2b. Computing Acceptable Use Policy

Executive Principal	Head of Education
Karyn Walton	Dr Laura Hillman
February 2024	Oct 2025
	
Policy Ref:	BIST2025 CAU-Vr.3
Next Review Due:	August 2026

Contents

Role of Technical Staff	3
Security	3
E-mail	3
Internet	4
Holding of Information/Data	4
Internal Communications	5
Treating Other Users with Respect	5
E-Safety Guidelines	5
ICT & Computing Science in the Curriculum	6
Role of Academic & Support Staff	7
Managing E-Safety	7
Misuse	7
Involvement with Parents & Guardians	8

This acceptable use policy is written for both staff and pupils. It does not exclusively restrict itself to the IT and computing domain but addresses copyright, privacy, responsibility, safety and respect in both real and virtual contexts.

Electronic devices, such as computers, smart devices, mobile phones with cameras, and laptops, and the Internet play an increasingly important role in all our lives. Such technology is extremely useful and allows for ease of communications, educational research and resource procurement, all of which assists us in providing the best education possible to our pupils. Whilst these communications provide unrivalled opportunities, they also bring risks. It is therefore important that all staff are aware of how to use such systems safely and how to avoid becoming vulnerable to a range of risks, including fraud, theft, harassment and embarrassment.

The British School of Tunis (BIST) expects and requires the responsible use of electronic devices and the Internet by all colleagues. This document sets out the School's guidance to staff on the safe use of electronic devices and the Internet.

Role of Technical Staff

Our technician has a key role in maintaining a safe technical infrastructure at BIST and in keeping abreast with technical developments. They are responsible for the security of the School hardware system, our data and for training staff in the use of ICT. They monitor the use of the Internet and emails and will report inappropriate usage to the Executive Principal. However, all staff are responsible for the safe use of their own personal devices. If you have any concerns or need any advice, please contact the IT Lead who will try to help as soon as possible.

Security

It is important that access to your electronic devices and areas of the School IT system is limited. Therefore, members of staff are advised to secure all hardware when not in use. It is critical that systems are password protected and that this password is not given to anyone else. Computers should be set up so that they self-lock after a certain time when not in use (15 minutes is recommended). Passwords should be changed on a regular basis, ideally monthly.

We also recommend that individual names, addresses, passwords, mobile phone numbers and other personal details are kept secure and not shared. When working on school business, staff and pupils should only use their school email address.

E-mail

E-mail can be used for internal and external communication though it is not expected to replace personal interaction; staff and pupils are expected and encouraged to choose the best method of communication in any given situation. Each member of staff is responsible for checking their emails daily (during working days) and responding accordingly.

Users are responsible for understanding the nature of data contained in any correspondence that they transmit and must ensure the information does not place the school in violation of any laws, regulations or bring the reputation of the school into disrepute. Email must not be used for sending confidential or sensitive information without the specific consent of the Principal. All staff should be aware that emails and the Internet cannot be guaranteed to be secure.

All messages generated on or processed by the school electronic systems, including back-up copies, are the property of the school. All users should note that use of email is subject to monitoring by the school; staff should have no expectation of privacy for any use of the schools systems including personal emails. No member of the school may use the email system for the operation of a personal business or for dissemination of chain letters, junk email or similar correspondence.

E-mail is not without its dangers. Some are frauds requesting confidential information (normally pretending to be from banks) whilst others contain viruses which are aimed at damaging private or business systems. Therefore, it is critical that pupils and staff only open emails from known sources and never provide confidential information via the Internet to sources that have not been checked. If in doubt, please report all such emails to the IT team and do not open them first.

Colleagues are reminded that the storage of emails and attachments takes up significant disk space if users do not manage their mailboxes by deleting old messages or those no longer required. This significantly slows down the system, as does the storage of large numbers of pictures/video/music files. The IT Lead will advise you when your mailbox is nearing capacity and requires reviewing.

Internet

Internet access is provided for school/work purposes, and although occasional personal use of this system is permitted, such use must not adversely affect the work of any individual or the business of the school. Unreasonable personal use will be considered a behaviour/disciplinary offence. The School reserves the right to conduct such monitoring and searching of Internet use (sites accessed, and time spent) as it thinks appropriate for the protection of the school, its staff or pupils. This will normally only take place when the School has a reasonable belief that some infringement of the policy is taking place.

The Internet must not be used to access or distribute any material which is or may be thought to be pornographic, sexual in nature or otherwise inappropriately offensive. Breach of this provision will be considered a serious disciplinary offence and will be dealt with in accordance with the laws of Tunisia.

Without specific instruction from the IT Lead and the Executive Principal, no one should download or open any executable program file. To do so creates an unacceptable risk of harm to the School's network. Breach of this provision will be considered a serious behaviour/disciplinary offence. The downloading or storing of material (including software) protected under copyright law is expressly forbidden without the prior permission of the IT team and the Executive Principal.

Those who possess their own desktop computer or laptop should also be aware that any misuse of that computer which brings the School into disrepute may also result in disciplinary action up to and including suspension, exclusion (pupils) or dismissal (staff.) Those who possess their own computer may not transfer any files from their computer to the school system unless they have agreement from the IT Lead and the Executive Principal that they have adequate virus protection software installed on their computer. Pupils (BYOD) and staff are responsible for the purchase and upgrading of software for their own desktop/laptop computer.

Holding of Information/Data

Pupils and members of staff should not hold any personal data on school systems without the permission of the IT Lead and the Executive Principal. Additionally, members of staff should not hold personal data about pupils without their permission and this should be

minimised for essential school use only (see the GDPR Policy). Information such as telephone numbers should only be held for limited times (such as the duration of a school trip) and then deleted.

Photographs of pupils can be taken for School promotional material and parents can opt out of this as part of the school contract. However, this generally applies to groups of pupils. If taking pictures of individual pupils, a member of staff should get permission from the parent first and then store the picture on the school system. Pictures of pupils must not be stored on private computers or mobile phones.

See GDPR Policy for more details.

Informal Communications

The last decade has seen an exponential increase in the use of informal communications means and social networking sites. These sites and apps can be an excellent way of maintaining contact with friends and professional networking, but they do come with risks. It is important to remember that once information or images are placed on these forms of communications it is unlikely to remain private and that it is likely to be available for viewing for a long time (even if you think you have removed that item). Therefore, BIST offers the following advice:

- Only join networks that you understand.
- Only allow people to join your network that you know well and trust (once someone is in your network, they can copy any of your posted information).
- Do not use social networks to communicate with current pupils.
- Do not post anything on a site that could cause you any embarrassment if read by someone who was not intended to read/see it.
- Ensure that your personal settings are correct for the information that you wish to have as public knowledge (being on many social network sites allows you to be “googled” and information about you obtained.)
- The use of the school name and logo cannot be used on private social media without the express permission of the Executive Principal.
- Pupils or staff who leave BIST should immediately remove any direct connection to the school name or logo if they previously had permission to use this.

If you have any concerns or questions, please take advice from the IT Lead or the Executive Principal.

Treating Other Users with Respect

BIST expects pupils and staff to treat other users of electronic communications with the same standards of consideration and good manners as they would during face-to-face contact. It is important to remember that emails and texts are written records that can easily be copied to large numbers of people and could be used in a court of law or printed media. Therefore, pupils and staff are advised to take time to consider what they are writing and do so in a professional manner. BIST also expects a degree of formality in communications between colleagues, staff and parents or pupils. The School would not normally expect staff to communicate with pupils by SMS/text, WhatsApp or mobile phone unless for School business.

E-Safety Guidelines

Technology plays an enormously important part in the lives of all young people. Sophisticated smart-phones, tablets and other portable devices provide unlimited access to the Internet, to SMS messages, to blogging services (such as Twitter), to communications technology (such as Zoom, Google Meets or WhatsApp), to wikis (collaborative web pages), chat rooms and social networking sites (such as Facebook) and video sharing sites (such as YouTube). The number of applications of this type is vast and ever changing.

This revolution in technology and communications gives young people unrivalled opportunities. It also brings risks. It is an important part of our role at BIST to teach our pupils how to stay safe in this environment and how to avoid making themselves vulnerable to a range of risks, including identity theft, bullying, harassment, grooming, stalking and abuse. They also need to learn how to avoid the risk of exposing themselves to subsequent embarrassment or reputational damage which may cause them harm years from now.

ICT & Computing Science in the Curriculum

Information and Communication Technology (ICT) and Computing Science have transformed teaching and learning. In the past, it was commonplace for the resources used by pupils in the classroom to have been carefully chosen or prepared by the teacher and determined by curriculum policies. Use of the Internet, by its nature, provides access to information which has not been selected by the teacher. Whilst pupils will often be directed to sites which provide reviewed and evaluated sources, at times, they will be able to move beyond these, to sites unfamiliar to the teacher.

ICT is embedded across the curriculum at BIST, enabling members of the community to access information from anywhere on Earth. This has many benefits for both teachers and pupils, which include;

- Rapid and cost-effective world-wide communication,
- Access to a wide variety of educational resources including research materials, libraries, art galleries and museums.
- USe of programmes within the curriculum i.e. Adawati for Arabic.
- Gaining an understanding of people and cultures around the globe.
- Access to new curriculum materials, experts' knowledge and practice.
- Exchange of curriculum and administration data with others.
- Enhanced literacy skills, particularly concerning reading, critical appraisal and dissemination of important and cogent facts to others.

However, the scope and potential to access such a huge range of material requires education and caution. All our pupils are taught how to research on the Internet and to evaluate sources. For example, websites exist which appear to provide serious, impartial, historical information but are actually sources of intolerant or illegal propaganda. Some free, on-line encyclopaedias do not evaluate or screen the material posted on them. BIST pupils are educated into the importance of evaluating the intellectual integrity of different sites, and why some apparently authoritative sites need to be evaluated for content, source and inherent bias; alongside remaining safe online.

BIST endeavours to embed e-safety messages across the curriculum whenever the internet and/or related technologies are used. These messages will be appropriate to the age of the

children being taught. The School provides opportunities within a range of curriculum areas to teach about e-safety. Educating students on the dangers of technologies that may be encountered outside BIST is done informally when opportunities arise and as part of the e-safety curriculum.

Role of Academic and Support Staff

BIST recognises that blocking and barring sites is no longer adequate to completely protect our pupils. Therefore, we need to teach all of them to understand why they need to behave responsibly if they are to protect themselves. All teaching staff have a role to play in achieving this aim. All teaching staff receive training in e-safety issues. Together, they ensure that all year groups in the school are educated in the risks and the reasons why they need to behave responsibly online.

Managing E-safety

Should staff or pupils encounter or access anything unsuitable or damaging, they must report it immediately to teachers, line managers or the Executive Principal. All internet activity within school is monitored and filtered. Whenever any inappropriate use is detected, the ICT Lead is notified, and the incident will be followed up.

The teaching of e-safety focuses on helping children to recognise inappropriate content, conduct, contact and commercialism and helps them learn how to respond or react appropriately. Students are made aware of the impact of online bullying (refer to the Anti-Bullying and Cyber-Bullying Policy) and know how to seek help if they are affected by these issues. Pupils should be encouraged to seek advice or help if they experience problems when using the internet and related technologies.

Pupils at BIST will have supervised access to the internet. If Internet research is set for homework, staff will routinely remind pupils of their e-safety training. Parents are encouraged to support and supervise any further research.

BIST allows staff to bring personal mobile phones and devices to School for their own use during designated break times outside of the classroom. The school is not responsible for the loss, damage or theft of any personal mobile device.

BIST does not permit the pupils to access their private accounts on social or gaming networks at any time during the school day. The school also strongly discourages children from using age-inappropriate social networking outside of School. Should the staff be made aware of incidents or activities on social networks which have a direct effect on children's behaviour or attitudes at BIST, then we reserve the right to act regarding their accounts. This may include discussions with parents, information letters or reporting the child's access to the respective organisations/companies. Also refer to the Anti-Bullying and Behaviour Policies.

Misuse: Statement of Policy

BIST will not tolerate any illegal material and will always report illegal activity to the appropriate body in line with Tunisian regulations. If the School discovers that a child or young person is at risk as a consequence of online activity, assistance may be sought from the relevant authorities. We will impose a range of sanctions on any pupil who misuses technology to bully, harass or abuse another pupil in line with our anti-bullying policy.

All users should report any accidental access to inappropriate materials. The breach must be immediately reported in writing to the Executive Principal. Staff must be aware that negligent use or deliberate misconduct could lead to disciplinary action. Deliberate access to inappropriate materials by any user will lead to the incident being logged and investigated The Executive Principal will lead the investigation in accordance with the staff disciplinary policy.

Involvement with Parents and Guardians

BIST seeks to collaborate closely with parents and guardians in promoting a culture of e-safety. We will always contact parents if we have any worries about a pupil's behaviour in this area, and we hope that parents will feel able to share any worries with the School. We recognise that not all parents and guardians may feel equipped to protect their child when they use electronic equipment at home. Therefore, the school is happy to provide workshops for parents during the academic year and advise on such issues if a parent requests it.

AI Use

Purpose:
To ensure the safe, responsible, and ethical use of Artificial Intelligence (AI) tools and technologies in the school, supporting learning while protecting pupils and staff from associated risks.

Scope:
Applies to all pupils and staff when using any AI tools or programs, including ChatGPT, automated writing or data analysis tools, educational robots, and similar technologies.

Responsible Use:

- AI must not be used to produce illegal, offensive, misleading, or harmful content.
- Users must verify the accuracy of AI-generated information and not rely on it as the sole source.
- Pupils should use AI as a learning aid, not as a means to cheat or bypass critical thinking.

Data Protection:

- No personal or sensitive data may be entered into online AI tools without explicit permission.
- AI use must comply with school data protection policies (GDPR and relevant legislation).

Supervision and Monitoring:

- AI use within school must be supervised by teachers or designated staff.
- The school monitors usage to ensure compliance with policies and to protect users from inappropriate content.

Training:

- Pupils and staff will receive guidance and training on safe, ethical, and effective AI use.

Reporting Issues:

- Any inappropriate AI use must be reported immediately to the Executive Principal.
- Violations will be handled in accordance with existing staff code of conduct, school behavior and disciplinary policies.