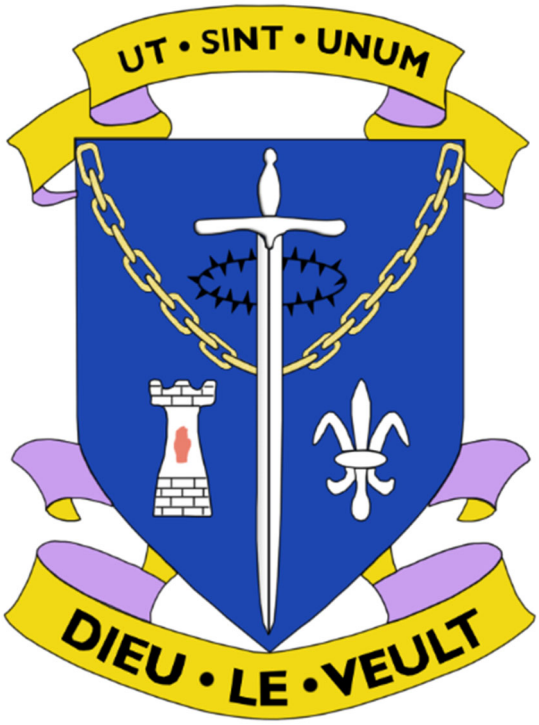
St Louis Grammar School
Kilkeel

Wireless Internet Policy



2026-27

Date of Policy: September 2026

Last Reviewed: September 2025

Reviewed by: Mr T.Brown

Date of Review: September 2027

Introduction

This Wireless Internet Policy operates within the broader context of the school's online governance framework. It has been agreed by staff and the Senior Management Team and approved by Governors. This policy should be read in conjunction with the school's **Online Safety and Acceptable Use Policy.**

Pre-Conditions for Use of the School's Wireless Network

Staff, pupils, members of the local community and Specialist Schools partners and pupils (hereafter referred to as 'Users') may use the school's wireless network for **educational purposes only**.

Users must have read and agreed to the school's **Online Safety and Acceptable Use Policy**, **St Louis Google Classroom Acceptable Use Policy**, and have signed the **St Louis Google Classroom Code of Conduct** prior to use.

In order to connect non-ENNI equipment to the school's wireless network, users must first seek permission from the Director of ICT. This permission may require the installation of additional ENNI software that allows access to the school's wireless network and printing facilities. Users are responsible for backing up all their files before installation, as the school is **not liable for any loss or damage** to user files caused unintentionally or by issues arising from incompatible software.

Conditions of Use for Compatible Devices (Bring Your Own Device - BYOD)

The use in school of devices owned personally by staff and pupils is subject to the same regulations as if they were provided by the school.

1. **Compatible Devices:** Users will only be allowed to attach Microsoft Windows® based or Apple Macintosh® laptops, Chromebooks, or other compatible devices such as iPads or tablets to access the school's wireless network.
2. **Pre-Use Checks:** Prior to use, devices must be checked by ICT staff for compatibility and staff and pupils must check for the presence of existing unsuitable material and remove this prior to connection to the schools' network.
3. **Security Software:** Devices must have an up-to-date anti-virus/internet security product installed.
4. **Sensitive Data Handling (Staff):** Staff must **not** store electronic copies of sensitive personal information on any personally owned portable or non-portable device, or on portable storage devices. All personal data transferred must be encrypted and stored on the schools network.
5. **Liability and Responsibility:** Users are **solely responsible** for the correct care, safety and security of their personal device. The school accepts **no liability** for any loss or damage to personal devices brought into school.
6. **Monitoring and Inspection:** Use of the Internet, cloud, and email is **monitored** to prevent misuse and to protect school data. By signing the agreement, the user

agrees to such monitoring being carried out and accepts the school's right to check devices for inappropriate use at any time.

St Louis Wireless Internet Acceptable Use Policy – Rules for Pupils

Users must not use the school's wireless network or personal devices within the school environment to:

Prohibited Activities (Illegal and Highly Unacceptable Conduct)

1. **Access or Share Illegal Content:** Access, post, download, upload, communicate or pass on material, remarks, proposals, or comments that contain or relate to:
    - **Child sexual abuse images** (the making, production or distribution of indecent images of children).
    - **Grooming, incitement, arrangement or facilitation of sexual acts against children**.
    - **Possession of an extreme pornographic image** (grossly offensive, disgusting or otherwise obscene character).
    - **Criminally racist material** in the UK, including content intended to stir up religious hatred.
2. **Filter Avoidance:** Access 'Proxy Avoidance' sites or attempt to **by-pass the school's internet filter** in any way. Mobile broadband or personal hotspots are also not allowed for network access.
3. **Network Misuse:** Use systems, applications, websites or other mechanisms that bypass the filtering or other safeguards employed by the school.
4. **System Security:** Do not access, or attempt to gain access to, computer systems, data or resources to which you are not authorised. Users must not change their IP address or network settings.
5. **Illegal Acts:** Engage in the promotion or conduct of illegal acts, including fraud.

General Conduct and Network Usage

1. **Offensive Content:** Send or otherwise make available to others any material that is offensive, obscene or indecent, or infringes the **copyright** of another person (for example, MP3/4 or other audio or video formats).
2. **Annoyance and Interference:** Cause annoyance to others by playing music, videos or other materials through laptop or mobile device speakers. Users must use **personal headphones** when listening to audio, and headphones must not be shared.
3. **Unauthorised Recording:** Use in-built web cams or other in-built recording devices to record material of any kind deemed inappropriate by the supervising teacher or the Senior Management Team.
4. **Unauthorised Sharing:** Provide network services or access to other machines that are not authorised to be attached to the school's wireless network, including via Bluetooth or 3G/4G/5G technology.
5. **Bandwidth Abuse:** Access the Internet or network services in such a way as to deny reasonable access to the network for other users (e.g., by excessive use of network bandwidth, bit torrent file-sharing software, or accessing streaming media).

6. **Unauthorised Access Sharing:** Pass on your username and password to a third party for use in accessing the wireless network. This act is illegal under The Computer Misuse Act.

Failure to comply with these rules means you forfeit your access to the school's wireless network and will no longer be able to bring your laptop/device into school.

Responding to Incidents of Misuse (Sanctions Procedure)

If a pupil is found to have breached this policy, the response will follow these steps:

1. **Initial Incident:** The supervising teacher will remove the device immediately. The device will be held in the school office until 3:20 pm.
2. **Disciplinary Action:** The pupil will receive a warning, and depending on the nature of the behaviour, further disciplinary actions may be taken in line with the school's Positive Behaviour Policy.
3. **Parental Involvement:** The parents will be informed of the nature of the inappropriate behaviour. The parents and pupil must provide **written assurances** that such inappropriate behaviour will not occur again.
4. **Repeated Offence:** If the pupil fails to comply with these rules a second time, they will no longer be able to bring their laptop/device into school, and wireless access will be permanently withdrawn.
5. **Illegal Activity:** If there is any suspicion or confirmed use related to **illegal activity** (such as child sexual abuse images or serious criminal conduct), the incident will be immediately referred to the **Principal or Child Protection Officer** who will inform the relevant external agencies (Social Services/Police Service Northern Ireland).

Wireless Internet Acceptable Use Policy – Consent Form

This document must be signed and returned to the Director of ICT before devices may be used on the school's wireless network.

Pupil Name: **Tutor/ Year Group:**

Pupil's Agreement	I have read and I understand the school rules for 'Wireless Internet Use'. I will use my laptop/device, the school's computer systems, and Internet in a responsible way and obey these rules at all times. I agree that my use of these resources will not interfere with the education of others.

Signed:_____Date:_____

Parent's Consent for Wireless Internet Access	I have read and understood the school rules for responsible wireless Internet use and give permission for my son/daughter to access the internet using their laptop/device. I understand that the school will take all reasonable precautions to ensure pupils cannot access inappropriate materials. I accept that the school monitors Internet, cloud and email usage, and that the school is not liable for any damages arising from the use of the Internet facilities or loss or damage to my child's laptop/device.

Signed:_____Date:_____

Please Print Parent Name:

_____

(Please ensure the pupil's device has up-to-date anti-virus/internet security installed before bringing it to school.)