



## **SABIS® Policy Document**

**Whilst all Policies have a minimum date for review as a guideline, policies are under constant review. Changes to policies will occur as required.**

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

Approved by: Governing Board

Date: November 2022

Last reviewed on:

Date: August 2026

Next review due by: 2 years

Date: August 2028

#### **Overview**

In addition to children and staff, the policy and its procedures also apply to senior managers and the board of trustees. This applies to paid staff, volunteers and agency employees.

- SABIS® strives to protect children and young people who receive its services through information technology (such as tablets, laptops, and the Internet).
- Provide staff and volunteers with our e-safety principles.
- The use of information technology should be in accordance with our values and within the law.

Disciplinary action will be taken if this policy is violated.

#### **Aims**

- Provide students with safe and controlled access to all computing and internet resources provided by the school. The use of these resources should be explained to students in a clear and concise manner.
- Students should be made aware that the Internet is a valuable resource in the classroom. Abuse of the resource will result in access being denied.
- As part of our development of the learning environment at ISCDIP, we will provide a variety of ICT opportunities and tools. As they develop their personalized learning according to our school's vision, they will have the freedom to make relevant, safe choices.



### **Students' access to the Internet**

- The Internet Service offered by ISCDIP is "filtered," so students will encounter a reduced amount of unwanted material on the Internet.
- Children are normally allowed access to the Internet only when an adult is present to supervise them. Nevertheless, it is impractical to assume that the teacher's attention will always be focused on the computer screen.
- It will be the responsibility of staff to make students aware of the potential for misuse, and to explain to them what is expected of them.
- In order for teachers to ensure that expectations of behavior are met, they will have access to students' screens and other Internet-related files.

### **Expectations of students using the Internet**

- The E-safety Agreement must be read and agreed to by all students.
- As with every other area of their school life, students at ISCDIP are expected to behave responsibly on the Internet as well. In addition, they are responsible for choosing what materials they wish to access and what language they wish to use.
- Students are expected not to intentionally seek out offensive materials on the Internet. In the event that a student accidentally encounters such material, they should inform a teacher immediately.
- A student is expected not to use rude language in his/her email communications and to contact only those persons whom he/she knows and has been approved by the teacher. Chain letters are prohibited.
- Before accessing the Internet, students must obtain permission from their teachers.
- Social networking sites cannot be accessed by students unless specifically authorized by the school or as part of a specific educational program.
- Students should not view other people's files without their permission.
- Unless permission has been granted, computers should only be used for schoolwork and homework.
- In order to ensure the safety of the school's computers, no applications should be downloaded from the Internet or brought into the school on portable media from home.
- The class teacher must scan portable media before it can be used for school work completed at home.
- A school network cannot be used for personal printing.



- Do not share personal information such as phone numbers and addresses. Do not arrange to meet someone unless it is part of a school project approved by the administration.
- Anti-virus software should be installed on all devices used at home by students.
- It is possible that students who fail to comply with these expectations consistently may be warned and subsequently denied access to Internet resources.

### **School Website**

- A review of the website will be conducted on a regular basis in order to maintain the safety of students and employees.
- Teachers will be responsible for determining whether children's work should be published.
- Whenever possible, the school will use digital photographs, audio or video clips focusing on group activities. Parental permission is required for the publication of photographs and videos focusing on individual students.
- Individuals in photographs will not have their full names published on the school website.
- As part of these efforts, the school will ensure that the image files are appropriately named. Also, if images are published online, the school will not use the names of students in the file names.

### **Personal devices**

- School administration may only authorize students to use their own technology in school in connection with a pre-arranged educational activity.
- Using a mobile phone inappropriately is in direct violation of the school's Acceptable Use and Mobile Phone Policy.

### **Sanctions**

- If students continue to misuse the internet, their access to the Internet will be restricted.
- A complete ban and/or confiscation will be imposed if other technologies are misused. A set period of time will be set by the Director for each of these actions. It is always our policy to notify parents. It is forbidden for students or their parents to use school-provided applications or services to discredit the institution or its members.
- Each user has the responsibility to report any misuse of technology, including unacceptable behavior.