# British International School and Montessori Education

## INFORMATION COMMUNICATION TECHNOLOGY AND DIGITAL LEARNING RESOURCES POLICY

| | | | |
|---|---|---|---|
| **Approved by:** | The Governing board | **Date:** | 04/07/2022 |
| **Last reviewed on:** | 04/07/2022 | | |
| **Next review due by:** | 04/07/2025 | | |

## INTRODUCTION AND SCOPE

The British International School and Montessori Education, Freetown aims to foster appropriate use of digital technologies and to establish attitudes and behavior that will protect the students, the school and it's I.C.T. resources, and the BIS community as a whole.

This Policy consists of two main parts:

i. Acceptable use of Information Communications Technology (I.C.T.) at BIS: Specific rules relating to the use of the school's IT systems and resources

ii. Guidelines for the use of digital technologies: General advice relating to the use of all digital technology, including social media, both within and outside the school environment

The technologies and resources covered include but are not restricted to:

- Shared classroom technology
- Local and wireless network resources
- Cloud based systems and resources provided by BIS
- Use of other digital resources
- Data protection and security
- Privacy and e-safety

All students and parents are expected to read the Acceptable Use Policy, below

## Acceptable Use of I.C.T. Policy

BIS's I.C.T. resources, including Internet access, are provided primarily for educational purposes. Students are responsible for good behavior and judgement in this digital environment just as they are in the physical school environment.

Please remember that access to BIS's I.C.T. resources is a privilege, not a right, and that access requires responsibility and prior permission. Individual users of the school's resources are responsible for their behavior, actions and communications.

## Shared Classroom Technology

The school provides a wide range of classroom technology resources including online learning programmes, laptops, workstations and mobile devices.

Students are expected to treat these resources with care and respect. Damage to any equipment should be reported, as soon as it is detected, to the class teacher.

Procedures for the loan and return of shared resources should be strictly followed.

Students must not change physical connections or alter in any way the configuration of the classroom technology, without the authorization of the I.C.T. Teacher and then only on the clear understanding that it will be returned to the original settings after use.

## Local and Wireless Network Resources

Access to the local network and the wireless network is permitted through generic accounts held by the school staff. In either case, accessing the network implies that students have read and understood our Acceptable Use of I.C.T. Policy.

This Policy is in place to protect our students and our network. Any attempt to bypass the access permissions set by the school to internal or external locations will be considered a serious breach of this Policy. Under no circumstances should any student install, or attempt to install, any software or change or adjust any of the security permissions for any device.

## Cloud-based Systems and Resources

The school aims to provide a wide and constantly evolving collection of online systems and resources, many of which require users to login with personal account names and passwords.
Such account details should be carefully protected and should not be divulged to, or shared with, any other person except teachers and parents.

It is extremely important to ensure that students are properly logged out from any secure system that are accessed through a shared BIS device.
If in the event that another user has left a personal account open, students are expected to sign out of the account immediately or inform a teacher.

Sending an inappropriate or unauthorised message from another user's account is considered a serious breach of the Acceptable Use of I.C.T. Policy.

Please do not synchronise personal data from an online system on any shared device.
Should a student suspect that one or more of their personal accounts may have been compromised they must inform a Teacher immediately.

## Use of Other Digital Resources

The following points relate specifically to use of the internet and social media and are intended to cover the areas where there might be serious, and possibly legal implications for the student and/or the school.

Students should:

- Respect minimum age limits for accessing social network sites (E.G: age 13 for Facebook)
- Not intentionally access, transmit, copy, or create material that would be considered inappropriate. This includes but is not limited to, messages or materials that are pornographic, threatening, rude, discriminatory, or meant to harass
- Respect and protect the intellectual property of others. Not infringe upon copyright or intellectual property rights. This includes, but is not limited to making and/or distributing illegal copies of music, games, or movies
- Not use the resources to further any acts that are criminal
- Not to use the resources to send spam, chain letters, or other unsolicited mass mailings
- Not buy, sell, advertise, or otherwise conduct business through BIS resources or systems
- Not commit acts of plagiarism. Always give full acknowledgement of the sources for any materials or ideas submitted as course work or assignments

## Personal Electronic Devices

Students are not permitted to bring mobile phones, tablets, laptops, music devices, electronic games or other similar devices to school unless (i) for educational purposes and (ii) with permission from a member of staff. With

or without permission: BIS cannot and will not except any responsibility for any loss of, theft of and/or damage to students' personal electronic devices and/or other valuables.

## Online Learning Subscriptions

Students of almost all year groups at BIS are subscribed to a plethora of online learning and sharing platforms. At the time of compilation of this Policy these platforms include:

- IXL
- Literacy Planet
- Purple Mash
- Education City
- Kognity
- SENECA
- Literacy Planet

As websites specifically created for and directed towards schoolchildren, the above list conforms to the standards expected by BIS. However, parents are strongly encouraged to play a part in their child's online usage opportunities at home.

## Data Protection

Students should:

- Use only assigned accounts to access BIS systems and/or resources
- Not attempt to view, use, or copy passwords, data, or networks to which they are not authorised
- Never attempt to install unauthorised software
- Report any suspected violations or vulnerabilities immediately to the Teacher
- Observe all network security practices, as posted
- Not delete, edit or move data or other resources that do not belong to them

## Privacy and E-safety

These points on good e-citizenship and e-safety are listed here for emphasis.

Students should:

- Respect and protect the privacy of others. Do not post online or otherwise distribute private information about others or themselves
- Report any incident which gives them any cause to feel threatened / uncomfortable immediately

## Supervision and Monitoring of I.C.T. Resources

School and network administrators monitor the use of I.C.T. resources to help ensure that use is secure and conforms to the school's standards. BIS reserves the right to examine, use and disclose any data found on the school's networks or information systems in order to further the health, safety, welfare, discipline or security of any student or other person, or to protect property.

BIS can and will monitor user accounts and internet access and keep logs of inappropriate activities. Please use our I.C.T. resources thoughtfully and responsibly. We may also use this information in disciplinary actions, and will, where appropriate, furnish evidence of crime to law enforcement agencies in line with Sierra Leone and international law.

## Consequences for Violation

Violations of any of these rules and expectations may result in disciplinary action, including the loss of a student's privileges to use the school's I.C.T. resources, suspension and / or expulsion.

## Guidelines for Use of Digital Technologies

New digital technologies mean that access to I.C.T. resources at BIS extends beyond the physical boundaries of the school and that the distinctions between school and home are not as clear cut as they once were. Please read carefully the following guidelines and notes on the use of digital technologies as they apply to Employees, students, parents and the wider BIS community (known hereon in as the 'BIS Community'):

1. Classroom Use of Social Media

The BIS Community is expected to refrain from accessing social network sites during school hours unless expressly asked to do so as part of a class activity. Employees are required to limit class activities to approved online tools.

2. Classroom Use of Other Public Online Applications

Where online tools are used to share information with students or about the class or school, appropriate care must be taken regarding content and security. Specifically, no photos should include names of the children in the photos and no student / parent names or contact details should be displayed.

3. Contributions to Social Media and Online Forums

When posting messages to BIS social media forums or blogs, the BIS Community should use appropriate etiquette and avoid posts or responses that could be misinterpreted, upset or offend any persons.

4. Social Media Relationships with Students, Alumni and Parents

Employees are instructed not to initiate or accept social media 'friend requests' from current students (of any age) or former students under the age of 18.

Employees and parents of current / prospective students are discouraged from "friending" each other due to the inherent conflicts of interest that may arise.

5. Social Networking Sites

Social networking sites usually have a minimum age for membership. Employees who see children under this age using these sites are asked to report the incident to the School Leadership Team.

6. Privacy Settings

On most sites, privacy settings can be changed at any time to limit searchability and access to profiles. Students and Employees should be prudent in allowing access to their online content, consistent with other requirements of this Policy.

7. Use of BIS Email Accounts

Messages sent from BIS email addresses should not include content that would reflect poorly on the sender or the school.

8. Data Protection

Students must ensure that their online accounts are protected with strong passwords. A 'strong' password may include a lowercase letter, and uppercase letter, a symbol and a number.

Passwords for accounts such as email and social media should not be shared with anyone except parents. Passwords for accounts such as subscribed BIS online learning and sharing platforms (E.G: Literacy Planet) should not be shared with anyone except parents and teachers.

Passwords should be changed immediately if there is any reason to believe an account has been or may be compromised (or shared) by another students for example.

9. E-safety

The BIS Community should ensure that they understand all the risks that digital technologies create and have clear strategies in place to minimize the impact of these risks.
E-safety is taken very seriously at BIS. It is incorporated into some of the activities that will be led by the PTA School Wellbeing sub-committee and there will workshops and presentations that parents can attend where they can learn more and discuss these issues with teachers.

10. Emerging Technologies

As new technologies and technology initiatives emerge, it may be necessary to make changes to this Policy. Where such changes are significant, prior to the policy review date as listed below; these will be communicated directly to students and their parents.

## Further Information, Guidelines and Regulations

BIS Employees are directed to the school's Communication Policy for further information, guidance and regulations, and in particular; to the following relevant chapters:

- Electronic Devices
- Photography, Videoing, Voice Recordings and Other
- WhatsApp / Email Communications
- BISME Wi-Fi and Electronic Devices
- Social Media
- Sensitive Information