BRING YOUR OWN DEVICE (BYOD)

"At our school use of technology is not a necessity but a privilege. When abused, privileges will be taken away."

Objectives

To ensure students learn collaboration, communication, creativity and critical thinking in a variety of ways throughout the school day.

To ensure that every student can be connected to the school's electronic resources throughout the school day, within the school and beyond.

Definitions:

Electronic Devices: all computing devices that can take photographs; record audio or video data; store transmit or receive messages or images; or provide a wireless connection to the Internet. Examples of these devices include, but shall not be limited to laptops, tablets, iPads, as well as any technology with similar capabilities. Mobile phones should be restricted/prohibited.

Digital Citizenship: the norms of responsible behavior related to the appropriate use of technology. It encompasses digital literacy, ethics, etiquette, and online safety.

Users: any individual granted authorization to use electronic devices. Users may include students, parents, staff, volunteers, visitors, contractors, or individuals employed by service providers.

Authorized Use of Electronic Devices and Restrictions:

- School Code of Conduct and Internet Acceptable Use policy
- Comply with guidelines set by school personnel while on school property
- Take photographs and audio/video recordings only when authorized by school personnel for educational purposes
- Access the school network using approved infrastructure only

Responsibilities: All Users are responsible for:

- Registering their electronic device with the school and submitting a signed Use of Electronic Devices Agreement prior to connecting to the school network.
- Ensuring electronic devices are used in accordance with school policies and procedures.
- Caring, maintaining, securing, and storing electronic devices; any damage may be caused
- 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.

All Administrators are responsible for:

- Informing users of school policy.
- Establishing and monitoring digital citizenship through the school Code of Conduct and Internet Acceptable Use policy.
- 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.
- Review cyber-safety rules with students frequently throughout the course of the school year and will offer reminders and reinforcement about safe online behaviors.

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.

Students are responsible for:

- Using electronic devices for educational purposes in approved locations under the supervision of school personnel only.
- Implementing virus and malware scanning on their electronic devices.
- 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.

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, and/or installing tracking software.
- Encouraging their children to follow school policy and practice digital citizenship.
- Contacting the school office to communicate with their child during the school day, instead of using text messages, emails, phone calls, or other digital means that have no curriculum related/education purpose.
- Assuming all responsibility for their child's unauthorized use of non-school Internet connections such as 4G cellular phone network or similar.

Unauthorized Use of Electronic Devices

Prohibited uses of electronic devices includes, but are not limited to:

- Areas where there is a reasonable expectation of privacy, such as change rooms or restrooms.
- Circumventing school's approved network infrastructure to access Internet connections using an external wireless provider.
- 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.
- Committing a crime under federal, local, regional, and/or community statues.
- Infringing upon copyright laws or plagiarizing protected information.

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 Internet Acceptable Use Policy.
- Consequences may include, but are not limited to, the following, either singularly or in combination depending on the individual circumstances:
- 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.

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; while attending school-sponsored activities.
- 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.

Technical Support:

School personnel shall not provide technical support, troubleshooting, or repair for user-owned electronic devices.

Risk Assessment

Security: Protecting data and system security

- Risk of compromising system security
- Managing secure access to school data and protecting students' personal data means an increased workload and responsibilities for school ICT support staff.
- Potential Legal Issues
- Poor Mobile Devices Management
- Lack of staff Training
- Safeguarding students and staff
- Strategies and school policies for ensuring safe internet use and dealing with bullying, cyber-bullying and cheating
- Develop a robust authentication system: school credential management
- Privacy: protection of school data and students' data and the employee's privacy.
- Compliance – local and international regulations and standards for how data is collected and stored

Security of Social Media

- Social media sites (e.g. Facebook, Instagram, Twitter etc.); often targeted with malware and viruses.
- Ensure the appropriate protection is in place on the device, and block all social media on campus

Protecting Schools

- Think through and test school BYOD policy before rolling it out school-wide
- Take inventory of every student and staff device accessing your network
- Conduct periodic audits of school BYOD policy

Pros and Cons of BYOD

Pros

- Savings for the school on purchasing and replacing technology
- No learning curve for staff
- Potential improvement of staff morale
- More up-to-date tech due to personal upgrades

Cons

- More complex IT support for disparate devices and operating systems
- Higher security risks
- Potential loss of staff and school privacy
- Some staff and or students may not have their own devices