Digital communications with students are also considered. *Staff may use social media to communicate with learners via a school social media account for teaching and learning purposes but must consider whether this is appropriate and consider the potential implications.*

Organisational control

Roles & Responsibilities

- **SLT**
  - Facilitating training and guidance on Social Media use.
  - Developing and implementing the Social Media policy
  - Taking a lead role in investigating any reported incidents.
  - Making an initial assessment when an incident is reported and involving appropriate staff and external agencies as required.
  - Receive completed applications for Social Media accounts
  - Approve account creation

- **Administrator / Moderator**
    - Create the account following SLT approval
    - Store account details, including passwords securely
    - Be involved in monitoring and contributing to the account
    - Control the process for managing an account after the lead staff member has left the organisation (closing or transferring)
- **Staff**
    - Know the contents of and ensure that any use of social media is carried out in line with this and other relevant policies
    - Attending appropriate training
    - Regularly monitoring, updating and managing content he/she has posted via school accounts
    - Adding an appropriate disclaimer to personal accounts when naming the school

Process for creating new accounts

The school community is encouraged to consider if a social media account will help them in their work, e.g. a history department X account, or a "Friends of the school" Facebook page. Anyone wishing to create such an account must present a business case to the School Leadership Team which covers the following points:-

- The aim of the account
- The intended audience
- How the account will be promoted
- Who will run the account (at least two staff members should be named)
- Will the account be open or private/closed

Following consideration by the SLT an application will be approved or rejected. In all cases, the SLT must be satisfied that anyone running a social media account on behalf of the school has read and understood this policy and received appropriate training. This also applies to anyone who is not directly employed by the school, including volunteers or parents.

Monitoring

School accounts must be monitored regularly and frequently (preferably 7 days a week, including during holidays). Any comments, queries or complaints made through those accounts must be responded to within 24 hours (or on the next working day if received at a weekend) even if the response is only to acknowledge receipt. Regular monitoring and intervention is essential in case a situation arises where bullying or any other inappropriate behaviour arises on a school social media account.

Behaviour

- The school requires that all users using social media adhere to the standard of behaviour as set out in this policy and other relevant policies.
- Digital communications by staff must be professional and respectful at all times and in accordance with this policy. Staff will not use social media to infringe on the rights and privacy of others or make ill-considered comments or judgments about staff. School social media accounts must not be used for personal gain. Staff must ensure that confidentiality is maintained on social media even after they leave the employment of the school.
- Users must declare who they are in social media posts or accounts. Anonymous posts are discouraged in relation to school activity.
- If a journalist makes contact about posts made using social media staff must follow the school media policy before responding.

- Unacceptable conduct, (e.g. defamatory, discriminatory, offensive, harassing content or a breach of data protection, confidentiality, copyright) will be considered extremely seriously by the school and will be reported as soon as possible to a relevant senior member of staff, and escalated where appropriate.
- The use of social media by staff while at work may be monitored, in line with school policies. *The school permits reasonable and appropriate access to private social media sites. However, where excessive use is suspected, and considered to be interfering with relevant duties, disciplinary action may be taken*
- The school will take appropriate action in the event of breaches of the social media policy. Where conduct is found to be unacceptable, the school will deal with the matter internally. Where conduct is considered illegal, the school will report the matter to the police and other relevant external agencies, and may take action according to the disciplinary policy.

Legal considerations

- Users of social media should consider the copyright of the content they are sharing and, where necessary, should seek permission from the copyright holder before sharing.
- Users must ensure that their use of social media does not infringe upon relevant data protection laws, or breach confidentiality.

Handling abuse

- When acting on behalf of the school, handle offensive comments swiftly and with sensitivity.
- If a conversation turns and becomes offensive or unacceptable, school users should block, report or delete other users or their comments/posts and should inform the audience exactly why the action was taken
- If you feel that you or someone else is subject to abuse by colleagues through use of a social networking site, then this action must be reported using the agreed school protocols.

Tone

The tone of content published on social media should be appropriate to the audience, whilst retaining appropriate levels of professional standards. Key words to consider when composing messages are:

- Engaging
- Conversational
- Informative
- Friendly (on certain platforms, e.g. Facebook)

Use of images

School use of images can be assumed to be acceptable, providing the following guidelines are strictly adhered to.

- Permission to use any photos or video recordings should be sought in line with the school's digital and video images policy. If anyone, for any reason, asks not to be filmed or photographed then their wishes should be respected.
- Under no circumstances should staff share or upload student pictures online other than via school owned social media accounts
- Staff should exercise their professional judgement about whether an image is appropriate to share on school social media accounts. Students should be appropriately dressed, not be subject to ridicule and must not be on any school list of children whose images must not be published.

- If a member of staff inadvertently takes a compromising picture which could be misconstrued or misused, they must delete it immediately.

Personal use

- **Staff**
    - Personal communications are those made via a personal social media accounts. In all cases, where a personal account is used which associates itself with the school or impacts on the school, it must be made clear that the member of staff is not communicating on behalf of the school with an appropriate disclaimer. Such personal communications are within the scope of this policy.
    - Personal communications which do not refer to or impact upon the school are outside the scope of this policy.
    - Where excessive personal use of social media in school is suspected, and considered to be interfering with relevant duties, disciplinary action may be taken
    - The school permits reasonable and appropriate access to private social media sites.
    - Staff are not permitted to follow students on their personal accounts or an account managed on behalf of the school if not regulated by designated social media team.

- **Students**
    - Staff are not permitted to follow or engage with current or prior students of the school on any personal social media network account.
    - The school's education programme should enable the students to be safe and responsible users of social media.
    - Students are encouraged to comment or post appropriately about the school. Any offensive or inappropriate comments will be resolved by the use of the school's behaviour policy

- **Parents/Carers**
    - If parents/carers have access to a school learning platform where posting or commenting is enabled, parents/carers will be informed about acceptable use.
    - The school has an active parent/carer education programme which supports the safe and positive use of social media. This includes information on the website.
    - Parents/Carers are encouraged to comment or post appropriately about the school. In the event of any offensive or inappropriate comments being made, the school will ask the parent/carer to remove the post and invite them to discuss the issues in person. If necessary, refer parents to the school's complaints procedures.

- **Comments posted by parents/carers**
    - Effective communication following principles of mutual respect is the best means of ensuring the best learning experiences for the child.
    - School policies and documents provide further information regarding appropriate channels of communication and means of resolving differences of opinion.
    - Parents must not post pictures of pupils, other than their own children, on social networking sites where these photographs have been taken at a school event.
    - Parents must not make complaints on social networking sites but through official school channels, to ensure that they can be dealt with appropriately.
    - Parents must not post malicious or fictitious comments on social networking sites about any member of the school community
    - In the case of inappropriate use of social networking by parents, the school will contact the parent asking them to remove such comments and seek redress through the appropriate channels.

In dealing with incidents of online bullying/inappropriate use of social networking sites the school understands that there are circumstances in which police involvement is appropriate. These include where postings have a racist element or where violence is threatened or encouraged

- ***"Laws of defamation and privacy still apply to the web and it is unlawful for statements to be written … which:***
    - ***expose (an individual) to hatred, ridicule or contempt***
    - ***cause (an individual) to be shunned or avoided***
    - ***lower (an individual's) standing in the estimation of right-thinking members of society or***
    - ***disparage (an individual in their) business, trade, office or profession****."*

Monitoring posts about the school

- As part of active social media engagement, it is considered good practice to pro-actively monitor the Internet for public postings about the school.
- The school should effectively respond to social media comments made by others according to a defined policy or process.

Appendix

Managing your personal use of Social Media:

- "Nothing" on social media is truly private
- Social media can blur the lines between your professional and private life. Don't use the school logo and/or branding on personal accounts
- Check your settings regularly and test your privacy
- Keep an eye on your digital footprint
- Keep your personal information private
- Regularly review your connections – keep them to those you want to be connected to
- When posting online consider; Scale, Audience and Permanency of what you post
- If you want to criticise, do it politely.
- Take control of your images – do you want to be tagged in an image? What would children or parents say about you if they could see your images?
- Know how to report a problem

Managing school social media accounts

The Do's

- Check with a senior leader before publishing content that may have controversial implications for the school
- Use a disclaimer when expressing personal views
- Make it clear who is posting content
- Use an appropriate and professional tone
- Be respectful to all parties
- Ensure you have permission to 'share' other peoples' materials and acknowledge the author
- Express opinions but do so in a balanced and measured manner
- Think before responding to comments and, when in doubt, get a second opinion
- Seek advice and report any mistakes using the school's reporting process
- Consider turning off tagging people in images where possible

The Don'ts

- Don't make comments, post content or link to materials that will bring the school into disrepute
- Don't publish confidential or commercially sensitive material
- Don't breach copyright, data protection or other relevant legislation
- Consider the appropriateness of content for any audience of school accounts, and don't link to, embed or add potentially inappropriate content
- Don't post derogatory, defamatory, offensive, harassing or discriminatory content
- Don't use social media to air internal grievances

E-Safety Section

Charlton School recognises that ICT and the internet are fantastic tools for learning and communication that can be used in school to enhance the curriculum, challenge students, and support creativity and independence. Using ICT to interact socially and share ideas can benefit everyone in the school community, but it is important that the use of the internet and ICT is seen as a responsibility and that students, staff and parents use it appropriately and practice good e-safety. It is important that all members of the school community are aware of the dangers of using the internet and how they should conduct themselves online. E-safety covers the internet but it also covers mobile phones and other electronic communications technologies. We know that some adults and young people will use these technologies to harm children. The harm might range from sending hurtful or abusive texts and emails, to enticing children to engage in sexually harmful conversations or actions online, webcam filming, photography or face-to-face meetings. There is a 'duty of care' for any persons working with children and educating all members of the school community on the risks and responsibilities of e-safety falls under this duty. It is important that there is a balance between controlling access to the internet and technology and allowing freedom to explore and use these tools to their full potential. This policy aims to be an aid in regulating ICT activity in school, and provide a good understanding of appropriate ICT use that members of the school community can use as a reference for their conduct online outside of school hours. E-safety is a whole-school issue and responsibility. Cyber-bullying by pupils will be treated as seriously as any other type of bullying and will be managed through our anti-bullying procedures which are outlined in our behaviour policy.

1. Roles and responsibility

The School e-Safety Coordinator is Assistant Vice Principal for Safeguarding, Angela Bithell

The designated member of the governing body responsible for e-safety is Ricki Thiara

2. Communicating school policy

This policy is available from the school office and on the school website for parents, staff, and pupils to access when and as they wish. Rules relating to the school code of conduct when online, and e-safety guidelines, are displayed around the school. E-safety is integrated into the curriculum in any circumstance where the internet or technology are being used, and during PSHEE lessons where personal safety, responsibility, and/or development are being discussed.

3. Making use of ICT and the internet in school

The internet is used in school to raise educational standards, to promote pupil achievement, to support the professional work of staff and to enhance the school's management functions. Technology is advancing rapidly and is now a huge part of everyday life,

education and business. We want to equip our students with all the necessary ICT skills that they will need in order to enable them to progress confidently into a professional working environment when they leave school. Some of the benefits of using ICT and the internet in schools are:

For students:

- Unlimited access to worldwide educational resources and institutions such as art galleries, museums and libraries.
- Contact with schools in other countries resulting in cultural exchanges between pupils all over the world.
- Access to subject experts, role models, inspirational people and organisations. The internet can provide a great opportunity for pupils to interact with people that they otherwise would never be able to meet.
- An enhanced curriculum; interactive learning tools; collaboration, locally, nationally, and globally; self-evaluation; feedback and assessment; updates on current affairs as they happen.
- Access to learning whenever and wherever convenient.
- Freedom to be creative.
- Freedom to explore the world and its cultures from within a classroom.
- Social inclusion, in class and online.
- Access to case studies, videos and interactive media to enhance understanding.
- Individualised access to learning.

For staff:

- Professional development through access to national developments, educational materials and examples of effective curriculum practice and classroom strategies.
- Immediate professional and personal support through networks and associations.
- Improved access to technical support.
- Ability to provide immediate feedback to students and parents.
- Class management, attendance records, schedule, and assignment tracking

4. Learning to evaluate internet content

With so much information available online it is important that pupils learn how to evaluate internet content for accuracy and intent. This is approached by the school as part of digital literacy across all subjects in the curriculum. Students will be taught:

- to be critically aware of materials they read, and shown how to validate information before accepting it as accurate
- to use age-appropriate tools to search for information online
- to acknowledge the source of information used and to respect copyright. Plagiarism is against the law and the school will take any intentional acts of plagiary very seriously. Students who are found to have plagiarised will be disciplined. If they have plagiarised in an exam or a piece of coursework, they may be prohibited from completing that exam.

The school will also take steps to filter internet content to ensure that it is appropriate to the age and maturity of pupils. If staff or pupils discover unsuitable sites then the URL will be reported to the school e-safety coordinator. Any material found by members of the school community that is believed to be unlawful will be reported to the appropriate agencies. Regular software and broadband checks will take place to ensure that filtering services are working effectively. (Appendix 1)

5. Managing information systems

The school is responsible for reviewing and managing the security of the computers and internet networks as a whole and takes the protection of school data and personal protection of our school community very seriously. This means protecting the school network, as far as is practicably possible, against viruses, hackers and other external security threats. The security of the school information systems and users will be reviewed regularly by the IT technicians and network manager and virus protection software will be updated regularly.

Some safeguards that the school takes to secure our computer systems are:

- ensuring that all personal data sent over the internet or taken off site is encrypted
- making sure that unapproved software is not downloaded to any school computers. Alerts will be set up to warn users of this
- files held on the school network will be regularly checked for viruses
- the use of user logins and passwords to access the school network will be enforced
- portable media containing school data or programmes will not be taken off-site without specific permission from a member of the senior leadership team.

For more information on data protection in school please refer to our data protection policy. More information on protecting personal data can be found in section 11 of this policy.

6. Emails

The school uses email internally for staff and pupils, and externally for contacting parents, and is an essential part of school communication. It is also used to enhance the curriculum by:

- initiating contact and projects with other schools nationally and internationally
- providing immediate feedback on work, and requests for support where it is needed.

Staff and pupils should be aware that school email accounts should only be used for school-related matters, ie for staff to contact parents, students, other members of staff and other professionals for work purposes. This is important for confidentiality. The school has the right to monitor emails and their contents but will only do so if it feels there is reason to.

6.2 School email accounts and appropriate use

Staff should be aware of the following when using email in school:

• Staff should only use official school-provided email accounts to communicate with pupils, parents or carers. Personal email accounts should not be used to contact any of these people and should not be accessed during school hours.

• Emails sent from school accounts should be professionally and carefully written. Staff are representing the school at all times and should take this into account when entering into any email communications.

• Staff must tell their manager or a member of the senior leadership team if they receive any offensive, threatening or unsuitable emails either from within the school or from an external account. They should not attempt to deal with this themselves.

• The forwarding of chain messages is not permitted in school. Students should be aware of the following when using email in school, and will be taught to follow these guidelines through the ICT curriculum and in any instance where email is being used within the curriculum or in class:

- in school, pupils should only use school-approved email accounts
- excessive social emailing will be restricted
- pupils should tell a member of staff if they receive any offensive, threatening or unsuitable emails either from within the school or from an external account. They should not attempt to deal with this themselves.
- pupils must be careful not to reveal any personal information over email, or arrange to meet up with anyone who they have met online without specific permission from an adult in charge.
- Pupils will be educated through the ICT curriculum to identify spam, phishing and virus emails and attachments that could cause harm to the school network or their personal account or wellbeing.

7. Published content and the school website

The school website is viewed as a useful tool for communicating our school ethos and practice to the wider community. It is also a valuable resource for parents, students, and staff for keeping up-to-date with school news and events, celebrating whole-school achievements and personal achievements, and promoting school projects. The website is in the public domain, and can be viewed by anybody online. Any information published on the website will be carefully considered in terms of safety for the school community, copyrights and privacy policies. No personal information on staff or pupils will be published, and details for contacting the school will be for the school office only. For information on the school policy on children's photographs on the school website please refer to section 7.2 of this policy.

7.2 Policy and guidance of safe use of children's photographs and work

Colour photographs and pupils work bring our school to life, showcase our student's talents, and add interest to publications both online and in print that represent the school. However, the school acknowledges the importance of having safety precautions in place to prevent the misuse of such material.

Under the Data Protection Act 1998 images of pupils and staff will not be displayed in public, either in print or online, without consent. On admission to the school parents/carers will be asked to sign a photography consent form. The school does this so as to prevent repeatedly asking parents for consent over the school year, which is time-consuming for both parents and the school. The terms of use of photographs never change, and so consenting to the use of photographs of your child over a period of time rather than a one-off incident does not affect what you are consenting to. This consent form will outline the school's policy on the use of photographs of children, including:

- how and when the photographs will be used
- how long parents are consenting the use of the images for
- school policy on the storage and deletion of photographs.

<u>Using photographs of individual children</u>.
The vast majority of people who take or view photographs or videos of children do so for entirely innocent, understandable and acceptable reasons. Sadly, some people abuse children through taking or using images, so we must ensure that we have some safeguards in place. It is important that published images do not identify students or put them at risk of being identified. The school is careful to ensure that images published on the school website cannot be reused or manipulated through watermarking and browser restrictions. Only images created by or for the school will be used in public and children may not be approached or photographed while in school or doing school activities without the school's permission.

The school follows general rules on the use of photographs of individual children:
Parental consent must be obtained.

Consent will cover the use of images in:

- all school publications
- on the school website
- in newspapers as allowed by the school
- in videos made by the school or in class for school projects.
- through the school's social media channels

- Electronic and paper images will be stored securely.
- Names of stored photographic files will not identify the child.
- Images will be carefully chosen to ensure that they do not pose a risk of misuse. This includes ensuring that pupils are appropriately dressed. Photographs of activities which may pose a greater risk of potential misuse (for example, swimming activities), will focus more on the sport than the pupils (ie a student in a swimming pool, rather than standing by the side in a swimsuit).

- For public documents, including in newspapers, full names will not be published alongside images of the child. Groups may be referred to collectively by year group or form name.
- Events recorded by family members of the students such as school plays or sports days must be used for personal use only.
- Pupils are encouraged to tell a member staff if they are concerned or uncomfortable with any photographs that are taken of them or they are being asked to participate in.
- Any photographers that are commissioned by the school will be fully briefed on appropriateness in terms of content and behaviour, will wear identification at all times, and will not have unsupervised access to the pupils. For more information on safeguarding in school please refer to our school child protection and safeguarding policy.

6.3 Complaints of misuse of photographs or video

Parents should follow standard school complaints procedure if they have a concern or complaint regarding the misuse of school photographs. Please refer to our complaints policy for more information on the steps to take when making a complaint. Any issues or sanctions will be dealt with in line with the schools' child protection and safeguarding policy and behaviour policy.

6.4 Social networking, social media and personal publishing

Personal publishing tools include blogs, wikis, social networking sites, bulletin boards, chat rooms and instant messaging programmes. These online forums are the more obvious sources of inappropriate and harmful behaviour and where pupils are most vulnerable to being contacted by a dangerous person. It is important that we educate students so that they can make their own informed decisions and take responsibility for their conduct online. Pupils are not allowed to access social media sites in school. There are various restrictions on the use of these sites in school that apply to both students and staff. Social media sites have many benefits for both personal use and professional learning; however, both staff and students should be aware of how they present themselves online. Students are taught through the ICT curriculum and PSHEE about the risks and responsibility of uploading personal information and the difficulty of taking it down completely once it is out in such a public place. The school follows general rules on the use of social media and social networking sites in school:

- Pupils are educated on the dangers of social networking sites and how to use them in safe and productive ways. They are all made fully aware of the school's code of conduct regarding the use of ICT and technologies and behaviour online.
- Any sites that are to be used in class will be risk-assessed by the teacher in charge prior to the lesson to ensure that the site is age-appropriate and safe for use.
- Official school blogs created by staff or students/year groups/school clubs as part of the school curriculum will be password-protected and run from

the school website with the approval of a member of staff and will be moderated by a member of staff.

- Pupils and staff are encouraged not to publish specific and detailed private thoughts, especially those that might be considered hurtful, harmful or defamatory. The school expects all staff and pupils to remember that they are representing the school at all times and must act appropriately.
- Safe and professional behaviour of staff online will be discussed at staff induction.

8. Mobile phones and personal device

While mobile phones and personal communication devices are commonplace in today's society, their use and the responsibility for using them should not be taken lightly. Some issues surrounding the possession of these devices are:

- they can make pupils and staff more vulnerable to cyberbullying
- they can be used to access inappropriate internet material
- they can be a distraction in the classroom
- they are valuable items that could be stolen, damaged, or lost
- they can have integrated cameras, which can lead to child protection, bullying and data protection issues.

The school takes certain measures to ensure that mobile phones are used responsibly in school. Some of these are outlined in our mobile devices policy.

9. Cyberbullying

Cyberbullying, as with any other form of peer on peer abuse, is taken very seriously by the school. Information about specific strategies or programmes in place to prevent and tackle bullying are set out in the behaviour policy. The anonymity that can come with using the internet can sometimes make people feel safe to say and do hurtful things that they otherwise would not do in person. It is made very clear to members of the school community what is expected of them in terms of respecting their peers, members of the public and staff, and any intentional breach of this will result in disciplinary action. If an allegation of bullying does come up, the school will:

- take it seriously
- act as quickly as possible to establish the facts. It may be necessary to examine school systems and logs or contact the service provider in order to identify the bully
- record and report the incident
- provide support and reassurance to the victim
- make it clear to the 'bully' that this behaviour will not be tolerated.

If there is a group of people involved, they will be spoken to individually and as a whole group. It is important that children who have harmed another, either physically or emotionally, redress their actions and the school will make sure that they understand what they have done and the impact of their actions. If a sanction is used, it will correlate to the seriousness of the incident and the 'bully' will be told why it is being used. They will be asked to remove any harmful or inappropriate content that has been published, and the service provider may be contacted to do this if they refuse or are unable to remove it. They may have their internet access suspended in school. Repeated bullying may result in a fixed-term exclusion.

10. Managing emerging technologies

Technology is progressing rapidly and new technologies are emerging all the time. The school will risk-assess any new technologies before they are allowed in school, and will consider any educational benefits that they might have. The school keeps up-to-date with new technologies and is prepared to quickly develop appropriate strategies for dealing with new technological developments.

11. Protecting personal data

Charlton School believes that protecting the privacy of our staff and pupils and regulating their safety through data management, control and evaluation is vital to whole-school and individual progress. The school collects personal data from pupils, parents, and staff and processes it in order to support teaching and learning, monitor and report on pupil and teacher progress, and strengthen our pastoral provision. We take responsibility for ensuring that any data that we collect and process is used correctly and only as is necessary, and the school will keep parents fully informed of the how data is collected, what is collected, and how it is used. National curriculum results, attendance and registration records, special educational needs data, and any relevant medical information are examples of the type of data that the school needs. Through effective data management we can monitor a range of school provisions and evaluate the wellbeing and academic progression of our school body to ensure that we are doing all we can to support both staff and students.

In line with the Data Protection Act 1998, and following principles of good practice when processing data, the school will:

- ensure that data is fairly and lawfully processed
- process data only for limited purposes
- ensure that all data processed is adequate, relevant and not excessive
- ensure that data processed is accurate
- not keep data longer than is necessary
- process the data in accordance with the data subject's rights
- ensure that data is secure
- ensure that data is not transferred to other countries without adequate protection.

There may be circumstances where the school is required either by law or in the best interests of our students or staff to pass information onto external authorities; for example, our local authority, Ofsted, or the Department of Health. These authorities are up-to-date with data protection law and have their own policies relating to the protection of any data that they receive or collect. For more information on the school's safeguards relating to data protection read the school's data protection policy.

Appendices

Appropriate Filtering for Education settings

May 2025

Schools[1] in England (and Wales) are required "*to ensure children are safe from terrorist and extremist material when accessing the internet in school, including by establishing appropriate levels of filtering*"[2]. Furthermore, the Department for Education's statutory guidance 'Keeping Children Safe in Education' [3] obliges schools and colleges in England to "*ensure appropriate filters and appropriate monitoring systems are in place and regularly review their effectiveness" and they "should be doing all that they reasonably can to limit children's exposure to the above risks*[4] *from the school's or college's IT system*" however, schools will need to "*be careful that "over blocking" does not lead to unreasonable restrictions as to what children can be taught with regards to online teaching and safeguarding*." Ofsted concluded as far back as 2010[5] that "Pupils in the schools that had 'managed' systems had better knowledge and understanding of how to stay safe than those in schools with 'locked down' systems. Pupils were more vulnerable overall when schools used locked down systems because they were not given enough opportunities to learn how to assess and manage risk for themselves."

To further support schools and colleges in England to meet digital and technology standards, the Department for Education published Filtering and Monitoring Standards[6] in March 2023 (as part of a broader suite of educational technology standards and guidance)[7]. In addition to aspects of both filtering and monitoring systems, these standards detail the allocation of roles and responsibilities, and that schools and colleges should be checking their filtering and monitoring provision at least annually. These standards were included within Keeping Children Safe in Education in 2023.

The Welsh Government has published a common set of agreed standards for internet access provides the tools for schools to make informed choices over filtered provision whether delivered by the local authority or another provider[8].

Previously included within the Scottish Government national action plan on internet safety [9], schools in Scotland are expected to "*have policies in place relating to the use of IT and to use filtering as a means of restricting access to harmful content*."

---

[1] The schools and registered childcare settings specified in Schedule 6 of the Counter-Terrorism and Security Act 2015 (CTSA 2015)

[2] Revised Prevent Duty Guidance: for England and Wales, 2015, https://www.gov.uk/government/publications/prevent-duty-guidance

[3] https://www.gov.uk/government/publications/keeping-children-safe-in-education--2

[4] Keeping Children Safe in Education Paragraph 136, Page 35 – Content, Contact, Conduct, Commerce

[5] Safe Use of New Technologies - http://webarchive.nationalarchives.gov.uk/20141107033803/http://www.ofsted.gov.uk/resources/safe-use-of-new-technologies

[6] https://www.gov.uk/guidance/meeting-digital-and-technology-standards-in-schools-and-colleges/filtering-and-monitoring-standards-for-schools-and-colleges

[7] Meeting digital and technology standards in schools and colleges - Guidance - GOV.UK (www.gov.uk)

[8] Web Filtering Standards - Hwb (gov.wales) https://hwb.gov.wales/support-centre/education-digital-standards/web-filtering-standards

[9] National Action Plan on Internet Safety for Children and Young People, April 2017, http://www.gov.scot/Publications/2017/04/1061

The aim of this document is to help education settings (including Early years, schools and FE) and filtering providers comprehend what should be considered as 'appropriate filtering'.

It is important to recognise that no filtering systems can be 100% effective and need to be supported with good teaching and learning practice and effective supervision. As such, filtering systems should be recognised as one of the tools used to support and inform the broader safeguarding provision in settings.

Illegal Online Content

The Online Safety Act now sets out[10] the kinds of illegal content and activity that includes content relating to:

child sexual abuse	Content that depicts or promotes sexual abuse or exploitation of children, which is strictly prohibited and subject to severe legal penalties.
controlling or coercive behaviour	Online actions that involve psychological abuse, manipulation, or intimidation to control another individual, often occurring in domestic contexts.
extreme sexual violence	Content that graphically depicts acts of severe sexual violence, intended to shock or incite similar behaviour, and is illegal under UK law.
extreme pornography	Pornographic material portraying acts that threaten a person's life or could result in serious injury, and is deemed obscene and unlawful.
fraud	Deceptive practices conducted online with the intent to secure unfair or unlawful financial gain, including phishing and scam activities.
racially or religiously aggravated public order offences	Content that incites hatred or violence against individuals based on race or religion, undermining public safety and cohesion.
inciting violence	Online material that encourages or glorifies acts of violence, posing significant risks to public safety and order.
illegal immigration and people smuggling	Content that promotes or facilitates unauthorized entry into a country, including services offering illegal transportation or documentation.
promoting or facilitating suicide	Material that encourages or assists individuals in committing suicide, posing serious risks to vulnerable populations.
intimate image abuse	The non-consensual sharing of private sexual images or videos, commonly known as "revenge porn," intended to cause distress or harm.
selling illegal drugs or weapons	Online activities involving the advertisement or sale of prohibited substances or firearms, contravening legal regulations.
sexual exploitation	Content that involves taking advantage of individuals sexually for personal gain or profit, including trafficking and forced prostitution.
Terrorism	Material that promotes, incites, or instructs on terrorist activities, aiming to radicalise individuals or coordinate acts of terror.

Schools should satisfy themselves that their filtering system manages this type of content specifically that the filtering providers:

- Are IWF members and use IWF services to block access to illegal Child Sexual Abuse Material (CSAM)
- Integrate the 'the police assessed list of unlawful terrorist content, produced on behalf of the Home Office'

Schools should ensure that these blocklists (IWF and CTIRU) are included with their filtering system and that anyone in your school or college should not be able to disable these blocklists or remove items from them (including any system administrator).

[10] Online Safety Act: explainer - GOV.UK

Inappropriate Online Content

Recognising that no filter can guarantee to be 100% effective, schools should be satisfied that their filtering system additionally manages the following inappropriate) content (and web search) including 'Primary Priority Content' and 'Priority Content' (as described by the Online Safety Act)

Content	Explanatory notes – Content that:
Gambling	Enables gambling
Hate speech / Discrimination	Content that expresses hate or encourages violence towards a person or group based on something such as disability, race, religion, sex, or sexual orientation. Promotes the unjust or prejudicial treatment of people with protected characteristics of the Equality Act 2010
Harmful content	Content that is bullying, abusive or hateful. Content which depicts or encourages serious violence or injury. Content which encourages dangerous stunts and challenges; including the ingestion, inhalation or exposure to harmful substances.
Malware / Hacking	promotes the compromising of systems including anonymous browsing and other filter bypass tools as well as sites hosting malicious content, including ransomware and viruses
Mis / Dis Information	Promotes or spreads false or misleading information intended to deceive, manipulate, or harm, including content undermining trust in factual information or institutions
Piracy and copyright theft	includes illegal provision of copyrighted material
Pornography	displays sexual acts or explicit images and text
Self-Harm and eating disorders	content that encourages, promotes, or provides instructions for self harm, eating disorders or suicide
Violence Against Women and Girls (VAWG)	Promotes or glorifies violence, abuse, coercion, or harmful stereotypes targeting women and girls, including content that normalises gender-based violence or perpetuates misogyny.

This list should not be considered an exhaustive list and providers will be able to demonstrate how their system manages this content and many other aspects.

Regarding the retention of logfile (Internet history), as the data controller, schools should understand their filtering providers data retention policies including the duration to which all data is retained and have associated data sharing agreements. Logfiles (Internet history) should include the identification of individuals and/or devices.

Providers should be clear how their system does not over block access so it does not lead to unreasonable restrictions. Welsh Government highlight that "It is critical that filtering standards are fit for purpose for 21*st* century teaching and learning, allowing the access schools require whilst still safeguarding children and young people."[11]

Given the extent of personal data involved with some filtering systems, Schools and Colleges should consider undertaking a Data Protection Impact Assessment[12] and ensure that this aligns with the organisational policies.

[11] Welsh Government Filtering Standards https://hwb.gov.wales/support-centre/education-digital-standards/web-filtering-standards#document

[12] https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/lawful-basis-for-processing/

Filtering System Features

Additionally, and in context of their safeguarding needs, schools should consider the required features of their filtering system;

- Context appropriate differentiated filtering, based on age, vulnerability and risk of harm – also includes the ability to vary filtering strength appropriate for staff
- Circumvention – the extent and ability to identify and manage technologies and techniques used to circumvent the system, for example VPN, proxy services, DNS over HTTPS and ECH.
- Control – has the ability and ease of use that allows schools to control the filter themselves to permit or deny access to specific content. Any changes to the filter system are logged enabling an audit trail that ensure transparency and that individuals are not able to make unilateral changes.
- Contextual Content Filters – in addition to URL or IP based filtering, Schools should understand the extent to which (http and https) content is dynamically analysed as it is streamed in real time to the user and blocked. This would include AI or user generated content, for example, being able to contextually analyse text and dynamically filter the content produced (for example ChatGPT). For schools' strategy or policy that allows the use of AI or user generated content, understanding the technical limitations of the system, such as whether it supports real-time filtering, is important.
- Deployment – filtering systems can be deployed in a variety (and combination) of ways (e.g. on device, network level, cloud, DNS). Providers should describe how their systems are deployed alongside any required configurations and/or limitations. As technology and security standards evolve, relying solely on network-level filters may become increasingly challenging and less effective. Schools might consider combining network-level filtering with device-level configurations tailored to school-owned and managed devices.
- Filtering Policy – the filtering provider publishes a rationale that details their approach to filtering with classification and categorisation as well as how the system addresses over blocking
- Group / Multi-site Management – the ability for deployment of central policy and central oversight or dashboard
- Identification - the filtering system should have the ability to identify users and devices to attribute access (particularly for mobile devices) and allow the application of appropriate configurations and restrictions for individual users. This would ensure safer and more personalised filtering experiences.
- Mobile and App content – mobile and app content is often delivered in entirely different mechanisms from that delivered through a traditional web browser. To what extent does the filter system block inappropriate content via mobile and app technologies (beyond typical web browser delivered content). Providers should be clear about the capability of their filtering system to manage content on mobile and web apps and any configuration or component requirements to achieve this.
- Multiple language support – the ability for the system to manage relevant languages
- Remote devices – with many children and staff working remotely, the ability for school owned devices to receive the same or equivalent filtering to that provided in school
- Reporting mechanism – the ability to report inappropriate content for access or blocking
- Reports – the system offers clear granular historical information on the websites users have accessed or attempted to access
- Safe Search – the ability to enforce 'safe search' when using search engines
- Safeguarding case management integration – the ability to integrate with school safeguarding and wellbeing systems to better understand context of activity

Schools and Colleges should ensure that there is sufficient capability and capacity in those responsible for, and those managing, the filtering system (including any external support provider). The UK Safer Internet Centre Helpline[13] may be a source of support for schools looking for further advice in this regard.

Filtering systems are only ever a tool in helping to safeguard children when online and schools have an obligation to "*consider how children may be taught about safeguarding, including online, through teaching and learning opportunities, as part of providing a broad and balanced curriculum"*[14]. To assist schools and colleges in shaping an effective curriculum, UK Safer Internet Centre has published ProjectEVOLVE[15]

Risk Assessment

UK Safer Internet Centre recommends that those responsible for Schools and Colleges undertake (and document) an online safety risk assessment at least annually or whenever any substantive changes occur, assessing their online safety provision that would include filtering (and monitoring) provision. The risk assessment should consider the risks that both children[16] and staff may encounter online, together with associated mitigating actions and activities.

A risk assessment module has been integrated in *360 degree safe*[17]. Here schools can consider identify and record the risks posed by technology and the internet to their school, children, staff and parents.

Checks and Documentation

Schools and Colleges should regularly check that their filtering and monitoring systems are effective and applied to all devices. Checks should be conducted when significant changes take place (for example, technology, policy or legislation), in response to incidents and at least annually. These checks should be recorded, including details about the location, device and user alongside the result and any associated action.

SWGfL testfiltering.com enables users to test fundamental capabilities of their filtering system and to inform improvement.

Filtering on Mobile devices

Schools and colleges should satisfy themselves that filtering systems are correctly working across all their devices' and across all internet connections, including their mobile devices. If your school owns mobile devices such as iPads or other tablets as part of your teaching strategy, then consider the following practices to ensure filtering is in place (you may need the help of your ICT support to do this):

For schools and colleges in England, the following DfE guidance is relevant

- Digital leadership and governance standards - Guidance - GOV.UK (www.gov.uk) – specifically guidance related asset registers in context of points 1 and 2 below
- Laptop, desktop and tablet standards - Guidance - GOV.UK (www.gov.uk)
- Mobile phones in schools - GOV.UK (www.gov.uk)

[13] https://www.saferinternet.org.uk/helpline
[14] https://www.gov.uk/government/publications/keeping-children-safe-in-education--2
[15] ProjectEVOLVE - Education for a Connected World Resources (https://projectevolve.co.uk/)
[16] http://netchildrengomobile.eu/ncgm/wp-content/uploads/2014/11/EU-Kids-Online-Net-Children-Go-Mobile-comparative-report.pdf
[17] www.360safe.org.uk, https://360safecymru.org.uk/, http://www.360safescotland.org.uk/

1. Audit the mobile device estate by detailing all the mobile devices they have.
2. Understand and detail the applications (apps) they use and how these are managed (installed and deleted). Specifically, ensure that apps can be centrally, and routinely, removed from mobile devices. This is best achieved through the use of a Mobile Device Management (MDM).
3. Identify who is responsible for mobile devices as well as filtering and monitoring solutions at the school, ensuring that the DSL is also aware (if different).
4. Test to provide confidence that the schools filtering and monitoring system is working across all mobile devices, across installed apps (not just internet browsers) and in various physical locations. Does filtering continue when away from the school network? Schools can use testfiltering.com to help in this regard.
5. Identify any vulnerable users of mobile devices, paying particular attention to ensure harmful content is not accessible on specific devices

Generative AI Technologies

New technology is enabling users to generate personalised content in real-time based on prompts and schools are being encouraged to exploit these potential advantages for "faster planning and record-keeping"[18]. The real-time nature and proliferation of these system present a challenge to schools when it comes to filtering this type of content. Filtering systems should effectively and reliably prevent access to harmful and inappropriate content generated by Generative AI systems. Schools should reflect on the following, as part of any risk assessment, when considering their systems and deciding what generative AI systems they allow students and staff to use:

- The level to which your filtering system can block content in real-time
- Assessing which generative AI systems the school which to approve for use after assessing safety features, and data protection
- Developing a policy around the use of generative AI systems
- Assessment of your ability to generate reports on the usage or generative AI systems within school

Further Governmental considerations for adopting Generative AI technologies in schools:

- England – Generative artificial intelligence (AI) in education - GOV.UK (Jan 2025)

  The DfE's *Generative AI: Product Safety Expectations* sets out clear guidance for ensuring AI tools used in schools are safe by design, including expectations for risk assessment, content moderation, transparency, and reporting—providing a helpful benchmark when determining which generative AI platforms should be accessible through school filtering systems.

- Wales - Generative artificial intelligence in education - Hwb (Jan 2025)

This detail has been developed by the SWGfL, as a partner of the UK Safer Internet Centre, and in partnership and consultation with the 80 national '*360 degree safe Online Safety Mark*'[19] assessors and the NEN Safeguarding group (www.nen.gov.uk).

[18] Artificial Intelligence: Plan to 'unleash AI' across UK revealed - BBC News

[19] www.360safe.org.uk, https://360safecymru.org.uk/, http://www.360safescotland.org.uk/

Appropriate Filtering for Education settings

May 2025

Filtering Provider Checklist Reponses

Schools (and registered childcare providers) in England and Wales are required "to ensure children are safe from terrorist and extremist material when accessing the internet in school, including by establishing appropriate levels of filtering". Furthermore, it expects that they "assess the risk of [their] children being drawn into terrorism, including support for extremist ideas that are part of terrorist ideology". There are a number of self review systems (eg www.360safe.org.uk) that will support a school in assessing their wider online safety policy and practice.

The Department for Education's statutory guidance 'Keeping Children Safe in Education' obliges schools and colleges in England to "*ensure appropriate filters and appropriate monitoring systems are in place and regularly review their effectiveness" and they "should be doing all that they reasonably can to limit children's exposure to [Content, Contact, Conduct, Contract] risks from the school's or college's IT system*" however, schools will need to "*be careful that "over blocking" does not lead to unreasonable restrictions as to what children can be taught with regards to online teaching and safeguarding*."

By completing all fields and returning to UK Safer Internet Centre (enquiries@saferinternet.org.uk), the aim of this document is to help filtering providers to illustrate to education settings (including Early years, schools and FE) how their particular technology system(s) meets the national defined 'appropriate filtering standards. Fully completed forms will be hosted on the UK Safer Internet Centre website alongside the definitions

It is important to recognise that no filtering systems can be 100% effective and need to be supported with good teaching and learning practice and effective supervision.

Company / Organisation	Lightspeed Systems
Address	Phoenix House, Christopher Martin Road, Basildon, Essex, SS14 3EZ
Contact details	+44 (0) 20 4534 5200 / sales@lightspeedsystems.com
Filtering System	Lightspeed Filter™
Date of assessment	May 2025

System Rating response

Where a supplier is able to confirm that their service fully meets the issue identified in a specific checklist the appropriate self-certification colour for that question is GREEN.	
Where a supplier is not able to confirm that their service fully meets the issue identified in a specific checklist question the appropriate self-certification colour for that question is AMBER.	

.

Illegal Online Content

Filtering providers should ensure that access to illegal content is blocked, specifically that the filtering providers:

Aspect	Rating	Explanation
• Are IWF members		Lightspeed Systems has been a member of IWF since 2009.
• and block access to illegal Child Abuse Images (by actively implementing the IWF URL list), including frequency of URL list update		Web pages or URLs that depict indecent images of children, advertisements for such content, or links to it are illegal and constantly tracked by IWF (Internet Watch Foundation). Lightspeed Systems immediately updates its Filter categories to match the IWF list and completely lock down access.
• Integrate the 'the police assessed list of unlawful terrorist content, produced on behalf of the Home Office'		To assist schools in complying with the Prevent Duty Guidance of the United Kingdom Counter Terrorism and Security Act 2015, Lightspeed Systems has established the *violence.extremism* category. This category is populated with a list of web addresses that promote extremism and/or radicalisation and is provided from The Home Office in the UK. The *violence.extremism* category is updated each time the Home Office supplies us with a list. Advanced reporting features allow IT administrators to easily view Internet activity across the whole school- or drill down to individual user activity. Also, email alerts can be set up so suspicious search activity notifies designated staff.
• Confirm that filters for illegal content cannot be disabled by anyone at the school (including any system administrator).		All websites categorised as illegal in Lightspeed's extensive, constantly updated URL database are placed in sealed categories that cannot be allowed by any IT admin or member of staff in a school or organisation.

Describing how, their system manages the following illegal content

Content	Explanatory notes – Content that:	Rating	Explanation
child sexual abuse	Content that depicts or promotes sexual abuse or exploitation of children, which is strictly prohibited and subject to severe legal penalties.		Any online material depicting child sexual abuse will be placed in the *porn.illicit* category which is permanently blocked. The category is constantly updated using our advanced web crawlers and the latest IWF lists.
controlling or coercive behaviour	Online actions that involve psychological abuse, manipulation, or intimidation to control another individual, often occurring in domestic contexts.		Locked categories such as *offensive* would stop students being able to access websites that would encourage coercive behaviour. Our safeguarding solution, Lightspeed Alert™, built into the filter also notifies the school when students type anything related to violence or cyberbullying.
extreme sexual violence	Content that graphically depicts acts of severe sexual violence, intended to shock or incite similar behaviour, and is illegal under UK law.		This content will be blocked using our sealed *offensive* category, blocking all gratuitous images of sexual violence and our broader *violence* category.
extreme pornography	Pornographic material portraying acts that threaten a person's life or could result in serious injury, and is deemed obscene and unlawful.		All potentially illegal pornographic material is locked in the *porn.illicit* category, containing potentially illegal and more severe pornographic material.
fraud	Deceptive practices conducted online with the intent to secure unfair or unlawful financial gain, including phishing and scam activities.		S*ecurity.malware* contains a combination of the *Security.virus, Security.spyware* and *Security.phishing* categories to protect users personal information and block all scams.
racially or religiously aggravated public order offences	Content that incites hatred or violence against individuals based on race or religion, undermining public safety and cohesion.		*The* permanently locked *violence.hate* and *offensive* categories would protect students from content that encourages racism or xenophobia of any kind.
inciting violence	Online material that encourages or glorifies acts of violence, posing significant risks to public safety and order.		Our *violence* category contains all sites that promote the use of physical force intended to harm or kill. Lightspeed Alert also notifies admins when students type anything related to violence.
illegal immigration and people smuggling	Content that promotes or facilitates unauthorized entry into a country, including services		Our *society.crime* category will automatically block anything related to crime and the justice

	offering illegal transportation or documentation.		system, including content promoting illegal immigration.
promoting or facilitating suicide	Material that encourages or assists individuals in committing suicide, posing serious risks to vulnerable populations.		To prevent any students from looking at websites that promote or display self-harm schools and several different categories can be controlled such as *forums* and *adult.* Our safeguarding solution Lightspeed Alert uses advanced AI and a 24/7 safety specialist team to notify administrators instantly when a student types anything relating to self-harm online. Alert works across all productivity and education apps, files, chat including Microsoft Teams and Google Workspace and provides schools with a timeline of the event including screenshots and activity logs.
intimate image abuse	The non-consensual sharing of private sexual images or videos, commonly known as "revenge porn," intended to cause distress or harm.		The *porn.illicit* category blocks any intimate images shared on any site with Lightspeed Filter an reports on any user who is attempting to access them. The image scanning technology built into Lightspeed Alert immediately identifies any sexual images, videos and users sharing them for intervention.
selling illegal drugs or weapons	Online activities involving the advertisement or sale of prohibited substances or firearms, contravening legal regulations.		We have specific categories for blocking access to *drugs* and our *security.proxy* category prohibits applications such as Tor browser, blocking access to the Dark Web and illegal marketplaces.
sexual exploitation	Content that involves taking advantage of individuals sexually for personal gain or profit, including trafficking and forced prostitution.		Filter's *porn.illicit* category would block all opportunity for sexual exploitation.
Terrorism	Material that promotes, incites, or instructs on terrorist activities, aiming to radicalise individuals or coordinate acts of terror.		Our *violence.extremism* category contains the latest URLs from the Home Office that promote terrorism, terrorist ideologies, violence or intolerance—as well as URLs added by the worldwide education community.

Inappropriate Online Content

Recognising that no filter can guarantee to be 100% effective, providers should both confirm, and describe how, their system manages the following content

Content	Explanatory notes – Content that:	Rating	Explanation
Gambling	Enables gambling		Lightspeed Filter's gambling category blocks all websites related to gambling, casinos, betting, lottery and sweepstakes.
Hate speech / Discriminiatio n	Content that expresses hate or encourages violence towards a person or group based on something such as disability, race, religion, sex, or sexual orientation. Promotes the unjust or prejudicial treatment of people with protected characteristics of the Equality Act 2010		Our *violence.hate* category contains sites that promote hostility against different groups. By leveraging AI-driven categorisation, we ensure that harmful material promoting unjust treatment is effectively restricted, fostering a safe and inclusive online environment for all students. This proactive approach not only protects students from exposure to discriminatory content but also supports educational institutions in upholding their legal obligations under the Equality Act, promoting equality and respect within the digital learning space.
Harmful content	Content that is bullying, abusive or hateful. Content which depicts or encourages serious violence or injury. Content which encourages dangerous stunts and challenges; including the ingestion, inhalation or exposure to harmful substances.		Using Lightspeed Filter schools can enable safe social media use with "read-only mode" and customisable on social media sites, block comments on YouTube with easy SmartPlay™ controls, and control app permissions using Lightspeed MDM™ to deter cyberbullying. Lightspeed Alert will detect instances of bullying and cyberbullying in real time, allowing schools to intervene before situations escalate. Trained in-house Safety Specialists will also conduct thorough reviews to assess context and severity, ensuring appropriate responses.
Malware / Hacking	promotes the compromising of systems including anonymous browsing and other filter bypass		Malware and other malicious content is blocked before it reaches the network. Our database categorises sites with

	tools as well as sites hosting malicious content		demonstrated or potential security risks into several security categories, and for extra safety, all unknown URLs can be blocked.
Mis / Dis Information	Promotes or spreads false or misleading information intended to deceive, manipulate, or harm, including content undermining trust in factual information or institutions		In addition to the education-focused and continuously updated categories integrated into Lightspeed Filter, schools have the flexibility to customise their own policies by including local or targeted websites, platforms, and individuals known for disseminating disinformation.
Piracy and copyright theft	includes illegal provision of copyrighted material		The *security.warez* category blocks all sites promoting illegal access and sharing of copyrighted and pirate material. *Forums.p2p* will also block access to all peer-to-peer and file-sharing sites that would enable plagiarism.
Pornography	displays sexual acts or explicit images		Naturally, all pornographic material in the main *porn* category is blocked. In addition, there are several other porn related categories for different languages and the *suspicious.script* category blocks javascript content frequently used for inappropriate sites such as pornography.
Self Harm and eating disorders	content that encourages, promotes, or provides instructions for self harm, eating disorders or suicide		Lightspeed Filter allows the utilisation of blocked-search key words related to self-harm and eating disorders. The *offensive* category blocks images that encourage self-mutilation and Lightspeed Alert proactively reports on any self-harm instances providing screenshots and a timeline of the events.
Violence Against Women and Girls (VAWG)	Promotes or glorifies violence, abuse, coercion, or harmful stereotypes targeting women and girls, including content that normalises gender-based violence or perpetuates misogyny.		The *violence.hate* category blocks all URLs that would encourage harm against women. All social media sites are blocked by default to discourage misogynistic content and algorithms.

This list should not be considered an exhaustive list. Please outline how the system manages this content and many other aspects

Lightspeed Systems utilises a sophisticated categorisation system, driven by both AI and a vast content database, to effectively classify websites and online content for educational purposes. This system categorises content into over 100 categories, which are continuously updated to reflect the latest online trends and threats. These categories help schools implement appropriate web filtering policies, ensuring a safe digital learning environment.

Lightspeed's safeguarding and monitoring solutions are driven by AI web crawlers, an extensive content database, and third party integrations to ensure our URLs and categories are as up to date as possible.

Regarding the duration and extent of logfile (Internet history) data retention, providers should outline their retention policy, specifically including the extent to the identification of individuals and the duration to which all data is retained.

Lightspeed Systems outlines its data retention and user identification practices in its privacy policies and trust documentation.

Data Retention Duration
Lightspeed Systems retains data for as long as necessary to fulfill the purposes for which it was collected. After the termination or deactivation of a school account, Lightspeed may retain profile information and content for a commercially reasonable time for backup, archival, or audit purposes. However, all student data associated with the school will be deleted in accordance with Lightspeed Systems' Data Deletion policy or in accordance with active Data Processing Agreements (DPA), Data Sharing Agreements (DSA), or Service Level Agreements (SLA).

In certain instances, such as compliance with legal obligations or for business continuity purposes, Lightspeed may retain data for longer periods. For example, system logs are stored for at least 12 months.

Identification of Individuals
Lightspeed Systems collects various categories of personal information that can be used to identify individuals. This includes identifiers such as real name, username, unique user ID, and other similar identifiers. Additionally, device information and connection and usage data, such as IP address, browsing activity, and search terms, are collected.
Access to this information is restricted to authorized personnel and is protected through strict administrative, technical, and physical procedures. Lightspeed Systems employs industry-standard security measures, including data encryption, firewalls, two-factor authentication, and physical-access controls, to safeguard personal information.

For more detailed information on Lightspeed Systems' data retention and privacy practices, please refer to our Privacy Policy and Trust Page here:
https://www.lightspeedsystems.com/en_uk/privacy-policy/

Providers should be clear how their system does not over block access so it does not lead to unreasonable restrictions

Using our innovative, patent-pending Smart Agent technology, Lightspeed Systems employs adaptive AI to automatically categorise millions of websites into our expanding database of 138 categories. This robust, education-focused system allows us to accurately classify web content, enabling our clients to tailor web access at a granular level, even down to individual users. This

ensures that students have the necessary access to a wide range of online resources for their learning without facing unreasonable restrictions.

Filtering System Features

How does the filtering system meet the following principles:

Principle	Rating	Explanation
• Context appropriate differentiated filtering, based on age, vulnerability and risk of harm – also includes the ability to vary filtering strength appropriate for staff		Lightspeed Filter has been designed specifically for education. It can be fully customised to perfectly match your organisational structure-tailoring policies based for different year groups, ability, location or for members of staff.
• Circumvention – the extent and ability to identify and manage technologies and techniques used to circumvent the system, specifically VPN, proxy services, DNS over HTTPS and ECH.		Lightspeed's Smart Agents filter any device, any app, any browser; and provide easy SSL decryption without proxies, PACs, or certificate hassles. Our extensive database of URL's is constantly being updated with the latest VPN's and filter bypassing tools and keeping them blocked.
• Control – has the ability and ease of use that allows schools to control the filter themselves to permit or deny access to specific content. Any changes to the filter system are logged enabling an audit trail that ensure transparency and that individuals are not able to make unilateral changes		Tiered administration across our products allows different levels of control to be permitted to different schools and users. Designated staff can add and edit keyword lists and create local allow and block lists. YouTube access can be managed by category, channel, and video. Using Lightspeed Classroom™, teachers can allow or block URLs to expand or constrict access with oversight.
• Contextual Content Filters – in addition to URL or IP based filtering, Schools should understand the extent to which (http and https) content is dynamically analysed as it is streamed to the user and blocked. This would include AI or user generated content, for example, being able to contextually analyse text and dynamically filter the content		Lightspeed Filter utilises a database system that dynamically scans page content to ensure that the page is correctly categorised. Our latest *AI – Detective* category is designed to detect the usage of AI to

produced (for example ChatGPT). For schools' strategy or policy that allows the use of AI or user generated content, understanding the technical limitations of the system, such as whether it supports real-time filtering, is important.		generate content including text analysis, images, video, and more.
● Deployment – filtering systems can be deployed in a variety (and combination) of ways (eg on device, network level, cloud, DNS). Providers should describe how their systems are deployed alongside any required configurations		Our Smart Agents sit on every device and are able to monitor all traffic and provide easy SSL decryption without proxies, PACs, or certificate hassles. For BYOD deployments, a virtual appliance easily installed on your network catches every bit of traffic the Smart Agents can't.
● Filtering Policy – the filtering provider publishes a rationale that details their approach to filtering with classification and categorisation as well as how the system addresses over blocking		There are more than a billion sites on the web, and thousands are added each hour. Your web filter needs to know them all. The adaptive AI database of Lightspeed Systems leverages AI, machine learning and the infinite cloud for the most accurate and comprehensive categorisation of the Web. This means you save time not having to re-categorise, and you can count on students staying safe without over blocking.
● Group / Multi-site Management – the ability for deployment of central policy and central oversight or dashboard		Lightspeed Filter allows tiered levels of control based on user's roles in the organisation, as well as centralised policies that work across entire schools, local authorities or multi-academy trusts.
● Identification - the filtering system should have the ability to identify users and devices to attribute access (particularly for mobile devices) and allow the application of appropriate configurations and restrictions for individual users. This would ensure safer and more personalised filtering experiences.		Lightspeed Filter can integrate with authorisation sources to gather user credentials, be configured for a captive portal or use local accounts. Lightspeed identifies users through a range of different methods including a web portal, agent

		(application) identification, and RADIUS integration.
● Mobile and App content – mobile and app content is often delivered in entirely different mechanisms from that delivered through a traditional web browser. To what extent does the filter system block inappropriate content via mobile and app technologies (beyond typical web browser delivered content). Providers should be clear about the capability of their filtering system to manage content on mobile and web apps and any configuration or component requirements to achieve this		All traffic that passes through a school or college network can be intercepted, including content via mobile and app technologies. If inappropriate apps are the issue, Lightspeed Mobile Device Management™, utilises app management to control device apps and restrictions.
● Multiple language support – the ability for the system to manage relevant languages		Our *world* categories contain websites from multiple countries that can be filtered accordingly. Flagged keywords can be added in any language to flag suspicious or concerning user activity. Further, we can enforce Google safe search, which has Google's own rules in multiple languages.
● Remote devices – with many children and staff working remotely, the ability for school owned devices to receive the same or equivalent filtering to that provided in school		Lightspeed Filter use gives schools and organisations the same level of filtering on any device and any OS remotely. Schools can also enable “after school rules” and time or location based policies to these devices to ease restrictions accordingly
● Reporting mechanism – the ability to report inappropriate content for access or blocking		We provide an extensive list of reporting and options to create customised and easily shareable reports.
● Reports – the system offers clear granular historical information on the websites users have accessed or attempted to access		Admins have immediate access to pre-installed web activity reports that may be customised by date range, school, and group.
● Safe Search – the ability to enforce ‘safe search’ when using search engines		We allow schools to force Safe Search for the entire school or individual groups.
● Safeguarding case management integration – the ability to integrate with school safeguarding and wellbeing systems to better understand context of activity		The integration of Lightspeed Filter and Lightspeed Alert with CPOMS provides a streamlined approach to safeguarding in schools.

		When Lightspeed Alert identifies a high-concern alert or imminent threat, it automatically transfers this information to CPOMS StudentSafe records. This allows safeguarding teams to manage and customise incidents alongside other records, ensuring that potential risks are addressed promptly. The seamless data synchronisation enhances the ability of schools to monitor student behaviour effectively, enabling staff to respond quickly to any concerns and maintain a comprehensive view of student safety and well-being.

How does your filtering system manage access to Generative AI technologies (e.g. ChatGPT, image generators, writing assistants)?

In your response, please describe whether and how your system identifies, categorises, or blocks Generative AI tools; how access can be controlled based on age, risk, or educational need; any limitations in filtering AI-generated content—particularly where such content is embedded within other platforms or applications; and what support or configuration guidance you offer to schools to help them align with the UK Safer Internet Centre's Appropriate Filtering Definitions and relevant national safeguarding frameworks.

Lightspeed Systems employs a sophisticated approach to identifying and categorising AI technologies. The system utilises a dynamic content categorisation engine powered by AI that proactively classifies billions of URLs before student access. Specific AI-related filtering categories, such as *Artificial Intelligence*, *AI Generative,* and *AI Detective,* have been implemented, leveraging the Smart Agent technology to ensure precise website classification of AI content. Access control is finely tuned through context-appropriate filtering based on age, vulnerability, and risk of harm. This allows for comprehensive visibility and control over digital interactions both on and off the network. Educators benefit from granular customisation capabilities, enabling web access control tailored to individual users. Additionally, Lightspeed Systems includes advanced monitoring capabilities with its AI Notify tool, which provides real-time visibility into student AI usage. This tool generates instant notifications when students navigate to AI websites, empowering educators to effectively monitor and manage AI tool usage in classroom settings. Overall, Lightspeed Systems is committed to ensuring a safe and educational environment for students while managing access to generative AI technologies and references this on various ebooks and guides on our website: https://www.lightspeedsystems.com/en_uk/

Filtering systems are only ever a tool in helping to safeguard children when online and schools have an obligation to "*consider how children may be taught about safeguarding, including online, through teaching and learning opportunities, as part of providing a broad and balanced curriculum*".[1]

Please note below opportunities to support schools (and other settings) in this regard

Digital Driver's License for Digital Citizenship: http://iDriveDigital.com Store: https://itunes.apple.com/us/app/idrivedigital/id550609295?mt=8 Google Play: https://chrome.google.com/webstore/detail/ddl/jpohacgnbefbjlgfdpeknggggppkolgdn?hl=en

[1] https://www.gov.uk/government/publications/keeping-children-safe-in-education--2

PROVIDER SELF-CERTIFICATION DECLARATION

In order that schools can be confident regarding the accuracy of the self-certification statements, the supplier confirms:

- that their self-certification responses have been fully and accurately completed by a person or persons who are competent in the relevant fields
- that they will update their self-certification responses promptly when changes to the service or its terms and conditions would result in their existing compliance statement no longer being accurate or complete
- that they will provide any additional information or clarification sought as part of the self-certification process
- that if at any time, the UK Safer Internet Centre is of the view that any element or elements of a provider's self-certification responses require independent verification, they will agree to that independent verification, supply all necessary clarification requested, meet the associated verification costs, or withdraw their self-certification submission.

Name	Brian Thomas
Position	President & CEO
Date	30th May 2025
Signature	

Telford & Wrekin IDT Managed Services

Education & Skills Funding Agency

Academy trust guide to cyber crime and cyber security

Telford and Wrekin IDT Services Response October 2022

Services for schools

www.twccommercial.co.uk

servicesforschools@telford.gov.uk

01952 380522

Contact us to discuss your requirements

Introduction

- Kirsty King - IDT Service Delivery Manager

- Presentation content provided by :

  Andy Carpendale – IDT Security Specialist

ESFA Checklist

Cyber crime: what can trusts do?

- To comply with the requirements of the Academies Financial Handbook (paragraph 4.8.1) and address the risk of fraud, theft and/or irregularity, trusts should as a minimum:
- use firewalls, antivirus software and strong passwords
- routinely back up data and restrict devices that are used to access data
- train staff to ensure that they:
  - check the sender of an email is genuine before, for example, sending payment, data or passwords
  - make direct contact with the sender (without using the reply function) where the email requests a payment
  - understand the risks of using public wifi
  - understand the risks of not following payment checks and measures

ESFA Checklist

Cyber crime: what do Telford and Wrekin IDT Services provide:

- Boundary firewall protection with internet filtering and proxy technology that protects machines from direct connectivity to the Internet.
- Antivirus protection is installed on all machines and updates every 2 hours. Any portable media is scanned when attached
- Deploy fine grained password policies which schools can use to set strong passwords, we also use a user creation toolkit so the password reset process can be delegated to the school.
- A backup solution that is hosted in the IDT Services datacentre. Backups run every morning and evening, with the SIMS database every 4 hours. Retention period is currently 90 days.
- As part of our investment in office365, multifactor authentication is available to provide extra security around logins into the office365 service.

ESFA Checklist

Cyber crime: what do Telford and Wrekin IDT Services provide:

- Regular email reminders about SPAM and Phishing Attacks and what you should do guidance.
- We can provide specific training on request.
  - Schools and Trusts procure Audit and Scrutiny advise though a number of different suppliers and we can support this.

ESFA Checklist – 5 Strategic Questions

1. Information Held

Does the trust have a clear and common understanding of the range of information assets it holds and those that are critical to the business?

We are able to help assist with audits.

ESFA Checklist – 5 Strategic Questions

2. Threats

Does the trust have a clear understanding of cyber threats and vulnerabilities?

Are you aware? Risks of sharing data over personal accounts, storage of any data, password security?

National Cyber Security Centre – Board Toolkit
Resources designed to encourage essential cyber security discussions between the Board and their technical experts.

https://www.ncsc.gov.uk/collection/board-toolkit

ESFA Checklist – 5 Strategic Questions

3. Risk management

Is the trust proactively managing cyber risks as an integrated facet of broader risk management including scrutiny of security policies, technical activity, user education and testing and monitoring regimes against an agreed risk appetite?

Automated internal vulnerability assessments are completed on a weekly basis and externally on a bi-monthly basis by an approved 3rd party.

Logging of privileged user activity, permission changes and access.

User awareness training around security themes is available on request

ESFA Checklist – 5 Strategic Questions

4. Aspects of risk

Does the trust have a balanced approach to managing cyber risk that considers people (culture, behaviours and skills), process, technology and governance to ensure a flexible and resilient cyber security response?

We maintain an IDT Risk Register which feeds into the Council's corporate risk register where the risk score is deemed as high.

Solutions and services will be risk managed as part of the project delivery mechanism or as part of the procurement process.

We report to a quarterly Governance Board chaired by Head Teachers on performance and any Cyber Security concerns.

ESFA Checklist – 5 Strategic Questions

5. Governance oversight

Does the trust have sound governance processes in place to ensure that actions to mitigate threats and maximise opportunities in the cyber environment are effective?

Report to a quarterly Governance Board chaired by Head Teachers on performance and any Cyber Security concerns.

Operate a change management board weekly.

Representation on the Council Security Group.

ESFA Checklist – 10 Steps

1. Home and mobile working

- A secure baseline build which can include encryption is applied to all equipment, delivered as part of our deployment process and this is the same deployment method for monthly security patches.
- We provide data in transit security as part of the remote access solution, Schools can also request bit locker for devices for data at rest protection as part of our bit locker encryption offering. Email encryption is also available.

ESFA Checklist – 10 Steps

2. User education and awareness

- User awareness training around security themes is available on request.
- Regular email reminders about SPAM and Phishing Attacks and what you should do.
- Issues and incidents can be reported via the IDT Self Service or if this is a priority 1 incident via Telephone (where appropriate)

ESFA Checklist – 10 Steps

3. Incident management

- We use ITIL Incident and Problem Management processes, in a major incident we will invoke an Emergency Response Team which will link into the council resilience team as appropriate.
- Disaster recovery capability through backup solution.
- IDT Services will work with or report to Schools SMT, Council Audit, internal Human Resources departments and law enforcement when required to do so.

ESFA Checklist – 10 Steps

4. Information risk management regime

- Update an IDT Risk Register which feeds into the Council's corporate risk register where the risk score is deemed as high.
- We will report risks to Head Teachers within schools and to the Governance Board.
- IDT have membership of the National Cyber Security Centre's Cyber Information Sharing

ESFA Checklist – 10 Steps

partnership to discuss and to gather intelligence relating to cyber security threats.

ESFA Checklist – 10 Steps

5. Managing user privileges

- Provide a user management toolkit for key staff within school and reporting is also available on request.
- Privileged accounts are monitored and restricted to permitted personnel only.
- Monitor and control access to log data, IDT use log analytical technology to monitor for unusual behaviour.

ESFA Checklist – 10 Steps

6. Removable media controls

- Provide an endpoint/device antivirus solution to enable staff to scan removable media.

ESFA Checklist – 10 Steps

7. Monitoring

- We have monitoring solutions and capabilities in place across our systems and networks. Ranging from reliability monitoring to threat monitoring allowing the ability to detect unusual activity.
- We use a product called Senso to enable schools to monitor usage. Designed with the UK Government Prevent duty, UK Safer Internet Centre, the UK Department for Education's Keeping Children Safe in Education (KCSiE) guidance and with keyword and URL lists from the Internet Watch Foundation(IWF) aids schools in fulfilling their legal duty of care around online safety and safeguarding.

ESFA Checklist – 10 Steps

8. Secure configuration

- Can assist with completion of a system inventory which will list the information on machines that you have joined to your network.
- Provide a secure defined baseline build which is delivered as part of a deployment process, this is the same deployment method for monthly security patches.
- Complete monthly patching in line with the IDT Services Patch Management Policy.

ESFA Checklist – 10 Steps

9. Malware protection

- Provide antivirus and anti-malware protection on endpoints/devices, email and internet filtering, with a combination of on access and scheduled scanning in place.
- Restrictions are in place for staff and students to prevent unauthorised software installations.

ESFA Checklist – 10 Steps

10. Network security

- Manage the network perimeter including boundary or client side Firewalls.
- We manage and control access to our own datacentres, IDT can assist in reporting on high risk assets on request.
- Complete automated internal vulnerability assessments on a weekly basis and external testing is completed on a bi-monthly basis by an approved 3rd party.

Telford & Wrekin IDT Managed Services

Education & Skills Funding Agency

Keeping Children Safe in Education Filtering and Monitoring

Telford and Wrekin IDT Services Response
October 2022

Services for schools

www.twccommercial.co.uk

servicesforschools@telford.gov.uk

01952 380522

Contact us to discuss your requirements

Filtering and Monitoring

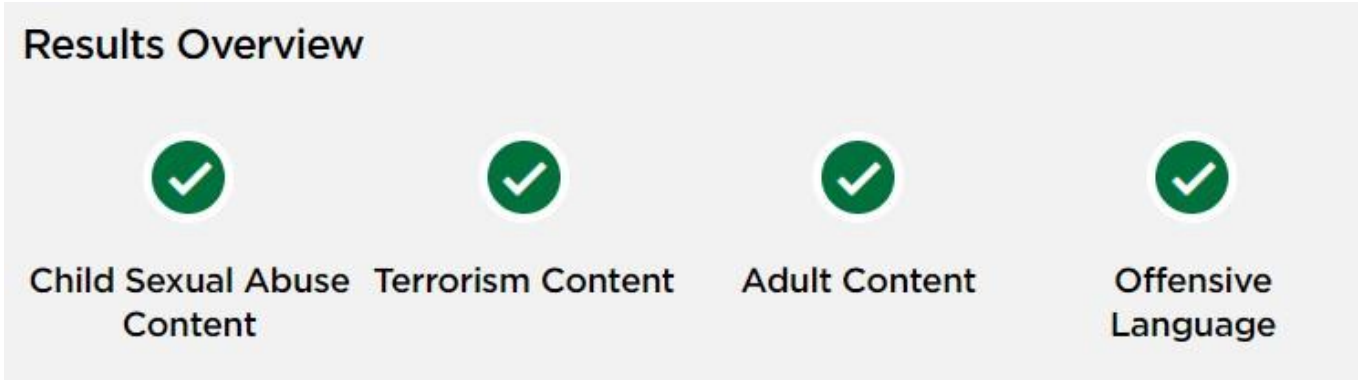
- Whilst considering their responsibility to safeguard and promote the welfare of children and provide them with a safe environment in which to learn, governing bodies and proprietors should be doing all that they reasonably can to limit children's exposure to the above risks from the school's or college's IT system.
- As part of this process, governing bodies and proprietors should ensure their school or college has appropriate filtering and monitoring systems in place and regularly review their effectiveness

How do IDT meet this requirement?

- Internet Filtering Provision: Smoothwall

  – This blocks access to any of the material listed below

- Using the DfE recommended testing site by SWGfL here are the results:-



How do IDT meet this requirement?

Child Sexual Abuse Content

Blocked

Description
Tests whether you are blocking websites on the IWF Child Abuse Content URL list.

Results & Recommendations
It appears that your filtering solution includes the IWF URL Filter list, blocking access to Child Sexual Abuse content online

Terrorism Content

Blocked

Description
Tests whether you are blocking websites on the Counter-Terrorism Internet Referral Unit list (CTIRU).

Results & Recommendations
It appears that your filtering solution includes the Counter-Terrorism Internet Referral Unit (CTIRU) URL filter list, blocking access to unlawful terrorist content online

Adult Content

Blocked

Description
Test whether your Internet filter blocks access to pornography websites

Results & Recommendations
It appears that your filtering solution includes blocking for online pornography

Offensive Language

Blocked

Description
Accesses a page containing offensive language to test if your filtering software blocks it

Results & Recommendations
It appears that your filtering solution includes blocking for offensive language

UK Safer Internet Checklist

Illegal Online Content

Aspect	Rating	Explanation
Are IWF members		Yes, Smoothwall is a member of the Internet Watch Foundation and implements the IWF CAIC list
and block access to illegal Child Abuse Images(by actively implementing the IWF URL list)		Smoothwall implements the IWF CAIC list of domains and URLs. Smoothwall Filter also uses a number of search terms and phrases provided by IWF and their members. We perform self certification tests daily to ensure that IWF content is always blocked through a Smoothwall Filter
Integrate the 'the police assessed list of unlawful terrorist content, produced on behalf of the Home Office'		Smoothwall Filter implements the police assessed list of unlawful terrorist content, produced on behalf of the Home Office

UK Safer Internet Checklist

Inappropriate Online Content

Aspect	Explanatory notes – Content that:	Rating	Explanation
Discrimination	Promotes the unjust or prejudicial treatment of people on the grounds of race, religion, age, or sex.		The 'Intolerance' category covers any sites which promote racial hatred, homophobia or persecution of minorities. Sites which advocate violence against these groups are also covered by the Violence category.
Drugs / Substance abuse	Displays or promotes the illegal use of drugs or substances		The Drugs category covers the sale, manufacture, promotion or use of recreational drugs as well as abuse of prescription drugs. Sites which provide resources which aim to help those suffering from substance abuse are covered by the 'Medical Information' category. Sites which discuss Alcohol or Tobacco are covered by the 'Alcohol and Tobacco' category.
Extremism	Promotes terrorism and terrorist ideologies, violence or intolerance		The 'Terrorism' category contains the 'police assessed list of unlawful terrorist content'. Smoothwall also provides both a 'Violence' category which covers violence against both animals or people; An 'Intolerance' category (covered further above) and a 'Gore' category which covers any sites which describe or display gory images and video.
Malware / Hacking	Promotes the compromising of systems including anonymous browsing and other filter bypass tools as well as sites hosting malicious content		As well as providing a level of protection against externally created malware, Smoothwall Filter provides a Hacking category which includes sites such as "how to" on hacking, and sites encouraging malicious computer use. Filter bypass tools are covered separately in a comprehensive "web proxies" category, which uses a combination of domain lists and dynamic content analysis.

UK Safer Internet Checklist

Inappropriate Online Content

Aspect	Explanatory notes – Content that:	Rating	Explanation
Piracy and copyright theft	Includes illegal provision of copyrighted material		The 'Piracy and Copyright Infringement' category contains sites which illegally provide copyright material or provide peer-to-peer software.
Self Harm	Promotes or displays deliberate self harm (including suicide and eating disorders)		The 'Self Harm' category contains sites relating to self-harm ,suicide and eating disorders. The category excludes sites which aim to provide medical or charitable assistance which are categorised as 'Medical Information' or 'Charity and Non-Profit' respectively
Violence	Displays or promotes the use of physical force intended to hurt or kill		The 'Violence' category contains sites which advocate violence against people and animals. We also provide a 'Gore' category which contains images and video of gory content
Pornography	Display ssexual acts or explicit images		The 'Pornography' category contains sites containing pornographic images, videos and text. Sites which contain mild nudity for purposes other than sexual arousal are covered by the 'Non-Pornographic Nudity' category. The 'Pornography' category uses both a list of domains/URLs as well as dynamic content rules which ensure new, previously unseen sites can be identified on the fly.

Multiple language support – the ability for the system to manage relevant languages		Smoothwall's combined blocklist include words in a wide variety of languages, focussed on those spoken in UK and US schools. This includes Polish and Spanish as well as "non latin" such as Urdu and Russian.

How to IDT meet this requirement?

- Classroom Monitoring Provision: Senso

senso.
Classroom Management Software

  - More than 99% active web coverage and accuracy Web traffic from 600+ million end users globally. Over 200 languages supported Daily and real-time updates. Senso's filter cloud not only benefits from extensive category-based libraries to block inappropriate websites, but also uses Artificial Intelligence to check the content of every website a student attempts to visit and will proactively include any inappropriate websites within the filtering libraries

UK Safer Internet Checklist

Illegal Online Content

Aspect	Rating	Explanation
Are IWF members		Senso® is a member of the IWF and actively communicate with them.
and block access to illegal Child Abuse Images(by actively implementing the IWF URL list)		IWF Lists are provided updated within Senso via an API
Integrate the 'the police assessed list of unlawful terrorist content, produced on behalf of the Home Office'		CTIRU URL Lists are provided and updated in real time within Senso via an API

UK Safer Internet Checklist

Inappropriate Online Content

Aspect	Explanatory notes – Content that:	Rating	Explanation
Discrimination	Promotes the unjust or prejudicial treatment of people on the grounds of race, religion, age, or sex.		Discrimination Category is one of 500 + unique content categories, and includes daily and real-time updates, as well as ActiveWeb traffic from over 600+ million end users globally with 99% ActiveWeb Coverage and Accuracy
Drugs / Substance abuse	Displays or promotes the illegal use of drugs or substances		Several categories combine to cover Drugs & Substance Abuse Categories as above
Extremism	Promotes terrorism and terrorist ideologies, violence or intolerance		Extremism category as above plus Daily updates of the CTIRU URL lists
Malware / Hacking	Promotes the compromising of systems including anonymous browsing and other filter bypass tools as well as sites hosting malicious content		Yes – covered within Malicious Internet Activity Category
Pornography	Display ssexual acts or explicit images		Adult Content Category included as above
Piracy and copyright theft	Includes illegal provision of copyrighted material		Covered within Criminal Activity / Piracy Category
Self Harm	Promotes or displays deliberate self harm (including suicide and eating disorders)		Self Harm Category included as above
Violence	Displays or promotes the use of physical force intended to hurt or kill		Weapons / Violence category included as above

How to IDT meet this requirement?

- Senso Safeguard Cloud :
- Cloud based, real time monitoring of activity on school owned devices, designed to highlight to school staff users who may be vulnerable or at risk to themselves, at risk to others or behaving inappropriately. Senso indicates a potential concern by raising a "violation" when a keyword, acronym or phrase typed, matches against those found within our libraries.
- The violation information including a screenshot can then be viewed in the dashboard by the relevant Senso Safeguarding Portal User. The screenshot will also be analysed by our AI driven image analysis to indicate whether a student is potentially viewing harmful or inappropriate content alongside the keyword typed. This helps with prioritisation of Senso violations.
- Integrates with CPOMS & Myconcern - If your school would like this integration please log a call on the IDT portal or speak to your IDT Gold Technician.