



**School of Knowledge**  
(St. Mary's Group of Schools)

# **Bring Your Own Device (BYOD) POLICY**



## 1. INTRODUCTION:

Technology plays a large role in our students' lives. The Bring Your Own Device (BYOD) initiative ensures students learn collaboration, communication, creativity and critical thinking in a variety of ways throughout the school day. The school is committed to integrating digital wellness to promote healthy, balanced technology use among students. In order to achieve this, we want to ensure that every pupil can be connected to the school's electronic resources throughout the school day, within the school and beyond. We require that pupils own and bring an appropriate mobile device to school. Personal devices can enhance and enrich learning opportunities both at home and at school.

## 2. PURPOSE:

This policy outlines the acceptable use of electronic devices to maintain a safe and secure education environment with the goal of preparing students for the future, improving learning, and fostering digital citizenship. An important component of B.Y.O.D will be education about appropriate online behaviors. We will review online safety rules with students frequently throughout the course of the school year and will offer reminders and reinforcement about safe online behaviors. Regular digital literacy sessions will be conducted to educate students on cyber safety, information verification, and responsible online interaction. In addition to the rules outlined in these guidelines, students will be expected to comply with all class and school rules while using personal devices. The use of technology is not a necessity but a privilege. When abused, privileges will be taken away.

## 3. AUTHORIZED USE OF ELECTRONIC DEVICES:

Electronic devices brought to school shall be restricted to educational and administrative purposes in approved locations and times under the supervision of school personnel. Devices must be equipped with up-to-date antivirus software

Authorized users shall

- Use electronic devices in accordance with the expectations set forth in the school Use Policy/Agreements.
- Comply with guidelines set by school personnel for the use of electronic devices while on school property or while engaged in a school-sponsored activity.
- Take photographs and audio/video recordings only with a person's consent and when authorized by school personnel for educational purposes.
- Access the school network using approved infrastructure only.
- Use of VPNs, proxies, or any means to bypass school filters is prohibited.

## 4. RESPONSIBILITIES:

All **Users** are responsible for:

- Registering their electronic device with the school's IT Administrator.
- Ensuring electronic devices are used in accordance with school policies and procedures.

- Caring, maintaining, securing, and storing electronic devices.
- Preserving privacy of accounts, login names, passwords, and/or lock codes to maintain security of electronic devices and data.
- Maintaining safe and productive learning environments when using electronic devices.
- Practicing digital citizenship.
- Must not install or use unauthorized software or applications on devices used within the school.

All **Administrators** are responsible for:

- Informing users of school policy.
- Establishing and monitoring digital citizenship through the schools Acceptable Use Policy/Agreements.
- Responding effectively to disciplinary issues resulting from inappropriate electronic device usage.
- Communicating appropriately with school personnel, parents, and students if school policy is violated from electronic device usage.
- Providing information to users explaining how to connect electronic devices to the school network.

**Teachers** are responsible for:

- Creating equitable learning opportunities that include electronic devices for education purposes when relevant to curriculum and instruction.
- Determining when students are able to use school or personal electronic devices for education purposes.
- Supervising student use of electronic devices.
- Responding effectively to disciplinary issues from inappropriate electronic device usage.
- Communicating appropriately with administrators, parents, and students if school policy is violated from electronic device usage.
- Including digital conduct expectations in lesson plans and regularly review them in class.

**Students** are responsible for:

- Using electronic devices for educational purposes in approved locations under the supervision of school personnel only.
- Reporting any inappropriate electronic device usage to a teacher or administrator immediately.
- Ensuring their electronic devices are charged prior to bringing them to school.
- Continuing to learn using an alternative method if an electronic device malfunctions.
- Not using devices during tests or assessments unless explicitly permitted.

**Parents** are responsible for:

- Helping their children take all reasonable steps to care, maintain, secure, store, and transport their

electronic device

- Helping their children preserve the privacy of accounts, login names, passwords, and/or lock codes.
- Identifying the electronic device by labeling it, recording details such as make, model, and serial number.
- Encouraging their children to follow school policy and practice digital citizenship;
- Monitoring screen time of their children at home and supporting digital well-being strategies initiated by the school.

## **5. UNAUTHORIZED USE OF ELECTRONIC DEVICES:**

Prohibited uses of electronic devices includes:

- Areas where there is a reasonable expectation of privacy, such as change rooms or restrooms.
- Downloading files that are unrelated to educational activities.
- Engaging in non-educational activities such as playing games, watching videos, using social media, listening to music, texting, or taking personal calls.
- Cheating on assignments or tests.
- Accessing information that is confidential.
- Using photographs and audio/video recordings for a purpose unrelated to the school assignment.
- Obtaining unauthorized access and using it to alter, destroy, or removing data.
- Engaging in cyberbullying which involves using technology to harass, threaten, embarrass, or target another person.
- Infecting a device with a virus or other program designed to alter, damage, or destroy.
- Infringing upon copyright laws or plagiarizing protected information.
- Using the devices for unauthorized recording or livestreaming of classes.

## **6. CONSEQUENCES: REMEDIAL AND DISCIPLINARY ACTION:**

Individuals who do not comply with this Policy will be subject to appropriate consequences consistent with the school Code of Conduct and Acceptable Use Policy/Agreements. Consequences may include;

- Temporary confiscation of device.
- Search of device contents to locate evidence of misuse.
- Limitations, suspension, and/or revocation of access privileges to personal and school technology resources.
- Disciplinary measures, up to and including dismissal.
- Legal action and prosecution by relevant authorities.

Repeated violations will be escalated to the school disciplinary committee and may lead to permanent restriction from the BYOD program.

**7. LIABILITY:**

- Users are solely responsible for the care and use of electronic devices they choose to bring to school. Users bringing these devices to school do so at their own risk.
- The school and school personnel shall not be liable for the loss, damage, misuse, or theft of any student-owned electronic device: possessed/used during the school day; in/on school buildings, property, vehicles, or contracted vehicles; during transport to/from school.
- The school and school personnel shall not be responsible for any negative consequences to electronic devices caused by running specific software or by accessing the school network.

**8. TECHNICAL SUPPORT:**

School personnel shall not provide technical support, troubleshooting, or repair for user-owned electronic devices. A basic troubleshooting guide and FAQ will be made available to assist students and parents in resolving common technical issues independently.

**POLICY REVIEW LOG:**

Policy Details	BYOD Policy
Reviewed/ Approved By & Date	E-safety Team and SLT / June 2025
Next Revision Date	June 2026