The British International School of Tunis

BRING YOUR OWN DEVICE (BYOD)
POLICY DOCUMENT

Introduction

At The British International School of Tunis our goal is for all of our students to be fully engaged in learning, achieve their potential, discover themselves, and prepare for the future. We are able to achieve this by exploring all possible means to fully expose our students to information, channels and platforms that provide such opportunities for exploration and self-discovery. In the 21st century learning environment where students use technology (i.e. computers, laptops, tablets and Ipads, etc) they are more likely to be engaged, motivated to learn and exposed to other inexhaustible sources of information and materials other than printed books. As a result, the school aims to utilize technology to improve their achievements by building an environment where students have monitored and regulated access to technology. Computer networks, Internet access facilities, computers and other ICT equipment/devices bring great benefits to the teaching and learning programs at any school if properly managed.

Parents are encouraged to read this document carefully, seek explanations to sections that are not clear to them and sign the attached User Agreement Form before students are allowed to bring a device to school for academic use.

ICT equipment herein referred to are for educational purposes appropriate to this environment, whether it is owned or leased either partially or wholly by the school or owned by the student or permitted for use within the school, and used within or outside the premises with strict adherence to policy rules.

Aim and purpose:

This policy is designed to allow the use of personal devices in school in a way that enhances and supports teaching and learning. It also aims to protect children from harm, minimize risk to the school networks and explain what constitutes acceptable use or misuse of the BYOD policy.

Objectives of the Policy:

To provide awareness and guidelines for what is acceptable or not and the effective use of gadgets in school and of social media, alongside the value of respect in a multicultural environment.

Protect the students from harassment or cyberbullying from social media and/or other internet websites.

Definition of terms:

'Cyber-safety' refers to the safe use of the Internet and ICT equipment/devices, including mobile phones.

'Cyber bullying' is bullying which uses e-technology as a means of victimizing others. It is the use of an Internet service or mobile technologies - such as e-mail, chat room discussion groups, instant messaging, webpages or SMS (text messaging) - with the intention of harming another person. Also refers to posting of photos, videos that humiliates an individual using social media sites or proliferation of any soft materials (e.g. electronic photos, screenshots) that devalues respect and compassion.

The school positions itself at the centre of the learning community, upholding safety for the ongoing development of its students, whilst promoting a safe school environment. We consider an act of bullying based on the definition:
"Whilst Bullying is an intentionally hurtful behaviour that is repeated over time and has an imbalance of power."

Cyber Bullying is defined as:
"The use of electronic communication to bully a person, typically by sending messages of an intimidating, humiliating or threatening nature."

As children are typically reluctant to admit to being the victims of cyberbullying, extra vigilance is essential. **'School ICT'** refers to the school's computer network, Internet access facilities, computers, and other ICT equipment/devices as outlined below.

'ICT equipment/devices' includes but is not necessarily limited to computers (such as desktops, laptops, tablets, notepads, etc), storage devices (such as USB and flash memory devices, CDs, DVDs, floppy disks, iPods, MP3 players), cameras (such as video and digital cameras and webcams), all types of mobile phones, gaming consoles, video and audio players/receivers (such as portable CD and DVD players), and any other, similar, technologies.

'Inappropriate material' means materials that deal with matters such as radicalisation, indoctrination, sex, cruelty or violence in a manner that is likely to be injurious to children or incompatible with a school environment. In particular uploading, forwarding or posting a link to any of the following types of material on social media or other website, will amount to gross misconduct and may lead to dismissal/ permanent exclusion from the school. This list includes but is not limited to:

a. Pornographic materials such as but not limited to, writing, pictures, films and video clips of sexually explicit or arousing nature;
b. Defamatory statement about any person or organization;
c. Material which is offensive (e.g. words, pictures, links), obscene, criminal discriminatory, (e.g. threat, bullying) derogatory (e.g. haters, accusers) or may cause embarrassment to the child and/or the community.

'E-crime' occurs when computers or other electronic communication equipment/devices (e.g Internet, mobile phones) are used to commit an offence, are targeted in an offence, or act as storage devices in an offence.

Permissive/ non permissive:

- Students may not use devices to record, transmit, or post images or video of a person or persons on site during school hours or during school activities, unless otherwise allowed by a teacher.
- Devices may only be used to access computer files on internet sites which are relevant to the classroom curriculum. Students are aware of what areas would be expected to be "BYOD free". Devices are not allowed to be used in potentially sensitive areas such as toilets, bathrooms and changing rooms.
- Students and parents should be aware that devices are subject to search by the Principal, or other authorised person, if the device is suspected of a violation of the school rules. If the device is locked or password protected the student will be required to unlock the device at the request of the Principal or other authorised person
- Printing from personal devices will not be possible at school.
- Using devices to bully and threaten other students is unacceptable. Cyber bullying, Sexting or Up Skirting will not be tolerated. In some cases, it can constitute criminal behaviour if the use of technology humiliates, embarrasses or causes offence it is unacceptable regardless of whether 'consent' was given.
- Students are expected to hand any non-essential devices to invigilators before entering the exam hall. Any student found in possession of any device during an examination will have that paper disqualified. Such an incident may result in all other exam papers being disqualified.
- Any student who uses vulgar, derogatory, or obscene language while using a device will face disciplinary action.
- Students must ensure that files stored on their device do not contain violent, degrading, racist or pornographic images. The viewing or transmission of such images may constitute a criminal offence. Similarly, 'sexting' – which is the sending of personal sexual imagery – may also constitute a criminal

offence.

- The school will not be liable for any loss, damage or theft of a personally owned device on site.

TERMS AND CONDITIONS

Technology Device

All students will be issued with a User Agreement and once signed and returned to school, students will be able to bring in their laptops for educational use. **No student can bring a device to school without a policy agreement signed by both the student and a parent**. **The only acceptable type of device is a laptop.**

1. Use of the school's network will be monitored. Filtering and/or monitoring software may be used to restrict access to certain sites and data, including e-mail.

2. Each student is entitled to come to school with only 1 laptop, which must be pre-registered and configured by the ICT unit and labelled uniquely by the school. This laptop will be used by the students all through their stay at The British International School of Tunis. If for any reason the laptop is to be changed, the replacement laptop must be submitted to the ICT unit for reconfiguration. From time to time, the school reserves the right to add additional monitoring tools to the student's laptop or remove existing ones as the need arises.

3. While deliberate efforts have been made by school to prevent student's exposure to inappropriate content when using technology gadgets, please note that it is **NOT possible to completely** eliminate the risk of such exposure. We cannot filter Internet content accessed by your child from other locations away from school or on mobile devices even though certain measures have been taken to monitor them as much as we can. Similarly, it may be impossible to **COMPLETELY** filter inappropriate content from computer networks including school's internet connection. However, The British International School of Tunis will continue to adjust and strengthen measures in place to keep students safe online and offline.

4. The security and safety of the laptop a student brings to school is the **sole responsibility** of the student. The student must comply with all directives the school provides in relation to the use of the laptop. Without notice, the student must comply with any request to produce the laptop for inspection whenever requested by a teacher, lab technologists, teaching assistants, security staff or any senior member of staff. The School is authorised to collect and examine any device that is suspected of causing technology problems or was the source of an attack or virus infection, or in line with the guidance provided via https://www.gov.uk/government/publications/searching-screening-and-confiscation

5. Devices are uniquely identified on the school's network and tied to the owner's profile. It is advised that personal devices are not shared amongst students. In the event of shared or unauthorized use, the owner of the laptop will bear responsibility for all usage, damages or harm inflicted upon, but not limited to, the school network, staff member, or other students.

6. Although the laptop is the personal property of the student for their educational use, its use within and outside the school whilst still tied to use The British International School of Tunis policy must adhere to the rules and regulations of The British International School of Tunis set out within this policy.

7. The student relinquishes administrative rights and control of the laptop to the school as soon as the Use Policy document is signed. The British International School of Tunis reserves the rights to enable or disable functionalities on the laptop to enforce policies of Safe Use. This may include revoking admin access and granting limited access to the students, which could cause an adverse effect on the pupil's ability to carry out learning orientated classroom tasks, if the use of a device is a requirement or advantage in the subject lessons effected.

8. When at school, engaging in chats or downloading files from the internet is strictly forbidden, unless forming part of a legitimate class activity, guided by the teacher of that lesson.

9. Laptops are expected to come preloaded with Microsoft Windows Operating System (Windows 10 or later - Professional or Enterprise edition), Basic Productivity applications such as Microsoft Office Suite 2016, 2019, or Office 365, Chrome Web Browser and VLC player. We do not recommend any specific anti-virus but the system must have Windows Defender enabled and is regularly updated.

10. Students can use Earphones and other audio/video accessories to listen to audio from their laptops, but earphones MUST not be used without express permission from the teacher during lessons.

11. Use of VPNs, identity cloaking tools, or the use of alternate sources providing connectivity outside of the school network of any kind is **expressly prohibited**.

12. Students are not allowed to use other sources of internet connection other than the one provided by the school. It is prohibited for students to use hotspots, personal wifi, or share other sources of online connectivity without authorization from the school.

13. The British International School of Tunis reserves the rights to adjust policies guiding the laptop use to better safeguard the students and the school without consulting the students or parents before such changes are made.

14. In the event of malfunction that requires complete system overhaul, the student is expected to present the system again to the ICT unit for assessment and reconfiguration. This may involve some financial commitment if new licenses are required.

15. Acceptable laptops must meet the following requirements:
    a. Must run Microsoft Windows 10 or later Operating System. We will update this policy to allow any other Operating Systems when we support Microsoft alternatives.
    b. Must have a minimum of 4GB RAM. 6GB to 12GB is recommended
    c. Must have a webcam, microphone and audio speaker
    d. Not more than 15'' screen size

16. The school may monitor and audit its computer network, Internet access facilities, computers and other school ICT equipment/devices or commission an independent forensic audit. Auditing of the above items may include any stored content, and all aspects of their use, including e-mail. This can be extended to the student's laptops under the BYOD policy.

17. If cyber-safe practices are disregarded, not followed, or not respected, the school may inform my parents/caregivers. In serious cases, the school may take disciplinary action against the perpetrator. The family may be charged for repair costs. If illegal material or activities are involved or e-crime is suspected, it may be necessary for the school to inform law enforcement agencies and hold securely personal items for potential examination by them. Such actions may occur even if the incident occurs off-site and/or out of school hours.

Software, Copyright and Intellectual Property

Each laptop will be joined to the The British International School of Tunis network. Approved monitoring software will be installed and the device configured for use on the school network. Administrative privileges to the laptop will be limited and/or restricted depending on the current laptop use policy, which will continually be adjusted based on antecedents. Software installed on the laptop by the school is copyright protected and must not be distributed, maliciously altered or deleted without written permission from the schools' ICT unit.

Games, Music & Non-School Applications

The British International School of Tunis does not object to the installation and use of non-school games and other applications that could benefit the student academically, but they are subject to the following:

1. Are appropriately licensed (i.e. they do not breach copyright and intellectual property laws this includes video and music downloads)

2. Are ethically and morally acceptable (including consideration of school appropriateness, age appropriate ratings and privacy issues)

3. Do not interfere with the school's network

4. Do not interfere with the learning program on the laptop.

5. Games must be installed with the assistance of the school ICT department and with the knowledge, approval and declaration of the application/program to the school.

Personal Safety Responsibility

- Students should ensure that anti-virus software is kept up to date. This happens automatically when they connect to the school network.
- Students are to always bear in mind that safety online is more than 70% personal and less than 30% technology. Try to avoid tendencies that compromise your safety.
- Viruses, ransomware and spywares can get into your system through removable media such as CDs, DVDs, and USB memory sticks, e-mails, the Internet (including web browsing, FTP programs and chat programs/rooms).

Helpful guide

- Do not open any files attached to suspicious or unknown emails,
- Do not share your personal information on the internet. Use code names if you must join a chat room. Do not share location, travel status, current city, school location, family information etc online.
- Exercise caution when downloading files from the Internet,
- Do not accept requests from people online especially if you are not expecting their requests.
- Delete chain and junk emails. Do not forward or reply to any of these,
- Never reply to Spam,
- Hundreds of viruses are discovered each month. Run your virus scan regularly,
- Avoid indiscriminately loading non-standard software onto the laptop as it can result in infection by viruses and spyware are common causes of laptop failure.

Student Roles

1. Students are personally responsible for context published into social media tools. Be aware that anything published will be public for many years.

2. Don't escalate heated discussions. Be respectful, and quote facts to lower the temperature and correct misrepresentations.

3. If you feel even slightly uneasy about something to publish, then it should not be posted. If in doubt, always discuss it with parents or teachers prior to posting.

4. Always consider others' privacy and avoid discussing topics that may be derogatory e.g. politics, religion, personal matter etc.

5. Keep the laptop locked when not in use. This reduces the risk of someone else performing actions using your username, which may result in the punishment of the laptop owner instead of the perpetrator.

6. Avoid publishing your contact details where they can be accessed and used widely by people you don't know and never publish anyone else's contact details.

7. Observe the activity on the site for a while before sharing your contributions/opinions of the content and any 'unwritten' rules that other contributors might follow.

8. Activity inside the classroom on social media websites during school hours should complement and/or support your role as students.

9. Seek the advice of the ICT Department to ensure safety awareness.

10. Don't bully, intimidate or harass others. Cyber bullying can be a criminal offense. Status which damages a person's reputation is considered harassment and can be punishable by law authorities.

11. Do not lend, or allow use of the laptop by anyone else, unless absolutely essential. If there is a requirement to do so, then a member of staff must be made aware and permission must be provided in advance.

12. Students should bring their laptops each day fully charged as classrooms have limited facilities to recharge laptops. Students are not allowed to plug chargers and laptops anywhere in the school, unless special permission is granted in advance.

Parental Roles

1. Know what your child doing online.

2. Consider monitoring your child's social media accounts.

3. Understand the challenges posed by technology (e.g. Mobile Phones, IPod, etc.)

4. Be aware of bullying in social media specifically group chat box.

5. Parents and students should report cyberbullying cases in school where it occurs, keep a record and report to the Guidance Centre/Head of Key Stages/Form Tutors.

Strategies to help keep The British International School of Tunis safe

Parents/caregivers play a critical role in developing knowledge, understanding and ethics around their child's safety and safe practices for themselves and the people around them regardless of the time of day. Being cyber-safe is no exception and we encourage you to discuss with your child the following strategies to help us stay safe when using ICT at school and after formal school hours.

1. If I have my own username, I will log on only with that username. I will not allow anyone else to use my account.
2. I will keep my password complex and private.
3. While at school or in a school related activity, I will inform the teacher when I need to use the laptop.
4. I will use the Internet, e-mail, or any ICT equipment only for academic purposes, not to be mean, rude or offensive, or to bully, harass, or in any way harm anyone else, or the school itself, even if it is meant as a joke.
5. I will not do anything to bypass security or content filtration measures put in place by the school to monitor the network users.
6. I will not uninstall, block, disable or interfere with the tools installed on my laptop to monitor my use of the laptop.
7. I will use my laptop only at the times agreed to by the school during the school day.
8. I will go online or use the Internet at school only when a teacher gives permission and an adult is present.
9. While at school, I will:
    1. Access, download, save and distribute only age appropriate and relevant materials.
    2. Report any attempt to get around or bypass security, monitoring and filtering that is in place at school.
    3. If I accidentally access inappropriate material, I will:
        a. Report the incident to a teacher immediately.
        b. Not show others
        c. Turn off the screen or minimize the window
10. To ensure my compliance with copyright laws, I will download or copy files such as music, videos, games or programs only with the permission of a teacher or the owner of the original material.
11. My laptop and other accessories (such as USB/portable, earphone, etc) that I bring to school or a school related activity, also is covered by the User Agreement. Any images or materials on such equipment/devices must be appropriate to the school environment.
12. Other than my laptop, I will respect and treat all ICT equipment/devices with care. This includes:
    a. Not intentionally disrupting the smooth running of any school ICT systems
    b. Not attempting to hack or gain unauthorised access to any system including other students or staff accounts.
    c. Following all school cyber-safety strategies.

d. Reporting any breakages/damage to a staff member.

Internet Usage

Students are only allowed to access the Internet through the School's network provided for students use while on site. This will be monitored and subject to strict filtration and other restrictions and limitations could apply to the student's internet link.

Consequences

Overall, consequences of violations will be finally determined by the Head of School.
Where there is a contravention of this policy, consequences may include:

1. Temporal or permanent ban from bringing in laptops into the school.
2. Temporal or permanent seizure of the laptop. (permanent seizure here refers to seizure until graduation or exit from the school).
3. Other sanctions may be imposed as appropriate and as determined in consultation with the ICT unit and the school management.

Please read this page carefully to check that you understand your responsibilities under this agreement.

Return the signed User Agreement to the school.

I understand the content of this document and hereby assure that I will:

1. Follow the cyber-safety strategies, policies and instructions whenever I use the school's ICT gadgets, my laptop and any other accessories. This may include relinquishing administrative privileges to my device to the school for the time I will use the device at The British International School of Tunis.
2. Respond to any breaches on my device in a calm and appropriate manner by first calling the attention of my teacher and immediately drawing the attention of the ICT unit.
3. Avoid any involvement with materials or activities that could put at risk my safety, or the privacy, safety or security of the school or other members of the school community.
4. If I have been involved in the damage, loss or theft of ICT equipment/devices belonging to the school or any other member of the school community, I and/or my family may be required to pay for the repairs or replacement.

The British International School of Tunis will ensure to provide members of the school community with cyber-safety orientation designed to complement and support the Use Agreement initiative. Welcome enquiries at any time from parents/caregivers/legal guardians or students about cyber- safety issues.

Student Information Technology User Agreement

STUDENT FORENAME: .... STUDENT SURNAME: ....
(Please Print) (Please Print)

We have read and understood this Computer User and Cyber-safety agreement and we are aware of the school's initiatives to maintain, care for, use and manage computers in a cyber-safe learning environment. We understand that failure to comply with the Laptop User Agreement could result in not being able to use laptops during classes, and or Prep, seizure, or more severe sanctions as stated in this document.

My responsibilities as a Parent/Caregiver include:

1. Reading this agreement carefully and discussing it with my child so we both have a clear understanding of our roles in using computing devices in learning.

2. Ensuring this User Agreement is signed by my child and by me and returned to the school

3. Encouraging my child to follow the cyber-safe rules.

4. Contacting the school if anything suspicious flags up with my child's access to technology.

This agreement will remain in force as long as your child is enrolled at this school.

PLEASE RETURN THIS PAGE TO SCHOOL AND KEEP A COPY FOR YOUR REFERENCE.

I have read the Laptop User Agreement. I understand my responsibilities regarding the use of the laptop and the Internet. In signing below, I acknowledge that I understand and agree to the Laptop User Contract. I understand that failure to comply with the Laptop User Contract could result in not being allowed to bring in my laptop to school.

....
Student's Signature Date

....
Parent's Signature Date

……………………………………………………
Parent's Name (Please Print)