Bring Your Own Device ("BYOD") Policy

This policy applies to the whole school including the EYFS

Purpose

The Bring Your Own Device (BYOD) policy outlines the rules and guidelines for the use of personal electronic devices within the school environment. The purpose of this policy is to promote responsible use of technology in supporting educational activities while ensuring a safe, secure, and respectful learning environment. This policy also includes provisions for school-provided laptops issued to teachers and some support staff and incorporates measures for data protection.

Scope

This policy applies to all students, staff, and visitors who bring personal electronic devices, including but not limited to laptops, tablets, smartphones, and other handheld devices, onto school premises. It also applies to school-provided laptops issued to teachers and some support staff.

The school supports the use of both personal electronic devices and school-provided laptops as educational tools, provided their use aligns with the school's educational goals and the requirements of this policy. The BYOD policy is designed to enhance learning opportunities, facilitate access to digital resources, and prepare students and staff for a digital future while maintaining the integrity, security, safety, and data protection of the school's network and environment.

Acceptable Use of Devices

All users of personal electronic devices and school-provided laptops must comply with the following acceptable use guidelines:

- **Educational Purpose:** Devices are to be used primarily for educational purposes, such as accessing digital resources, completing assignments, conducting research, and collaborating on school projects.
- **Respectful Use:** Devices must be used in a manner that respects the privacy and rights of others. Recording or taking photos of individuals without their consent is strictly prohibited.
- **Restricted Areas:** Device usage is prohibited in areas where privacy is expected, such as changing rooms, toilets, and any other areas designated by the school.

- **Disruption-Free:** Devices should not be used in a manner that disrupts the educational environment or distracts other students. Teachers have the authority to limit or prohibit device use during their classes or activities if deemed necessary.
- **Adherence to School Policies:** All use of devices must comply with the school's Safeguarding Policy, Acceptable Use Policy (AUP), Online Safety Policy, Data Protection Policy, and all other relevant policies and guidelines.

Network and Security

To ensure the security and integrity of the school's network and data:

- **Network Access:** Personal devices and school-provided laptops may connect only to the designated school network for internet access. Connection to any other school network or bypassing the school's network security is prohibited.
- **Security Measures:** Users must ensure that their devices are protected with up-to-date antivirus software and have the latest security updates installed. Devices should have secure passwords or passcodes to prevent unauthorised access.
- **Data Protection:** Users must ensure that any sensitive or personal information stored on their devices is protected in accordance with data protection laws and the school's Data Protection Policy. Unauthorised access, sharing, or dissemination of such information is strictly prohibited.
- **Prohibited Activities:** Users are prohibited from engaging in any activities that compromise network security, including but not limited to hacking, installing unauthorised software, or accessing restricted sites.

Data Protection

To safeguard personal and sensitive data in compliance with the General Data Protection Regulation (GDPR) and other applicable data protection laws:

- **Handling of Personal Data:** All personal data accessed or stored on personal devices or school-provided laptops must be handled in accordance with the school's Data Protection Policy. Staff and students are responsible for ensuring that any personal data is processed lawfully, fairly, and transparently.
- **Data Storage:** Personal and sensitive data should not be stored on personal devices unless absolutely necessary for educational purposes. If such data must be stored on a personal device, it should be encrypted and securely deleted once it is no longer needed.
- **Data Access:** Access to personal and sensitive data must be restricted to authorised individuals only. Users must not share login credentials or access rights with others.
- **Data Breach:** Any suspected or actual data breach must be reported immediately to the school's Data Protection Officer (DPO).

Responsibilities

Students

- Ensure personal devices are fully charged and ready for use during school hours.
- Use devices responsibly and in accordance with the school's BYOD policy and other relevant policies.
- Protect personal and sensitive data by following the school's data protection guidelines.
- Report any security concerns, technical issues, or inappropriate behavior immediately to a teacher or school administrator.
- Maintain the security of personal devices at all times and avoid leaving them unattended.

Teachers and Support Staff

- Use school-provided laptops primarily for educational and professional purposes in line with school policies.
- Ensure school-provided laptops are securely stored when not in use and report any loss or damage immediately.
- Follow the school's data protection guidelines when handling personal and sensitive data.
- Model and enforce appropriate use of devices in accordance with the BYOD policy.
- Monitor student use of devices in their classrooms and take appropriate action when misuse is detected.
- Provide guidance to students on acceptable use, digital citizenship, and data protection.
- Report any violations of the BYOD policy or data protection breaches to the school administration or Data Protection Officer.

Parents/Guardians

- Ensure that their child understands and adheres to the BYOD policy.
- Provide appropriate internet filtering and monitoring at home to support safe and responsible use of devices.
- Understand that the school is not responsible for loss, damage, or theft of personal devices.

School-Provided Devices

- **Issuance:** Teachers and some support staff will be issued school laptops for educational and professional use. These devices remain the property of the school and must be returned upon request or when employment ends.
- **Use:** School-provided laptops are to be used primarily for school-related activities and should not be used for personal purposes that conflict with the school's Acceptable Use Policy.
- **Maintenance and Updates:** The IT department is responsible for maintaining and updating all school-provided laptops to ensure they remain in good working condition and have the latest security updates and software installed.
- **Security:** Staff must ensure school-provided laptops are used securely, with passwords or other security measures enabled to prevent unauthorised access.

Liability and Insurance

- **Responsibility for Devices:** The school does not accept any responsibility for personal devices brought onto school premises. Users bring devices at their own risk.
- **Insurance:** It is the responsibility of the device owner to ensure their device is covered by appropriate insurance. The school does not provide insurance coverage for personal devices.
- **School-Provided Laptops:** The school provides insurance coverage for school-provided laptops. Staff must report any damage or loss immediately to the IT department.

Monitoring and Compliance

- The school reserves the right to monitor and review the use of personal devices and school-provided laptops on its network to ensure compliance with this policy.
- Any breach of this policy or data protection laws will be addressed in accordance with the school's disciplinary procedures. This may include temporary or permanent suspension of network access, confiscation of the device, or other appropriate actions.

Training and Awareness

- The school will provide training sessions and resources to educate students, staff, and parents about safe and responsible use of devices and data protection.
- Regular updates and reminders about the BYOD policy, acceptable use, and data protection will be communicated through the school's communication channels.

- This policy will be reviewed annually by the school's IT department in conjunction with the Senior Leadership Team to ensure it remains effective, compliant with ISI standards, and reflective of technological advancements.
- Amendments to the policy will be communicated to all stakeholders and will take effect immediately upon approval.

- The BYOD policy will be made available to all students, staff, and parents via the school's website, handbooks, and at school assemblies and meetings.
- New students and staff will be informed about the BYOD policy during their orientation programs.