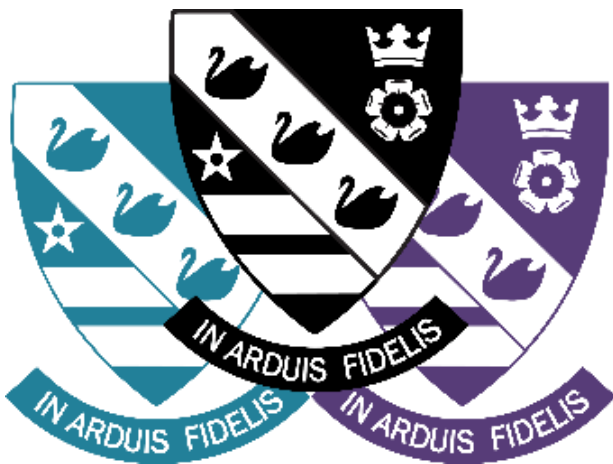


SELBY HIGH SCHOOL

SPECIALIST SCHOOL FOR THE ARTS AND SCIENCE



2026 Online Safety Policy

Ratified by the Board of Governors

Date September, 26

Signed Andy Reed

Chairperson Andy Reed

Review Date: September, 27

Learning today,
leading tomorrow

Aspiration
for all

A caring school at the
heart of the
community

Contents

Contents	2
Introduction	3
The Four Cs	4
Roles and Responsibilities	4
Governors	4
The Principal and SLT	4
Designated Safeguarding Lead with the ICT Manager:	5
The Digital Learning Steering Group	5
ICT Manager / Technical Staff:	5
Cyber Security	5
Information Security, Filters, Access and Monitoring	6
1. Introduction and Statutory Compliance	6
2. Roles and Clear Accountabilities	6
3. The Filtering Standard (Smoothwall Filter)	6
4. The Monitoring Standard (Smoothwall Monitor)	7
5. Mobile Devices and Off-Site Protections	7
6. Annual Effectiveness & Out-of-Cycle Reviews	7
Cyberbullying	7
Safe Use of Photographs and Videos of members of the school community	7
Use, storage and sharing of videos and photographs	8
Informed Consent	8
Low-risk publishing choices	8
Using photographs of individual children	8
Staff awareness and training	9
Complaints of Misuse of Photographs or Video:	9
Social Networking, Social Media and Personal Publishing:	9
Learning to Evaluate Internet Content	10
Managing Emerging Technologies	11
Review of online safety policy	11

Selby High School recognises that online, there are excellent tools for learning and communication that can be used in school to enhance the curriculum, challenge students, and support creativity and independence. Equally and increasingly, online tools can be used by staff in a vast variety of ways, including to reduce workload.

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 develop good online practices. 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.

Online safety covers ICT use, AI and 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, through webcam filming, photography or virtual meetings. There is a 'duty of care' for any persons working with children; educating all members of the school community on the risks and responsibilities of online safety falls under this duty. This online safety policy also deals with how to protect members of the school community from any form of online abuse, including through use of photographs by the school.

In the last couple of years there has been an exponential growth in the use of Artificial Intelligence, and AI can be used in ways that add extra layers of complexity to online safety. Currently, Selby High School has a separate AI Policy, which is being updated every 6 months. The links between the Online Safety Policy and the AI Policy will be kept under review.

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- but safeguarding of young people always comes first. This policy aims to be an aid in regulating ICT activity in school and provide a good understanding of appropriate ICT, so that members of the school community can use it as a reference for their conduct online outside of school hours. Online safety is a whole-school issue and responsibility.

This policy should be read in conjunction with the following policies for further clarity:

- AI Policy
- Safeguarding and Child Protection
- Mobile Phone Policy
- Anti-Bullying
- Positive Relational Behaviour Policy
- Staff Code of Conduct
- Information Security Policy and Acceptable Use Policy.
- Values Curriculum
- Data Protection Policy

Governing bodies and proprietors should ensure online safety is a running and interrelated theme whilst devising and implementing their whole school or college approach to safeguarding and

related policies and procedures. This will include considering how online safety is reflected as required in all relevant policies and considering online safety whilst planning the curriculum, any teacher training, the role and responsibilities of the designated safeguarding lead (and deputies) and any parental engagement.

The Four Cs

Keeping Children Safe in Education categorises online issues into 4 areas of risk.

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

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

Conduct: online behaviour that increases the likelihood of, or causes, harm; for example, making, sending and receiving explicit images, including those generated using AI and online bullying, and

Commerce: risks such as online gambling, inappropriate advertising, phishing and or financial scams. If you feel any students or staff are at risk, please report it to the Anti-Phishing Working Group (<https://apwg.org/>).

At Selby High School, we keep these in mind as we are planning for online safety, including curriculum planning and staff training.

Roles and Responsibilities

The designated member of the governing body responsible for online safety is Andy Reed.

Governors

Governors are responsible for the approval of the online safety policy and for reviewing the effectiveness of the policy by reviewing online incidents and monitoring reports. Online safety falls within the remit of the governor responsible for Safeguarding. The role of the online safety governor will include:

- ensure an online safety policy is in place, reviewed every year and/or in response to an incident and is available to all stakeholders.
- ensure that the school's designated safeguarding lead pays due attention to online safety and has been trained to a higher level of knowledge which is relevant to the school, up to date and progressive.
- ensure that procedures for the safe use of ICT and the Internet are in place and adhered to, including the school's systems for filtering and monitoring appropriate use of the internet through the Smoothwall system. As set out in Keeping Children Safe in Education, the

designated member of the governing body will regularly review the effectiveness of web filtering and monitoring systems.

- hold the principal and staff accountable for online safety.

The Principal and SLT

The principal has a duty of care for ensuring the safety (including online safety) of members of the school community, though the day-to-day responsibility for online safety will be delegated to the designated safeguarding lead. Any complaint about staff misuse must be referred to the designated safeguarding lead at the school or, in the case of a serious complaint, to the principal.

- Ensure access to induction and training in online safety practices for all users.
- Ensure all staff receive regular, up to date training.
- Ensure appropriate action is taken in all cases of misuse.
- Ensure that Internet filtering methods are appropriate, effective and reasonable.
- Work in partnership with the DfE, the Internet Service Provider and school ICT Manager to ensure systems to protect students are appropriate and managed correctly.
- Ensure the school ICT system is reviewed regularly regarding security and that virus protection is installed and updated regularly.
- The Senior Leadership Team will receive monitoring reports from the designated safeguarding lead.

Designated Safeguarding Lead with the ICT Manager:

- Work in partnership with the DfE and the Internet Service Provider and school ICT Manager to ensure systems to protect students are reviewed and improved.
- Ensure the school ICT system is reviewed regularly with regard to security and that virus protection is installed and updated regularly.
- Receives reports of online safety incidents and creates a log of incidents to inform future online safety developments.
- Reports to the Senior Leadership Team.
- Liaise with the nominated member of the governing body & principal, providing an annual update to governors on online safety.

The Digital Learning Steering Group

- Ensure the effective delivery of the Digital Learning Strategy, including embedding online safety, which is the first aim of the strategy.

ICT Manager / Technical Staff:

The ICT Manager is responsible for ensuring:

- That the school's technical infrastructure is secure and is not open to misuse or malicious attack.
- That the school meets required online safety technical requirements and any relevant body online safety policy / guidance that may apply.
- That users may only access the networks and devices through a properly enforced password protection policy.
- The filtering policy is applied and updated on a regular basis and its implementation is not the sole responsibility of any single person.

- That they keep up to date with online safety technical information to effectively carry out their online safety role and to inform and update others as relevant.
- That the use of the network, internet, Virtual Learning Environment, remote access and email is regularly monitored in order that any misuse or attempted misuse can be reported to the designated safeguarding lead or principal for investigation.
- That monitoring software systems are implemented and updated as agreed in school policies.

Cyber Security

Governing bodies and proprietors should take measures to safeguard children by protecting personal information and ensuring their school or college has appropriate cyber security systems in place. This should be approached as part of the school or college's wider safeguarding responsibilities. As part of this, Selby High School will implement measures in line with the [Cyber security standards for schools and colleges](#).

In addition, all Selby High School staff undertake Cyber Security training on an annual basis.

Information Security, Filters, Access and Monitoring

1. Introduction and Statutory Compliance

Selby High School provides a safe online environment to ensure students can learn safely and productively. This section meets all requirements of the Department for Education's (DfE) [Filtering and Monitoring Standards for Schools](#) and [Keeping Children Safe in Education (KCSIE) 2026].

The school uses [Smoothwall](#) as its unified web filtering and proactive digital monitoring platform.

2. Roles and Clear Accountabilities

Safeguarding online is a leadership and child protection priority, not just an IT task. The school maintains clear lines of governance and responsibility:

- Governing Body: Ensures appropriate, non-bypassable systems are active and guarantees that the annual effectiveness review takes place and is officially recorded.
- Senior Leadership Team (SLT) Named Lead: Tom Sergeant holds ultimate operational accountability for reviewing system effectiveness.
- Designated Safeguarding Lead (DSL): manages the day-to-day safeguarding triggers, leads the contextual review of alerts, and informs governors of system efficacy.
- IT Support / Network Team: Manages technical configurations, carries out system tests, and responds immediately to hardware/software issues.

3. The Filtering Standard (Smoothwall Filter)

Our web filter blocks harmful or illegal content without excessively restricting educational access.

- **Scope:** Filtering applies to all internet-connected devices across the school network, including managed school laptops, tablets, and desktop computers.
- **Illegal Content Blocking:** Smoothwall enforces non-bypassable blocklists for Child Sexual Abuse Material (via the Internet Watch Foundation) and terrorist content (via the Counter-Terrorism Internet Referral Unit). These lists cannot be disabled by school administrators.
- **Advanced Real-Time & AI Filtering:** The system uses **dynamic, real-time analysis** to filter user-generated text and harmful **AI-generated content** (including deepfakes and text-based generative AI outputs), moving beyond static URL blocklists.
- **Categorisation:** Content is restricted across the DfE "Four Cs" risks (Content, Contact, Conduct, Commerce), specifically blocking material related to:
 - Radicalisation and extremism
 - Pornography and harmful sexual behaviour
 - Self-harm, suicide, and severe mental health crises
 - Misogyny, extreme online harassment, and weapon-related violence
 - Disinformation, misinformation, and online conspiracy theories

4. The Monitoring Standard (Smoothwall Monitor)

Filtering alone is insufficient. Active monitoring identifies children exhibiting concerning online behaviours or vulnerabilities.

- **Proactive Digital Capture:** Smoothwall proactively logs keystrokes, searches, and screen interactions across all school devices.
- **Contextual Alerts:** The monitoring system captures screenshots and text context to provide a clear timeline of events for the safeguarding team.
- **Triage & Interventions:** Alerts are categorised by risk severity. High-risk alerts (e.g., immediate threat to life, severe self-harm, or radicalisation) trigger daily notifications to the DSL team for intervention.
- **User Identification:** Where possible, and in most occasions, the system resolves data directly to the individual logged-in user account, enabling targeted safeguarding actions.
- **Follow-up:** After an alert is received action will be taken by the DSL or one of the DDSs, and recorded appropriately, (for example on CPOMs or the Low Level Concern log).

5. Mobile Devices and Off-Site Protections

- **Mobile-Free Environment:** In compliance with national defaults, Selby High School operates as a **mobile phone-free environment** during the school day. Personal devices must not access school learning platforms via unmonitored means.
- **Off-Site Devices:** School-managed devices loaned to pupils for remote learning or homework are equipped with **Smoothwall Cloud** clients. This ensures the same level of filtering and monitoring applies at home as it does on the school campus.

6. Annual Effectiveness & Out-of-Cycle Reviews

- **Mandatory Annual Review:** At least once every term, the assigned SLT member—supported by the DSL and IT support—will audit the system using the DfE’s self-assessment framework. A formal written log of this review must be retained for compliance audits.
- **Testing Routine:** IT support carries out regular, recorded physical checks across all campus locations to ensure Smoothwall cannot be bypassed (e.g., via unauthorized VPNs).
- **Out-of-Cycle Review Triggers:** The filtering and monitoring setup will be immediately re-reviewed outside of the annual window if the school introduces new generative AI tools, identifies a system bypass method, or updates its physical IT infrastructure.

Cyberbullying

The school, as with any other form of bullying, takes Cyber bullying very seriously. Information about specific strategies or programmes in place to prevent and tackle bullying is set out in **the school anti-bullying 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.

Safe Use of Photographs and Videos of members of the school community

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.

Any image shared publicly can be copied, altered, or reused without a school’s knowledge or consent. Advances in technology mean that images of children may be manipulated, including through artificial intelligence, and reused in harmful or misleading ways. Safeguarding responsibilities and data protection duties apply just as much to online images as they do to face-to-face practice.

The following policy guidance has been developed following guidance from the [UK Safer Internet Centre](#).

Use, storage and sharing of videos and photographs

Any photographs or videos taken of students or staff during activities must be removed from the camera as soon as possible, and stored securely on the shared google drive file. The file should be saved as NAMEOFACTIVITY followed by DATE- eg PROM26062026.

Photographs and videos of students must never be recorded or saved on staff’s personal equipment. Photographs and videos that are going to be viewable by students and parents, for example Prom photographs, or photographs from school visits, must be placed on Ready, Steady, Learn. Only students and registered parents and carers will have access to these folders.

Informed Consent

Parents and carers will be clearly informed about how images may be used. Whenever a pupil begins their attendance at the school they, or their parent, where appropriate, will be asked to complete a consent form in relation to the use of images and videos of that pupil. We will not use images or videos of pupils for any purpose where we do not have consent.

We respect student data privacy and comply with UK GDPR by operating a dual-consent model for the use of student photographs and videos. For students under the age of 13, explicit written consent is obtained from parents or carers. **For students aged 13 to 16, we require informed consent from both the parent/carers and the student** before any identifiable images are used or published. Consent is captured at enrolment, reviewed annually, and can be withdrawn at any time by either the student or their guardian. We never publish student photographs alongside their full names on our website, social media, or marketing materials.

Low-risk publishing choices

Where images are shared publicly, for example in the prospectus, the newsletter or on the website, Selby High School will minimise risk by:

- Using group photos rather than close-ups
- Removing images that are no longer needed
- Applying a consistent “Images-no-names / Names-no-images” approach on public platforms
- Technical protections- Where appropriate, taking practical steps such as reducing image quality, removing hidden metadata (EXIF data)

Please note, we will not publish photographs of students on our social media platforms, without explicit consent from both parents/carers and students.

Using photographs of individual children

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.

- Parents and others attending school events cannot take videos or photographs of students during school performance.
- The school asks that parents and others do not post any images or videos which include any child other than their own child on any social media or otherwise publish those images or videos.
- As a school we want to celebrate the achievements of our pupils and therefore may want to use images and videos of our pupils within promotional materials, or for publication in the media such as local, or even national, newspapers covering school events or achievements. We will seek the consent of pupils, and their parents where appropriate, before allowing the use of images or videos of pupils for such purposes.

Staff awareness and training

Staff training will ensure that staff understand why image misuse is a safeguarding concern and know how to follow school procedures, including when using personal devices or school social media accounts.

For more information please refer to our data protection policy.

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 school's child protection and safeguarding policy and behaviour policy.

Social Networking, Social Media and Personal Publishing:

Personal publishing tools include blogs, wikis, social networking sites, bulletin boards, chat rooms and instant messaging. These online forums are the more obvious sources of inappropriate and harmful behaviour and where pupils are potentially more vulnerable to content, contact and conduct behavioural issues. It is important that we educate pupils 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, unless it is for a specific purpose within a lesson.

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 Computing curriculum and Life Development 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 always representing the school and must act appropriately.
- Safe and professional behaviour of staff online will be discussed at staff induction, and is clearly outlined in the staff Code of Conduct..

Curriculum Content

The school's curriculum ensures that preemptive education is in place to advise students so that they are aware of potential online dangers and how to navigate these. This is currently covered in the following curriculum lessons (please note that the nature of this subject means that curriculum plans are adapted to meet local need regularly):

	Life Development	Computer Science
Year 7	○ Online Safety & Sexting. ○ Cyberbullying. ○ Radicalisation & Extremism.	○ Respectful online communication. ○ Digital footprints. ○ How to access support if something has gone wrong.
Year 8	○ Cyberbullying. ○ Online Safety.	○ Online reputation. ○ Fake news. ○ Internet bubble.
Year 9	○ Sexting. ○ Consent and Pressure. ○ Mobile Phone addiction.	○ Social engineering. ○ Hacking. ○ Viruses & Malware, including methods of defence.
Year 10	○ Online effects on self-esteem and confidence. ○ Radicalisation, including Fake News. ○ Online reputation. ○ Online grooming.	
Year 11	○ Grooming. ○ Gambling. ○ Pornography.	

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. Students will be taught to:

- Be critically aware of materials they read, and shown how to validate information before accepting it as accurate
- Use age-appropriate tools to search for information online
- Acknowledge the source of information used and to respect copyright. Plagiarism is against the law and the school will take any intentional acts of plagiarism 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's ICT Manager. 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.

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.

Review of online safety policy

Reviewing online safety Technology, and risks and harms related to it, evolve, and change rapidly.

Selby High School will carry out an annual review of the approach to online safety, supported by an annual risk assessment that considers and reflects the risks their children face. A free online safety self-review tool for schools can be found via the [360 safe website](#) or [LGfL online safety audit](#).

This policy will be reviewed at least annually.