SABIS®

SABIS®

Acceptable Use Policy

Education for a changing world.®

Americas | Europe | Africa | Middle East & Asia

sabis.net

Table of Contents

Introduction

Purpose

The **SABIS® Acceptable Use Policy** outlines the terms and guidelines for the use of electronic devices, software, and systems.

The policy has been designed to safeguard SABIS® and all users within the SABIS® Network including but not limited to employees, teachers, students, parents, consultants, and freelancers. All network users are informed that violation of these terms could expose SABIS® and/or SABIS® Network schools to security breaches, system attacks, financial loss, and legal issues, among other risks.

Scope

This policy covers the use of all equipment and devices owned or managed by SABIS®, as well as the company's IT systems related to Internet, Intranet, and Extranet, which include, among others, computing software, operating systems, network resources, and storage media, in addition to E-mail, browsing, and FTP network accounts.

All SABIS® Network users are expected to use information, electronic devices, and network resources in compliance with this policy.

Policy Terms

Acceptable Use

SABIS® Network users are expected to abide by the following general use terms.

Proprietary Information

- All proprietary information remains the exclusive property of SABIS®, regardless of whether it is stored on devices owned, managed, or leased by the organization, its employees, or third parties.
- Users are permitted to access, use, and share SABIS® proprietary information only when explicitly authorized and solely for the purpose of fulfilling assigned responsibilities.
- Any loss, theft, or suspected unauthorized access to SABIS® proprietary information must be reported immediately to the appropriate authority to ensure timely response and mitigation.
- To maintain system integrity and enforce this policy, the SABIS® IT Department reserves the right to conduct regular or random monitoring of devices, systems, and networks.

Security and Access

- SABIS®'s equipment and software are to be used for SABIS® business purposes only while serving the interests of the company and SABIS® Network schools.

- The SABIS® IT Department must approve any mobile and computing devices prior to their connection to the internal network.
- SABIS® Network users and administrators must create strong passwords following the **SABIS® Password Policy**. They must secure their password and never share it with or grant access to any unauthorized internal or external party.
- IT Administrators should secure all computers with a password-protected screen that is automatically activated within a maximum of 10 minutes from leaving the device inactive. Users must lock the screen whenever they leave their computer unattended.
- Users are expected to remain vigilant against suspicious or unsolicited emails and must avoid opening attachments or clicking links that may contain malware or phishing attempts.
- Any device connected to the organization's network and used to access or store organizational data must run approved antivirus software with up-to-date virus definitions at all times to ensure system security.

Unacceptable Use

Illegal activities under local law are strictly prohibited and should under no circumstances be performed by SABIS® Network users while using resources owned or managed by the company or SABIS® Network schools.

The following is a list of practices considered as unacceptable use of computing devices and resources.

Unauthorized Access and Disclosure

- Using corporate data, servers, or accounts to conduct activities that are not related to SABIS®, even when having authorized access.
- Exporting any technical material without first consulting the SABIS® IT Department.
- Disclosing any SABIS® account password to anyone, including co-workers and family.
- Allowing others to use one's account, whether within or outside the company.
- Providing external parties with any information about, or lists of, SABIS® or SABIS® Network school employees or students.
- Installing unauthorized software of altering system configurations.

Improper Behavior

- Using company-owned devices, software, or accounts to engage in any illegal activity, sexual harassment, or hostile activity.
- Using any SABIS® account for fraudulent activity.

Security Breaches

- Deploying malicious software (e.g., viruses, worms, Trojan horses, E-mail bombs, etc.), honeypots, or similar technology into and/or from the SABIS® Network or server
- Breaching security through unauthorized access to any data, server, or account, unless this falls within the scope of regular job requirements
- Interfering with network communications in any way, such as network sniffing, pinged floods, packet spoofing, denial of service, and forged routing information.

- Performing any kind of network monitoring to intercept data not intended for the employee's host, unless this falls within the scope of normal duties
- Disrupting or disabling a user's terminal session by using any computing practice or by sending messages

Exceptionally, and in certain isolated cases, some of the restrictions in the Unacceptable Use section may be permitted. For example, IT administrators or specialists can be granted permission to disable network access of a host that is harming production or performance.

Inappropriate Use of Online Communications

E-mail

- Sending unsolicited emails or promotional content, including messages related to school services or products, to internal or external recipients without prior authorization.
- Creating, forwarding, or participating in deceptive or harmful email schemes, including chain letters, phishing attempts, or similar activities.
- Harassment through digital communication—whether by content, frequency, or volume—is strictly prohibited. All users must communicate respectfully and professionally.
- Manipulating or forging email headers or sender information. All communication must be transparent and accurately represent the sender's identity.
- Posting unrelated or non-educational content to school-managed communication platforms or forums.
- Using school or organizational accounts to make false or misleading offers of products, services, or opportunities.

User Compliance

- The SABIS® IT Infrastructure Department is responsible for ensuring the proper application of the policy herein, via business tool reports, internal and external audits, and the like.
- Violation of any term of this policy may lead to disciplinary action.
- Exceptions to any term of the policy may be granted only upon written approval by the SABIS® IT Infrastructure Department.

Should you have further questions or concerns about this policy, do not hesitate to contact your IT Infrastructure Department.