



E-Safety Policy 2025

St Louis Grammar School

Date of Policy:	February 2025
To be reviewed:	February 2026

J Scullion
ICT Coordinator

Contents	Page Number
Policy Rationale	3
Policy Aims	3
Roles and responsibilities	3-4
Filtering & Monitoring	4
Useful Links	5
Contact Information	5

Policy Rationale

The integration of digital technologies into education provides numerous benefits including enhanced learning opportunities and access to a wealth of resources. However, it also presents potential risks such as cyberbullying, online predators and exposure to inappropriate content. This policy is designed to mitigate these risks and ensure that technology used at St Louis Grammar School is secure, educational and aligned with our values.

DENI state; 'We all deserve to be able to use the internet to learn, explore and connect with each other. But all of us need to be aware of the risks in doing so. Our advice is:

- Don't share personal information or images with people you don't know.
- Don't accept any friend requests with someone you don't know.
- Set privacy settings on all devices so that only people you know can view your account.
- Don't post anything online that you are not happy to be shared."

Policy Aims

- To educate students, staff and parents about safe and responsibly use of digital technologies.
- To safeguard personal and sensitive information from unauthorized access and cyber threats.
- To minimise risk related to cyberbullying, online exploitation and other online dangers.
- To use technology to enhance the learning experience while ensuring that its use is appropriate and secure.

Roles and responsibilities

Governing Body

- Ensure all school personnel and stakeholders are aware of and comply with this policy.
- Ensure that St Louis Grammar School complies with related legislation.

SLT

- Ensure that this policy is implemented effectively and reviewed regularly.
- Provide the necessary resources and training to support e-safety initiatives.
- Regularly update the policy to reflect new developments in technology and best practices.

IT Coordinator/Designated E-safety coordinator

- Oversee the implementation of this policy is undertaken by all stakeholders.
- Organise and deliver e-safety training for students and staff.
- Provide guidance and support for addressing e-safety incidents and concerns.

- Keep up to date with new developments and resources

Teachers and staff

- Comply with this policy.
- Integrate e-safety into the curriculum and promote awareness of safe online practices.
- Monitor students' use of technology in school to ensure compliance with e-safety deadlines.
- Report any e-safety incidents or concerns to the Designated E-Safety Coordinator.
- Demonstrate responsible and ethical use of technology.

Students

- Use digital technologies in a responsible and respectful manner.
- Be aware of online materials and validate information before accepting its accuracy.
- Respect copyright when using the internet for research purposes.
- Follow the school guidelines and rules related to e-safety.
- Report any e-safety issues or concerns to a trusted adult.

Parents and Guardians

- Support this policy and educate children about safe online behaviour at home.
- Maintain open communication with the school regarding any e-safety concerns or incidents involving their children.
- Utilise resources provided by the school to better understand and support e-safety measures.

Filtering & Monitoring

The C2K network has a comprehensive system for filtering and monitoring to ensure safe and secure internet use within educational settings. C2K employs web filtering technologies that categorize different groups such as social media, gambling, adult content etc and block access to the same. Schools can have some level of customization to tailor filtering settings according to their specific needs. The filtering system is regularly updated to protect against new online threats and emerging content categories.

C2K monitors network traffic to identify unusual patterns or potential security threats. The network is designed to flag and respond to potential breaches or security incidents in real time.

Useful Links

[Department of Education Guidance](#)

[EA Guidance](#)



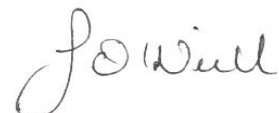

[NSPCC Guidance](#)

Contact Information

For any questions or concerns regarding this policy, please contact:

- **IT Coordinator:** J Scullion, jscullion300@c2kni.net
- **IT Support:** P Heffron, pheffron038@c2kni.net

E-Safety Policy
February 2025 – February 2026

Designated Teacher	Jane Scullion 
Signature	
Designated Governor	Alan Law
Signature	
Principal	Jacqui O'Neill
Signature	
Chairperson of Board of Governors	Mary Black
Signature	
Date	<u>24.03.25</u>