Electronic Devices / Digital Resources / Bring Your Own Device (BYOD)/ Acceptable Use Policy

POLICY FOR	Acceptable Use of Digital Resources
PERSON RESPONSIBLE	Head of Pastoral/ Digital Leader
REVIEW DATE	March 2024
REVIEWED BY	Assistant Principals and Head of School
APPROVED DATE	March 2024
APPROVED BY	ELT
DATE OF NEXT REVIEW	June 2025
RELATED POLICIES	Rewards and Sanctions Policy, Social Media Policy, E-Safety Policy, Anti-Bullying Policy, Wellbeing Policy

Executive Principal / CEO ……

ACCEPTABLE USE OF DIGITAL RESOURCES POLICY

Introduction:

The Westminster School, Dubai (TWS) recognizes that access to technology in school gives students greater opportunities to learn, engage, communicate, and develop skills that will prepare them for work, life, and citizenship. We are committed to helping students develop 21st-century technology and communication skills and provide infrastructure access to technologies for student use.

This policy describes the acceptable use of digital technology. It is designed to minimize the potential risk to students, protect employees and the school from litigation as well as maintain levels of professional standing. The policy is designed to ensure the safe and responsible use of electronic devices by all users, both on the school premises and elsewhere where the school is represented.

The device will be registered for internet access through the school network using students.
GEMS-learning ID. Students will be expected to follow the Acceptable Use Digital Policy in social media, whichis printed in the school planner for both parents and students. Furthermore, all students will carry **only non-cellular devices**. Special permission is to be taken from the Form Tutor for carrying cellular devices. Cellular devices/mobile phones cannot be used in school before 2.30 PM.

The purpose of the 'Electronic Devices / Digital Resources / BYOD / Acceptable Use Digital Agreement' is to ensurethat all students use technology in school effectively, safely, and responsibly, to facilitate learning and to help ensure that they develop the attributes of competent digital citizens.

In order to use the school's digital resources, the students must follow the guidelines set forth in this policy. TWS reserves the right to change this agreement as and when necessary to do so. It is a general agreement that all facilities (hardware, software, Internet, etc.) are to be used in a responsible, ethical, and legal manner, in and out of school. By using any digital resources, whether owned personally or by the school,users acknowledge their understanding of the Electronic Devices / Digital Resources / BYOD Agreement as a condition of using such devices and the Internet. The school provides services to promote educational excellence. The school has a responsibility to maintain the integrity, operation, and availability of its electronic systems for access and use.

Whilst on site, access to the school network and the Internet should be considered a privilege, not a right, and can be suspended immediately, without notice in case of non-compliance of the policy. Access on site is available only for educational and research purposes. Digital resources are to be used in accordance with this policy and all users will be required to comply with its regulations. Use of private data network/ VPN is strictly prohibited.

The guidelines provided in this policy are intended to help users understand appropriate use. The school may restrict, suspend, or terminate any user's access to the school's computer systems upon violation of this policy and action will be taken according to the school's Rewards and Sanction policy. This policy applies to all digital resources, not only the computers, devices and equipment provided in the school's IT labs but also the personal devices students bring to school in accordance with the school's Bring Your Own Device initiative.

The Electronic Devices / Digital Resources / BYOD policy provides guidelines for using all digital hardware and software (on individual computers/devices, on local area networks, wide area networks, wireless networks, the Internet and companion technological equipment - e.g. printers, servers, whiteboards, projectors, etc. when students are at school). The policy also establishes rights and responsibilities for all users in the school. All users of the school network are expected to follow the guidelines or risk loss of digital privileges. In cases of serious breaches, further action may be taken, in line with the school's standard disciplinary procedures.

Netiquette:

- Users should not attempt to open files or follow links from unknown or untrusted origins.
- Recognizing the benefits collaboration brings to education, TWS provides the students with access to websites or tools that allow communication, collaboration, sharing, and messaging among students. Students are expected to communicate with appropriate, safe, mindful, and courteous conduct online and offline.
- Playing commercial/online games and visiting sites not related to education is not permitted. Watching Movies, TV Shows, etc. while at school is prohibited unless the media has been checked-out from the school library.
- Respect the use of copyrighted materials. Respect the rights and privacy of others.
- Downloading of unauthorized programs is not allowed.
- Avoid modifying or copying any protected system files, system folders, or control panel files on school equipment.
- Obey the laws and restrictions of UAE, do not use personal equipment to record (audio/visual) of others without their/school's permission and upload them on social media.
- Alert a teacher or other staff member if seen threatening, inappropriate, or harmful content(images, messages, posts) online and help maintain the integrity of the school network.
- You should use trusted sources when conducting research via the Internet.

Personal Safety:

- Students should not share personal information, including phone number, address, ID number, passwords or birthday over the Internet without adult permission.
- Students should recognize that communicating over the internet brings anonymity and associated risks and should carefully safeguard the personal information of themselves and others.
- Students should not agree to meet someone they met online in real life without parental permission.
- Students should not share private pictures/videos online which could lead to cybersecurity threat.
- If students see a message, comment, image, or anything else online that makes them concerned for their personal safety, they must bring it to the attention of an adult (teacher if they are at school; parent if they are using the device at home) immediately.
- Students should always use the internet, network resources, and online sites in a courteous and respectful manner.
- Students should also recognize that some valuable content online is unverified, incorrect, or inappropriate.
- Students should avoid any irrelevant post/s online that they would not want parents, teachers, future colleagues, employers, or the UAE government to see.

Equipment:

- The school highly recommends the use of tablet devices including **iPad or Android** for **Primary / Secondary** students and **Mac or Windows laptops** for **senior students**.
- **Students** are strictly prohibited from using cellular devices to school without prior permission from FT/KSL/HOH/HOP. **The only exemption to this rule is for the Sixth Form students.**
- Phones without SIM can be used only for learning purposes during school hours with **explicit permission** from a teacher.
- If the teacher suspects the misuse of the device, then the teacher could confiscate the device and escalate the matter to the parent.
- If students need to contact parents at any time, this is allowed via the Head of House/ Head of Pastoral/ Key Stage Leader.
- Only One Device (BYOD) per user is allowed to be connected to school Wi-Fi.
- TWS will **not** be financially accountable for any loss or damage of any individual devices**.**

Violations:

Misuse of devices will result in a denial of access and possible further disciplinary action. The corrective measures will involve notification to parents/ detention/ warning letter or suspension from school and school-related activities and disciplinary action will be taken as per the school's Rewards and Sanctions Policy. The school maintains the right to collect and examine any device that is suspected of causing problems or violating the policy.

- Mobile phones / other devices are not allowed to be used until 2.30 PM.
  Smart watches or blue tooth devices are not allowed.
- Any attempts to transmit software designed to compromise the operation or security of the school network in any manner.
- Prohibition of installation and use of Virtual Private Networks in school.
- Students are not permitted to use school technologies to pursue information on illegal activities.
- Students should not download or attempt to download any software onto school equipment.
- Students are not permitted to use or attempt to use another student's e-learning ID, hardware, subscriptions, files, or personalinformation.
- Tampering or experimenting with the school network or equipment, including efforts to bypass the school's Internet filters or proxies is not permitted.
- Students are not allowed to use school technologies in a way that could be personally or physically harmful.
- Students are not permitted to:
  - attempt to hack or access sites, servers, or content that is intended for any personal use.
  - Use school technologies to send spam or chain mail.
  - Use Plagiarized content found online and attempt to find inappropriate images/material post-personally identifying information, about oneself or others.
  - Use language online that would be unacceptable in the classroom and/or at home.

During Lessons:

- Use of personal devices is at the discretion of teachers and staff. Students must only use devices as permitted by their teacher.
- Devices must not disrupt classroom learning in any way and devices should be switched offat all other times.
- Recording video, audio or taking a photograph required for an assignment, a student must obtain written permission from the people appearing in the video and from the concerned teacher.

During Independent Study:

- Students can use personal devices only in:
  - ✓ supervised study lessons
  - ✓ library (tablets, kindle)
  - ✓ Self Learning Room (Sixth Form)

Students will not be allowed to use their devices in transit between lessons, or in the corridors or anywhere within the school premises, therefore minimizing disruption and in doing so could lead to confiscation of the device.

Cyber-Bullying/Social Media:

Cyber-bullying will not be tolerated. "Harassing, dissing, flaming, denigrating, impersonating, outing, tricking, excluding, body shaming and cyber-stalking" are some examples of cyber-bullying. Students should not send emails or post comments with the intent of scaring, hurting, or intimidating someone else. Engaging in these behaviours, or any online activities intended to harm (physically or emotionally) another person, will result in severe disciplinary action and loss of privileges. In such cases, cyber-bullying can be considered a crime. Remember that your activities are monitored and retained.

Students will be held accountable for Cyber-Bullying, even if it occurs off-campus during the school year and negatively impacts the academic environment at TWS or if using the TWS name or logo to post memes or trolls on any site. Students are informed and kept updated that in the UAE there are extreme consequences for online defamation of character of person or an organization and punishable by law.

The UAE Student Conduct Disciplinary Bylaw and the Federal Decree-Law no. (5) outline that deliberately creating, transferring and publishing photos and comments on social media (Instagram and WhatsApp) that undoubtedly shows defamation of individuals or staff members or School Leadership of character, dignity and integrity are breaking the law.

Key provisions relevant to schools extracts of Federal Decree-Law no. (5) state:

21	Invasion of privacy, including photographing others, or creating, transferring, disclosing, copying or saving electronic photos (just taking a photo or video of someone without their permission, or saving a photo they have posted, is enough). Defamation. Publishing news, photos, scenes, comments, statements or information, even if true and correct. Amending or processing a record, photo or scene for the purpose of defamation of or offending another person or for attacking or invading his privacy.	Up to 6months' imprisonment +/ fine of AED 150k – 500k

School Liability Statement:

- Students bring their devices to use at The Westminster School at their own risk. Students are expected to act responsibly in regard to their own devices, keeping them up to date with anti-virus software and as secure as possible. It is their duty to be responsible for the upkeep and protection of their devices. The Westminster School is not responsible for:
  - personal devices that are damaged while at school or during school-sponsored activities.
  - personal devices that are lost or stolen at school or during school-sponsored activities.
  - network costs incurred should the student not use the school-provided wireless- network.
- Any damage or disruption to the school network caused as a result of improper use of a student-owned device will be regarded as a very serious matter and could lead to strong disciplinary actions from the school.
- Students must keep their devices switched off and in a secure place when not in use.

Consequences for Device Misuse/ Disruption to Learning (one or more may apply):
Stage 1: Device confiscated and given to Head of House to return at the end of the day.
Stage 2: Device confiscated and given to Head of House to return s to the parent / Head of House issues detention/Warning Email sent to parents.
Stage 3: Device confiscated and passed to Head of House / SLT Warning letter issued.

<u>These stages could include the student's e-learning account to be suspended till the matter is resolved.</u>

Students arguing with any member of staff over a mobile phone infringement will be dealt with very seriously. Members of staff have been asked to implement the policy consistently, and therefore there should be no cause for argument.

School will have the authority to confiscate any device under the following conditions:

- *Misuse (using it for purposes other than academic exercises) and without the teacher's permission.*
- *As a source of an attack physical assault or threat*

Students need to be fully aware of their responsibilities that are reinforced at school via the curriculum that covers **Common Sense Media**. This provides the students with a clear understanding of the above conditions within the UAE and includes comprehensive coverage of issues relating to students' own 'digital footprints' and creating a positive online presence, as well as interaction with others.

Confidentiality:
All reported cases will be treated with utmost confidentiality at all times.

Referral:

The school may refer the student to the government or non-government agency concerned if deemed necessary.

Monitoring and Evaluation:

Pastoral and Inclusion Team will monitor and evaluate the effectiveness of this Policy alongside with Rewards and Sanctions Policy annually. In case of any new legislation from the UAE government and the United Nations pertaining to Bullying or Cyber Bullying, the policy should be amended in accordancewith the national and international law set forth.