



## THE WESTMINSTER SCHOOL, DUBAI

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

POLICY FOR	BEHAVIOUR
PERSON RESPONSIBLE	Head of Pastoral
REVIEW DATE	June 2020
REVIEWED BY	Assistant Principals and Head of School
APPROVED DATE	
APPROVED BY	
DATE OF NEXT REVIEW	May 2021
RELATED POLICIES	Behaviour Policy, Social Media Policy

Executive Principal / CEO .....



## 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 21<sup>st</sup> 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 risk to students, protect employees and the school from litigation as well as maintain levels of professional standings. The policy is designed to ensure the safe and responsible use of electronic devices by all users, both on the school premises and elsewhere in which the school is represented.

The device will be registered for internet access through the school network using student's **GEMS-BYOD access ID**. Students will be expected to follow Acceptable Use Policy in Social Media, which is printed in the school planner for both parents and students. Furthermore, in line with school BYOD policy, all students will carry **only non-cellular devices**.

The purpose of the 'Electronic Devices / Digital Resources / BYOD acceptable Use' Agreement is to ensure that 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, they 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. 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.

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. 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 Agreement 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 Agreement also establishes rights and responsibilities for all users in 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 origin.
- Recognizing the benefits collaboration brings to education, TWS provides the students with access to web sites or tools that allow communication, collaboration, sharing, and messaging among students. Students are expected to communicate with appropriate, safe, mindful, 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 permission and upload them on social media.
- Alert a teacher or other staff member if I see threatening, appropriate, 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.
- If you see a message, comment, image, or anything else online that makes you concerned for your personal safety, bring it to the attention of an adult (teacher if you're at school; parent if you're 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 online that they would not want parents, teachers, future colleges, 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**.
- **Primary students** are strictly prohibited to bring cellular devices at school.
- Phones can be used only for learning purposes during school hours with **explicit permission** from a teacher.
- If the teacher suspects, misuse of the device then she could take the device and call in the parents to look at the content.
- If students need to contact parents at any time, this is allowed via 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 or suspension from school and school-related activities and disciplinary action will be taken as per the school behaviour policy. The school maintains the right to collect and examine any device that is suspected of causing problems or violation of the policy.

- Mobile phones / other devices are not allowed to be used between lessons.
- Not respecting the values and ethics of the local host culture.
- Smart watches or blue tooth devices are not allowed to be used during examination.
- Any attempts to transmit software designed to compromise the operation or security of the school network in any manner.
- Install and use of Virtual Private Networks within the school network and outside.
- Use school technologies to pursue information on illegal activities.
- Students should not download or attempt to download any software on to school equipment.
- Use or attempt to use another student's hardware, subscriptions, files, or personal information.
- Tampering or experimenting with the school network or equipment, including efforts to bypass the school's Internet filters or proxies.
- Use school technologies in a way that could be personally or physically harmful.
- Attempt to hack or access sites, servers, or content that isn't intended for any personal use.
- Use school technologies to send spam or chain mail.
- Plagiarise content found on line 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 the class or learning in any way and devices should be switched off at 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:
  - nominated private study rooms
  - supervised study lessons
  - library (tablets, kindle)
  - Common 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 organisation 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 6 months' 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 with regards to their own device, keeping it 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 after 3 days / Head of House issues detention/ Email sent to parents.

Stage 3: Device confiscated and passed to Head of House / SLT link. Device will be confiscated for 5 days.

Parents/ Guardian to receive the device after 5 days. Detention issued

Stage 4: Device confiscated for a term and would be returned to the parents / guardian and a warning letter will be issued.

*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 teachers permission.*
- *As source of an attack*

Students need to be fully aware of their responsibilities that is 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.

**Electronic Devices / Digital Resources / BYOD Acceptable Use Policy and Procedures Agreement**

Student name \_\_\_\_\_ Year \_\_\_\_\_ Section \_\_\_\_\_

As a student at **The Westminster School, Dubai**, I acknowledge that I have read through the policy and agree to it.

Student Signature \_\_\_\_\_ Date \_\_\_\_\_

I acknowledge that my son/daughter and I have read the policy and agree to it.

I will instruct my child regarding the importance of following all the guidelines included in this policy.

Parent Signature \_\_\_\_\_ Date \_\_\_\_\_