St Louis Grammar School Online Safety and Acceptable Use Policy

2026-27

Date of Policy: September 2026

Last Reviewed: September 2025

Reviewed by: Mr T Brown

Date of Review: September 2027

St Louis Grammar School Comprehensive Online Safety, Acceptable Use, and Digital Media Policy

NOTE: This Policy replaces the separate Acceptable Use and e-Safety policies

(Applicable to Staff, Pupils, Parents/Carers, Governors, Volunteers, and Visitors)

I. Introduction, Vision, and Core Principles

1.1 Policy Statement and Vision St Louis Grammar School is committed to providing a secure and supportive environment for all members of our community when engaging in the online world. Our vision, aligned with the Northern Ireland Executive Online Safety Strategy, is that **all children and young people enjoy the educational, social and economic benefits of the online world, and that they are empowered to do this safely, knowledgeably and without fear**. We recognise that online and offline lives are integrated, and that issues arising online can significantly impact pupil attendance, well-being, and school reputation.

In all matters relating to safeguarding and child protection, including online safety, the best interests of the child must be the paramount consideration.

1.2 Scope and Definitions This policy applies to all engagement in the online world, focusing on activities and behaviours rather than solely the device used. This includes access to all school-provided Information and Communication Technology (ICT) resources (network, hardware, software, email, virtual learning environments (Google Classroom), and personal devices (Bring Your Own Device) when used on school premises or when their use impacts on the school community.

Online risks are broadly categorised into four areas of risk:

1. **Content:** Being exposed to illegal, inappropriate, or harmful material (e.g., pornography, hate speech, self-harm promotion).
2. **Contact:** Being subjected to harmful online interaction with other users (e.g., grooming, peer pressure, exploitation).
3. **Conduct:** Online behaviour that increases the likelihood of, or causes, harm (e.g., sharing nudes, cyberbullying).
4. **Commerce:** Risks involving scams, fraud, or hidden costs (e.g., online gambling, in-app purchases).

1.3 Aims and Objectives The purpose of this combined policy is to:

- Ensure the protection, safety, and well-being of pupils when accessing the internet within our premises or using digital devices to engage with the school, its activities, or events.
- Educate and empower pupils to make informed choices and develop **digital resilience** so they can effectively manage and respond to harmful online experiences.
- Provide clear guidelines for all users (staff, pupils, parents) regarding acceptable and unacceptable use of digital technologies and social media.

- Ensure the school operates in line with our core values and within Northern Ireland law and Department of Education (DE) guidance, such as the *Co-operating to Safeguard Children and Young People in Northern Ireland*.

II. Roles, Responsibilities, and Education

2.1 Staff Responsibilities All staff (teaching and non-teaching) must understand that **online safety is a core part of safeguarding**. Staff must ensure they:

- Read, understand, and sign the staff acceptable use agreement.
- **Immediately report** any suspected misuse of technology or online safeguarding concern to the Designated Teacher (DT) or Deputy Designated Teachers (DDT) in line with school safeguarding procedures.
- Ensure all digital communications with pupils or parents/carers are professional and conducted using **official school systems** (such as school email or approved learning platforms). Personal email addresses, text messaging, or social media must not be used for these professional communications.
- Do not communicate with, 'friend,' or 'follow' current or prior pupils using **personal social media accounts**.
- Maintain the same professional boundaries online as they would in person, ensuring personal online activity does not damage the school's reputation or breach confidentiality.
- Model safe, responsible, and professional online behaviours in their use of technology, including social media outside of school.
- Avoid using personal equipment to take photographs or videos of children, opting only for school-owned devices for educational purposes.

2.2 Designated Teacher (DT)/ Deputy Designated Teacher (DDT) Responsibilities The DT has **lead responsibility for safeguarding and child protection, including online safety**. The DT/DDT will act as the primary point of contact for staff concerning online safety issues and ensure incidents are logged.

2.3 Pupil Responsibilities (Acceptable Use) Pupils must adhere to this policy and the Pupil Acceptable Use Agreement. Pupils must:

- Use school ICT systems and their personal devices (when permitted) **only for educational purposes**.
- **Immediately tell a member of staff or trusted adult** if they see or experience anything unpleasant, inappropriate, or if someone asks them for personal information or images.
- Keep their usernames and passwords safe and **never share them** with anyone else. Password security must be effective, and pupils should not write down or store a password where it may be stolen.
- **Not create, browse, or access material that could be considered harmful, offensive, or illegal** (including pornography, racist, or sexist content).

- Be polite and respectful in all online communication (Netiquette) and **not engage in cyberbullying, harassment, or spreading rumours or lies about other members of the school community**.
- Understand that attempts to bypass the school's filtered systems (e.g., through proxy avoidance sites or mobile internet) are **prohibited** and constitute serious misconduct.

2.4 Parent/Carer Responsibilities Parents/carers have a key role in supporting their child to grow up safe online. Parents/carers must:

- Read and sign the Acceptable Use Agreement (Section V) and encourage their children to follow the guidelines set out for both school and personal devices.
- **Model safe, responsible, and positive online behaviours** and refrain from posting negative, threatening, or violent comments about school staff, pupils, or others on social media.
- Be aware that **additional filters and parental controls** may be necessary to support online safety at home, especially for younger children.
- Be proactive in the monitoring of their child's online activities
- Protect children's privacy online and think carefully about what content they share, where they share it, and who they are sharing it with, recognising the impact on their child's digital footprint (often referred to as 'sharenting').

2.5 Online Safety Education (The Preventative Curriculum) Online safety education is embedded within the curriculum, particularly within Personal Development and Mutual Understanding (PDMU) and Learning for Life and Work (LLW) lessons, assemblies, and the ICT curriculum.

- This education must be age-appropriate and relevant, covering topics including managing online information, understanding responsible online behaviour, recognising online risks (such as grooming, sexting, and online blackmail), and developing **digital resilience**.
- The school reinforces key messages through national initiatives such as Safer Internet Day and Anti-Bullying Week.
- The curriculum covers sensitive sexual issues, such as sexting, where pupils are taught the legal implications and other risks associated with sharing nude or semi-nude images.

III. Managing Online Risks and Incidents

3.1 Reporting Concerns and Misuse

All staff, pupils, and parents should be aware of robust reporting channels. Any suspected misuse or online safeguarding concern must be reported **immediately** to the DT/DDT or the ICT Network Manager.

3.2 Defining and Responding to Bullying and Cyberbullying

Bullying includes (but is not limited to) the repeated use of any verbal, written, or electronic communication, or any combination of these, by a pupil or a group of pupils against another pupil or group of pupils, with the intention of causing physical or emotional harm to that pupil or group of pupils.

Behaviour becomes bullying type behaviour when the following criteria are met: the behaviour is **targeted** at a specific pupil or group, it is **repeated**, it is **intentional**, and it is causing **physical, emotional, or psychological harm**.

The school may also consider single, severe, or significant incidents as bullying type behaviour, particularly when there is evidence of pre-meditation or a major impact on the individual or the wider school community.

- **Online Bullying (Cyberbullying):** Online bullying incidents that take place outside school but are likely to have a detrimental effect on a pupil's education in school may be addressed through the Anti-Bullying Policy.
- The school maintains a **zero-tolerance approach** to incidents of online bullying, sexual harassment, or discrimination. Staff must challenge inappropriate behaviour or language and not dismiss it as 'banter'.

3.3 Sharing Nudes (Sexting) Sexting is defined as the sending or posting of sexually suggestive images, including nude or semi-nude photographs, via mobiles or the internet.

- **Legality:** Pupils must be aware that it is illegal under the Sexual Offences (NI) Order 2008 to take, possess, or share 'indecent images' of anyone under 18, even if they are the person in the picture.
- **Procedure:** Staff responding to incidents should proceed sensitively, seeking to protect the child rather than criminalise them, unless severe intent to cause distress is identified.
- If an indecent image is received or possessed, staff advice is **not to delete it** and to contact the Police (101) immediately, as sharing it further may constitute an offence. The UK Safer Internet Centre (via the **Report Remove tool**) may be able to assist in removing or blocking the image to prevent further distribution.

3.4 Social Media Conduct

- **School Reputation:** If the school feels that a pupil has brought its reputation into disrepute by publishing online unsuitable comments, images, or videos about pupils or staff, or through materials posted with the aim of bullying, humiliating, or intimidating any member of the school, these matters will be investigated. As this is classed as serious misconduct, sanctions may include suspension or expulsion. All sanction decisions in this regard are the responsibility of the Principal and the Board of Governors.

- **Staff Conduct:** Staff must ensure that publicly available information about them is accurate and appropriate for viewing by a whole school audience. Inappropriate content or material that is unprofessional or that contains content which is defamatory towards the school or any of its stakeholders is a disciplinary matter and will be dealt with under the Staff Code of Conduct and related policies.

3.5 Use and Misuse of Artificial Intelligence (AI)

St Louis Grammar School recognises that Artificial Intelligence (AI) tools present significant opportunities to enhance learning, efficiency, and professional practice, supporting our core vision that all children and young people should enjoy the educational, social, and economic benefits of the online world safely and knowledgeably.

When incorporating AI into teaching, administration, or personal study, all users (staff, pupils, and parents/carers) must ensure adherence to principles of academic integrity, honesty, and professional conduct. Staff must be aware that online safety is a core part of their safeguarding responsibility, and their use of AI must strictly conform to the expected professional boundaries and the Staff Code of Conduct. It is essential that all users critically evaluate AI-generated content for accuracy and ethical soundness, acknowledging that relying solely on AI output can diminish critical thinking and intellectual ownership, especially concerning academic work.

The misuse of AI is considered a serious breach of this policy and will be treated as misconduct. For pupils, the submission of work wholly or substantially generated by AI tools and presented as their original effort constitutes academic dishonesty and undermines the principles of pupil achievement (See the Exams Policy for further guidance). For all users, AI tools must never be deployed to create, disseminate, or post any content that is abusive, discriminatory, illegal, defamatory, threatening, or harmful, including content used for cyberbullying, harassment, or the infringement of copyright. Staff, in particular, must ensure that their use of AI does not involve the input of confidential school data or personal pupil information, maintaining the strict confidentiality required of their professional position, even when conducting private activities outside school hours.

Any suspected or actual misuse of AI, including attempts at academic fraud or the generation of inappropriate material, must be reported immediately to the Designated Teacher, Deputy Designated Teacher, or the Senior Leadership and Management Team. Investigations will be conducted in line with the school's safeguarding and positive behaviour policies. Pupils found to be in breach may face disciplinary sanctions, ranging from loss of access to the school network and IT resources to suspension or expulsion in cases of serious misconduct, as determined by the Principal and the Board of Governors. Where AI misuse involves illegal materials or activity, such as generating content relating to child sexual exploitation or hate crimes, the matter will be reported immediately to the Police and the appropriate Children’s Services Gateway Team for external investigation.

IV. Management of Technology, Devices, and Digital Media

4.1 Filtering and Monitoring The school uses the Education Authority (EA)/C2K filtered Internet service. This service is essential for safeguarding and protects users and systems from abuse.

- The system uses filtering mechanisms (such as Forcepoint/Websense) to block illegal or inappropriate content, including IWF updates.
- **All online activity is tracked and recorded** using unique usernames. The Principal or designated senior staff can request Internet Usage Reports to investigate misuse.
- Monitoring systems (such as Securus) are used to detect potential breaches, including cyberbullying, self-harm language, and inappropriate content.
- Users should be aware that network administrators may review files and communications to maintain system integrity and legal compliance; a limited expectation of privacy exists on publicly-funded networks.
- Pupils must immediately advise a staff member, or any member of the Safeguarding team, if they are able to access sites that should be blocked.

4.2 Use of Mobile Phones and Personal Devices (BYOD) The use of personally owned devices (BYOD) by staff and pupils is subject to the same regulations as school-provided equipment.

- **General Use Restriction:** The personal use of pupil mobile phones and similar devices should be **restricted** during the school day for the vast majority of pupils, including during lunch and recreational periods. Phones are handed in at the start of each lesson, and returned at the end of each lesson.
- **Liability:** The school accepts **no liability** for any loss or damage to personal devices brought onto school premises. Pupils/staff are solely responsible for the care and security of their devices. We advise that high value items are not brought into school.
- **Permission:** Pupils require a fully completed and signed Bring Your Own Device Form (Pupil Declaration and Parent/Guardian Approval) to use personal devices in school and to connect to the wireless network. See the **Wireless Internet Policy** for more details.
- **Unsuitable Material:** If a teacher suspects school rules have been broken, pupils can be asked to hand over their device or to display images stored on their device. Any inappropriate content must be removed before the device is brought onto school premises. Before viewing any images advice must be sought by staff from a member of the Safeguarding team.

4.3 Photography and Filming The capturing and use of photographs/videos of pupils must adhere to safeguarding standards and require informed, written consent which is collected from Parents / Guardians / Carers when a child joins the school.

- **Consent:** Written consent is required from the pupil and their parent/carer before a child's image or video is taken and used (e.g., for publicity or school publications).
- **Identification:** Photographs published online or elsewhere that include pupils should be selected carefully, and pupils' full names will not be used anywhere in association with photographs. Identifying information (such as school logos) should be disguised

where appropriate, especially if the activity carries a heightened risk of image misuse.

- **Staff Devices:** Staff must use school equipment for taking photographs of pupils and ensure images are stored securely on monitored school systems.
- **Prohibited Areas: Personal phones or devices capable of taking photographs or recording video are NOT permitted in changing areas or toilets**. Devices must be switched off and secured in a bag or pocket in these areas. This ban applies to all users (staff, pupils, and visitors).

V. Forms for Acceptance and Consent (Parent Friendly)

1. Pupil ICT and Online Safety Acceptable Use Agreement (AUP)

St Louis Grammar School Internet, Cloud & Digital Media/Images Permission Form

Pupil Section

Name of Pupil: ________________________ Year Group/Class: _____________________

I understand that my access to the school’s technology (Internet, Cloud, email, and devices) is a privilege and not a right. I have read, understood, and agree to follow the school’s Online Safety Policy and Pupil Acceptable Use Agreement.

I understand that if I fail to comply with this agreement, I will be subject to disciplinary action, which may include losing my access to the school network.

I agree to the following terms for my safety and the safety of others:

- I will keep my username and password safe and secure and will not share it with anyone.
- I will immediately tell a member of staff or another adult if I see or experience anything unsuitable, illegal, or inappropriate online.
- I will be polite and respectful to everyone online and will not spread rumours, send mean messages, or engage in bullying behaviour.
- I will not attempt to bypass the school's internet filters using my own devices or any other methods.
- I will never share my personal information (name, address, phone number, etc.) or the personal information of others online.
- I understand that my personal phone or other device capable of taking photographs or recording video is **NOT permitted** in changing areas or toilets. I will ensure that it is switched off and securely in my bag or pocket in these areas.

Pupil Signature: ___________________________________ Date: ____________________

Parent/Guardian Section

As the parent or legal guardian of the pupil named above, I grant permission for my child to use the internet, cloud, and digital media systems provided by St Louis Grammar School.

I acknowledge that I have read and understand the school's Online Safety Policy and Acceptable Use Agreement. I understand that the school takes every reasonable precaution (including monitoring and filtering) to ensure safety, but cannot ultimately be held responsible for the nature and content of all materials accessed. I agree that my child must follow the guidelines set out for using all digital technology in relation to the school, whether they are using school devices or their own devices.

Photography and Video Consent

Please tick YES or NO below:

Permission	**I agree to the school taking and using digital/video images of my child. I understand that the images will only be used to support learning activities or in publicity that reasonably celebrates success and promotes the work of the school.**
YES	**NO**

Permission	**I confirm that I have made my child aware that a personal phone/device capable of taking photographs or recording video is NOT permitted in changing areas or toilets. I understand that anyone found with a camera device switched on in a changing area or toilet may be subject to disciplinary proceedings.**
YES	**NO**

Parent/Guardian Signature: ______________________________

Print Name: ___________________________ Date: ____________________

2. Bring Your Own Device (BYOD) User Agreement – Pupil Declaration

I request permission to use my own personal ICT device in school for educational purposes.

Device Type: ___________________________ Serial Number: _____________________

I confirm that I have read and understood the relevant sections of the school's Online Safety and Acceptable Use policies regarding personal devices. I understand that the school accepts **no liability** in respect of any loss or damage to my personal ICT device while at school or during school activities. I understand I am personally and solely responsible for the correct care, safety, and security of the device, and that all data stored on it must be free from inappropriate or illegal material.

Pupil Name: __________________________________ Class: _________

Signed: __________________________________ Date: _________

Parent/Guardian Approval for BYOD Use

I have read and understood the Pupil BYOD Declaration. I understand and accept the disclaimer regarding liability for damage or loss to the device. I give my approval for my child to use their personal ICT device in school under the terms of this policy.

Parent/Guardian Signature: ______________________ Date: ____________________

VI. Key Contacts

Role	Name	Contact Details
Designated Teacher (Safeguarding Lead)	Miss Caroline King	028 4176 2747
Deputy Designated Teacher	Mr K Martin Mr E McGlue Mr T Brown Mrs B Cunningham Mrs S Morris	028 4176 2747
ICT Network Manager	Mr T Brown	028 4176 2747
Children's Services Gateway Team (Out of Hours)		028 9504 9999
PSNI (Non-Emergency)		101
Childline (Confidential Support)		0800 1111