School Computer, Personal Computer, Mobile Phone, & Internet Use Policy

Purpose

The purpose of this policy is to provide clear guidelines to ensure the safe and responsible use of school computers, the IBSB Wi-Fi, and personal digital devices used in the capacity of the computer.

IBSB Computer Use

Individuals who are provided access to IBSB computer facilities assume responsibility for their appropriate use. IBSB expects individuals to be careful, honest, responsible, and civil in the use of computers and network.

The use of IBSB computing resources is for purposes related to the School's mission of education, research, and public service and shall not be used for personal purposes in any way.

User Responsibilities

- Individuals assume personal responsibility for the use of their accounts and should not disclose their passwords to anyone, both computer and photocopier. Any written user authentication forms must always be out of site and kept separate from the computer.
- Individuals are forbidden to use other individual's accounts. Everyone is responsible for his/her given account.
- Computer facilities have tangible value. Consequently, attempts to circumvent accounting systems or to use the computer accounts of others will be treated as forms of attempted theft.
- Individuals must Log Off / Sign Out every time they are leaving the computer they've just used. Do not "lock" it! Leaving yourselves logged in on different computers in the same time will lead to document loss and unsaved data.
- Installation of programs / applications without the consent of the IT Department is strictly forbidden.
- The introduction of data or programs which in some way endangers computing resources or the information of other users (e.g., a computer worm, virus, or other destructive program), or which infringes upon the rights of other IBSB (e.g., inappropriate, obscene, pornographic, bigoted, or abusive materials) is prohibited.
- Any hardware modification without the consent of the IT Department is strictly forbidden.
- Individuals may not attempt to circumvent security systems or to exploit or probe for security holes in IBSB network or system, nor may individuals attempt any such activity against other systems accessed through IBSB's facilities. Execution or compilation of programs designed to breach system security is prohibited.
- The compilation or redistribution of information from IBSB directories (printed or electronic) to third parties is forbidden.
- Users are forbidden to use the school's computers for their own personal use. All use must be related to pre-approved (by adult staff employed by the school) school activities.
- IBSB is entitled to remove any data and programs that are found to be inappropriate, as defined above and/or to terminate the computing privileges of any user who violates the policies outlined above.
- Individuals must not eat or place any food or drinks near computers.

- Individuals are expected to abide by the rules and policies outlined in this document and to consult an official of the IBSB group prior to any activity that would appear to violate any of them. Failure to do so may result in disciplinary action.

Mobile Phone & Smart Watch Use

The use of mobile phones and smart watches in both the Primary School and Secondary School is forbidden during school hours, including during break times and lunchtime, unless sanctioned within a lesson for a particular monitored educational purpose.

The reasons for this policy are:

1. That mobile phone use has been identified as a form of anti-social behaviour reducing the level of face to face communication between students, which the school actively promotes.
2. Research indicates that unmonitored phone use is distracting and is having a negative impact on learning
3. Phones have been used to take photos of students and staff and then posted on social media, which is strictly forbidden at IBSB.
4. The content accessed by students on campus with personal phone cannot be monitored and controlled and as such this poses a health and safety risk to all students

The only exception to this rule is where students are given permission to use a phone for an emergency phone call, or for educational use in a classroom. Earphones may be used for different purposes as long as they are plugged into a computer.

Sanctions for unauthorised Mobile Phone Use

1st Time Offence
If phones or smart watches are seen out or used during school hours without the express permission of a member of staff, they will be collected and held in a secure location and returned at the end of the school day.

An email will be sent home on the day the phone is collected to notify parents that the phone has been collected, asking the parents to speak with their child to ensure this is not repeated.

2nd Time Offence
If the phone is collected again within the same week, the phone will again be collected and returned at the end of the school day. Parents will be informed that due to the phone being collected twice in one week the student will either be required to leave their phone at home or to hand in their phone to the Head of School at the start of the school day, to be collected at the end of the school day for the remainder of the half term.

3rd Time Offence
If a phone is collected from the student during the period when they were not supposed to have a phone on their person, owing to them having a second phone, the student will be suspended for a period of 1 day. A meeting will be organised with parents to inform them of school policy and of further sanctions to be imposed for continued phone use leading to full exclusion.

Use of Personal Digital Devices in the Capacity of a Computer

This policy applies to all areas of the school. IBSB believes that computers are essential tools used to support learning and enhance instruction. With these tools comes a responsibility that must be accepted by our school community. Our school-wide network provides access to shared resources such as printing, file storage, email, and the Internet, which offers vast, diverse, and unique educational resources. This worldwide access is accompanied by additional responsibilities. The user's behaviour and actions now represent the IBSB community in a global arena. Although the Internet provides a unique opportunity for learning, its nature also makes materials available that have no educational value, and some that many may find inaccurate and offensive. Though we will try to protect our students from such sites and reserve the right to supervise our students, we cannot look over everyone's shoulder all the time. IBSB cannot guarantee that every objectionable site will be disabled in advance or that every student will be monitored at every moment. To permit your child to use our School computers, student laptops, the Network, and more specifically the Internet, both you and your child must adhere to the following guidelines regarding use. Breaches of these guidelines may result in disciplinary proceedings, and/or notifying the appropriate law enforcement agency.

Digital Device Use Restrictions:

1. Permission to use personal laptops or digital devices during lessons is **entirely** up to each teacher in each lesson. If a teacher deems that laptops or digital devices should not be used, then they **should not be used**.
2. Personal laptops must NOT have pirated or illegally obtained software installed. All software must be fully licensed and all software licenses should be shown to the teachers on request and copies will be kept by the ICT department.
3. Personal laptops must have Virus Protection installed and submitted to the ICT technician for checking on request.
4. Personal computers are not allowed to be connected through network cable in the local area lan, nor access the local File Sharing Server. For internet access, only WiFi can be used.
5. Permission to use the computers in the ICT rooms must be obtained, prior to using the computer or printer.
6. A staff member must be present in the ICT room before permission is granted to use the computers or photocopier.

The following uses of the IBSB Network and Internet access are NOT permitted:

1. Accessing, uploading, downloading, or distributing pornographic, sexually explicit, promoting terrorism/extremism or otherwise obscene material or material of an excessively violent or hateful nature. If a suspected criminal act has been committed the school is legally required to contact the Police without informing parents.
2. Transmitting obscene, abusive, or sexually explicit language.
3. Using another person's credentials in any way.
4. Violating copyright or otherwise using the intellectual property of another individual or organisation without permission- e.g. music, games, software.
5. Attempting to circumvent network filters or security systems.
6. Accessing music/games/portable apps in school, except with permission from a member of staff.
7. Identifying yourself as someone other than who you are (or being anonymous) by the use of screen names or any other means of disguising or changing identity.
8. Plagiarising the work of others.

9. Using the network or accessing the Internet for financial gain, or commercial activity.
10. Installing any software onto a machine connected to the School network, including personal laptops, without permission from a member of the ICT Department.
11. The use of social networks or chat web sites and applications is not permitted at any time.
12. Amending the settings of the computer in relation to the system or desktop.
13. Using "download clients" (utorrent, bittorrent…), even on personal equipment.
14. Downloading movies, videoclips, or any other large videos without permission from a member of the IT Department.

The following rules of e-safety are to be observed at all times:

1. Adhere to the same standards of behaviour online that you follow in real life. Be polite. Abusive, derogatory language or cyber bullying is not permitted.
2. Any personal information such as your full name, address or telephone number will not be revealed without your parent's or teacher's permission.
3. Do not give out your network password to anyone other than your parents or teachers.
4. Never agree to get together with someone you "meet" online without your parent's permission/attendance.
5. Any information obtained that makes you feel uncomfortable should be reported to your teachers and parents.

Security Policy

Upon request of an IBSB staff member, a student must provide access to his/her laptop or digital device. The School reserves the right to review any information stored on a student's laptop or digital device, including any removable media he/she may have with him/her at school. This will only be requested when we feel that some aspect of the Acceptable Usage Policy has been violated. Automated systems will be used to monitor student's use of the network and Internet. At all other times we respect the students' right to keep their data confidential. IBSB will ensure that the security of users' personal data, where held, will be secure and IBSB will operate within the Data Protection Act.

Laptop Identification

It is recommended that each laptop and case exhibit the owner/student's name clearly. Luggage tags and Paint Pens are recommended. Personal laptops are the responsibility of the owner.

Procedure if a digital device is brought from home for educational purposes

The school will not be liable for damage caused by inappropriate use by the student or others.

Procedure if laptop or digital device is missing

If a laptop or other digital device cannot be found in school, the student must report the matter to school staff and parents. IBSB does not accept any responsibility if a personal laptop or digital device is stolen or damaged. Laptops and other digital devices must never be left unattended in any part of the school site and should be locked in a student's locker.

IBSB Internet Use

The World Wide Web can provide a valuable resource in terms of information and content. It is also important that we equip our students with ICT skills and the internet is an important aspect of today's technology. However, the web is an uncensored medium that is very diverse in its content, can be misused and can be misleading or corrupting. This policy seeks to define, and provide guidelines for, acceptable use of the internet by all members of the school community.

IBSB Internet Aims

We will enable all students to access the internet in appropriate ways. They will use it to search for information and then learn to discriminate between the varieties of information presented to them. As they progress through school they will work in the medium with an increasing degree of independence.

The administration of the school will use the internet to access information related to the administration of the school, to access educational resources and materials and to provide information related to the school to interested parties (email). The administration will supervise the school's website and maintain an interesting and informative site as a good advertisement for the school.

Guidelines

Students will be taught how to access the internet and use search engines. Students will be supervised at all times to ensure the sites visited are relevant to the age group of the students and the content suitable to their age.

Students will use email to communicate with others, asking questions and seeking information as well as corresponding with a member of staff.

School computers may not be used by any member of the school to access sites considered to be contrary to the aims and values of the school (e.g. pornographic, racist, sexist, extremist etc.). School computers may not be used to access chat rooms. School computers may not be used for the download and installation of any program – only the IT Department will install new programs onto computers. The school will monitor both email and internet usage to ensure the above.

The administration will ensure the school computers have adequate protection against viruses and against penetration by external computers. Junk mail and attachments from insecure or unknown sources will be deleted without opening in order to guard against virus infection.

School email addresses will be used for the purposes of the school and should not be used for personal messages. The school will provide email addresses to enable correspondence between teachers and parents (firstname.surname@ibsb.ro). Teachers are advised to use this and not disclose their personal email addresses to parents or pupils. More information can be found in 'Whole School Office 365 Policy' and "Whole School G Suite Policy".

1. I will not give out personal information such as my address, telephone number, pictures of myself or the name and location of my school without permission.
2. I will never agree to meet someone I have only spoken to on the internet.
3. I will not tell anyone my passwords (even my best friends). Only I, my parents, and my teachers may know it.
4. I will not respond to any messages that are mean or in any way make me feel uncomfortable.
5. I will tell my parents or a teacher right away if I find any information that makes me feel uncomfortable.
6. I will not download programs or bring programs on a USB memory stick, USB portable hard drive or CDROM.
7. I will not try to circumvent network filters or hack security systems, servers or any accounts.
8. I will be a good online citizen and not do anything that hurts other people.
9. I will not use the internet or computers at school without my parents' or teacher's permission.
10. If I break any of these safety rules whilst in school or at home I accept that I will not be allowed to use the internet until my teacher or parents allow me.

Related Policies

Whole School Health and Safety Policy
PS/SS Curriculum Policy
Whole School Anti-bullying Policy
Whole School Office 365 Policy
Whole School G Suite Policy
Whole School File Sharing Structure and Policy
Staff Personal Computer Use Policy

Updated November 2018_MB