

Educational Technology Usage Policy

Our Lady of Good Counsel Girls' Primary School



1. Introduction

2. Aims

3. Scope

4. Roles and Responsibilities

- Board of Management
- School staff
- Parents/Guardians
- Students

5. Acceptable Use Guidelines

- General
- Students
- Website and Instagram

6. Online Safety and Digital Citizenship

7. Data Protection and Privacy

8. Remote and blended learning

9. Breaches of Policy

10. Review

1. Introduction

This policy outlines the acceptable use of educational technology (edtech) within Our Lady of Good Counsel Girls' School. It applies to all students, staff, and volunteers using school-owned or personal digital devices in the context of teaching and learning.

2. Aims

- Support teaching and learning through the safe use of digital tools.
- Ensure the well-being and safety of students in digital environments.
- Comply with national and European data protection laws.
- Promote responsible digital citizenship.

3. Scope

This policy applies to:

- All devices used on the school premises (computers, iPads, smart boards, phones and smart watches etc.).
- Online platforms, learning management systems and Apps, (e.g., Google Workspace, Seesaw, ClassDojo).
- Internet and email usage related to school.

4. Roles and Responsibilities

The Board of Management should:

- Ratify the policy and ensure resources are allocated for its implementation.

The Principal & ICT Coordinator should:

- Ensure implementation and regular review of the policy.
- Provide training and support to staff as necessary.

Teachers & SNAs should:

- Integrate edtech in alignment with curricular goals.
- Supervise students' use of digital tools.
- Be vigilant for and report misuse.
- Not use the school's name, logos, images or comment on the school or members of the school community on-line.

- Ensure the school should not be identified or identifiable on social media or any other websites. (It's important to remember that as members of the school staff we are all identifiable as members of this school community and therefore care and consideration should be given to any post.)
- Ensure all written communications with parents are through the Aladdin platform. (Staff should not use WhatsApp or email to communicate with parents.)
- Logout of devices when not in use and protect their passwords.
- Keep devices secure.

Parents/Guardians should:

- Monitor at-home use of technology for homework.
- Support the school's efforts in promoting safe online behaviour.
- All communications with teachers and staff should be through the Aladdin platform and will be accessible between 8 am and 4pm, Monday-Friday during term time.

Students should:

- Use technology responsibly and respectfully.
- Report inappropriate content or cyberbullying.

5. Acceptable Use Guidelines

General:

- Internet access is filtered and monitored.
- Communication on digital platforms must be kind, respectful, and school-related.
- Cyberbullying or misuse will result in disciplinary action.
- The generation of images and recordings of students should only be done on school-owned devices with the consent of all parties involved for educational reasons.
- Staff should not take images of the children where they are identifiable. They may take photos of the children engaged in activities for the school Instagram or for educational purposes so long as the children are not identifiable.

Students:

- Students use school-approved software and platforms only.
- Personal devices (phones, iPads and smartwatches) may not be used during school hours unless approved. Mobile phones and smartwatches must remain switched off in a pupil's school bag while a pupil is on school grounds. If a pupil uses their personal device without prior approval, it will be confiscated and held by the Principal for a parent/guardian to collect.

- Students will not send or receive by any means any material that is illegal, obscene, defamatory, or that is intended to annoy or intimidate another person at any time or on school devices.
- Students accept that any use of school devices is subject to inspection by their teacher.
- Students will be made aware that any usage, including sharing or receiving information that occurs within the school network will be monitored for unusual activity, security and and/or network management reasons.
- Students are not permitted to take or send photos or videos of other students or teachers without their consent.
- The use of USB-sticks or other digital storage devices in school requires the permission and supervision of the teacher.
- Any photos taken on the school iPads should be deleted when the iPad session finishes.
- Students should not send voice or text messages of a threatening or hurtful nature to another person.
- Any intimidation, harassment, cyber-stalking, vilification, rejection, impersonation or exclusion over technology will be considered as cyberbullying and subject to disciplinary action*.

School Website & Instagram Account:

- Managing and posting to the school website (www.johnstowngns.com), and Instagram account (<https://www.instagram.com/johnstowngirlsschool>), is the responsibility of the AP1 postholder responsible for this area. This person may take photos of the children with the purpose of posting to the website or Instagram. The photos will be deleted from their device once used.
- Images of pupils will only be posted to the school website with consent from parents or other parties as relevant.
- Photographs of pupils published on the school's Instagram account must ensure that individuals are not identifiable.

6. Online Safety and Digital Citizenship

- The school teaches online safety as part of the SPHE and Wellbeing curriculum.
- The school celebrates Internet Safety Day annually with activities and the promotion of on-line safety awareness.
- Children are taught about privacy, critical thinking, and the ethical use of technology.
- No student images, videos, or work will be shared online without parental consent.

7. Data Protection and Privacy

- All edtech platforms used are GDPR-compliant.

- As applicable parents are informed about what data is collected and why.
- Staff follow the school's Data Protection Policy and ensure student information is stored securely.

8. Remote and Blended Learning

- During school closures, platforms such as Google Classroom or Seesaw, will be used for remote instruction.
- Video conferencing tools are used with appropriate safeguards (e.g., adult supervision, no recordings unless agreed upon).

9. Breaches of Policy

- Minor breaches will be addressed through restorative practice and education.
 - Serious or repeated breaches (e.g., accessing harmful content or cyberbullying) will lead to disciplinary measures and parent involvement.
- *Procedures in relation to sanctions relating to inappropriate use of digital devices are covered in our ***Bí Cinéalta Policy*** and our ***Code of Behaviour***.

10. Review

This policy will be reviewed every two years or in response to significant changes in legislation or edtech practices.

Ratified by the Board of Management & school principal:

Date published: September 8, 2025.

Chairperson Signature: 

Principal: 

Policy Review Date: _____