Acceptable Use Policy (AUP)

Scoil Bhríde Shantalla

Address: Shantalla Road, Galway
Website: www.scoilbhrideshantalla.ie
Email: info@scoilbhrideshantalla.ie

---

1. Aim of the AUP

The aim of this Acceptable Use Policy (AUP) is to ensure that all students and staff at Scoil Bhríde Shantalla benefit from access to digital technologies, including the internet, in a safe and responsible manner. The AUP sets out the guidelines for using these technologies, both on school premises and during any school-related activities off-site. Breaches of this policy may result in the withdrawal of digital privileges and other disciplinary measures.

2. Scope of the AUP

This policy applies to all members of the school community (students, staff, and volunteers) who use the school's digital devices, network, and internet connections, as well as personal devices used on school premises.

3. Digital Technologies at Scoil Bhríde Shantalla

The school provides a range of technologies for use in education, including:

- **Chromebooks for students:** Each student may use school-provided Chromebooks for educational activities.
- **Google Workspace for Education:** All students have individual school-managed Google Accounts, providing access to Google Classroom, Google Drive, Gmail (if activated), and other educational tools.
- **Smartboards and Teacher Laptops:** Windows laptops tethered to SmartBoards are used by teachers to facilitate interactive lessons.

- **Internet Access:** The school's internet connection is filtered and monitored using the Oide's Filtering Service (Level 6), designed to block harmful or inappropriate content.

The school employs an external support company to help manage, repair or replace hardware or systems.

The school's IT coordinators Robin White and Adrian Carey manage the school's day to day digital environment and ensure secure and efficient use of all technologies.

---

4. General Guidelines for Internet and Device Use

4.1 Educational Use

- The use of the internet and digital devices is solely for educational purposes.
- Students will not use the internet or school devices to access social media, chat rooms, or gaming sites unless explicitly permitted by a teacher for educational reasons.
- Students should refrain from downloading or installing software or apps on school devices without teacher permission.

4.2 Responsible Online Behavior

- Students must act responsibly and ethically in all their digital interactions.
- Personal details such as addresses, phone numbers, and passwords should not be shared online.
- Students are advised to avoid disclosing personal information in emails or any other online platforms.
- Inappropriate use, such as accessing offensive, illegal, or harmful websites or materials, is strictly prohibited.

4.3 Privacy and Data Protection

- Students and staff must respect the privacy of others. Unauthorized access to another person's files, emails, or digital accounts is forbidden.
- The school will adhere to General Data Protection Regulation (GDPR) guidelines to ensure that student data is processed lawfully, fairly, and transparently.

---

5. Email, Messaging, and Communication Tools

5.1 Use of Google Accounts

- All students have access to a school-managed Google Account, which includes tools such as Gmail, Google Drive, and Google Classroom.

- Emails and other communications using these accounts are monitored for appropriate use.
- Students are expected to use these tools only for school-related communications.
- Personal email accounts and social media are not to be accessed during school hours.

5.2 Guidelines for Email and Messaging

- All messages should be polite, respectful, and related to schoolwork. Offensive or threatening messages will be dealt with under the school's disciplinary procedures.
- Students should never agree to meet someone in person whom they have only met online.
- Any suspicious or inappropriate communication should be reported to a teacher immediately.

---

6. Online Safety and Cyberbullying

6.1 Cyberbullying

- Cyberbullying is taken very seriously by the school and will not be tolerated in any form.
- Cyberbullying includes the use of email, messaging apps, or social media to harass, threaten, or harm others.
- Students and staff are encouraged to report any incidents of cyberbullying immediately to a teacher, principal, or the IT coordinators.

6.2 Digital Literacy and Safety Education

- The school integrates digital literacy into the curriculum, teaching students about online safety, data privacy, and responsible online behavior.
- Regular lessons on identifying and reporting online threats or inappropriate content will be conducted.

---

7. Use of Images and Media

7.1 School Website and Social Media

- With parental/guardian consent, student achievements, class projects, or school activities may be shared on the school’s website and social media platforms.
- No personal information, such as full names or contact details, will be published alongside student images.

7.2 Consent for Use of Images

- Parental consent will be sought before posting any images or media of students online. Parents may opt-out at any time by notifying the school in writing.

---

8. Mobile Phones and Personal Devices

8.1 General Policy

- Students are not permitted to use mobile phones during school hours unless explicitly allowed by a teacher for educational purposes.
- Personal devices such as tablets, smartwatches, and phones must be switched off and handed to the teacher if brought to school.
- The school takes no responsibility for the loss, damage, or theft of personal devices on school grounds.

8.2 Mobile Phone Use in Emergencies

- In emergencies, students may use their phones with the permission of a teacher or staff member. Parents should contact the school office if they need to reach their child during school hours.

---

9. Sanctions and Consequences

Misuse of digital technologies or violation of the school's AUP will lead to consequences. These may include:

- **Verbal or written warnings** for minor breaches.
- **Loss of access privileges** to the school network or devices for repeated or more severe breaches.
- **Detention or suspension** for serious violations or for cyberbullying, inappropriate use of digital devices, or accessing prohibited websites.
- **Referral to Gardaí** or other authorities if illegal activities, such as hacking or accessing indecent material, are involved.

All sanctions will be imposed in accordance with the school's Code of Behaviour policy.

---

10. Review and Updates

This Acceptable Use Policy will be reviewed periodically by the school management, the Board of Management, and parent representatives to ensure it remains current and effective. Any changes to the policy will be communicated to parents and staff in writing.

Chairperson of Board of Management:
Fr. Kevin Keenan

Principal:
Frank Keane

ICT Coordinators:
Robin White & Adrian Carey