
# Information and Communications Technology (ICT) Acceptable Use Policy

***Updated July 2025***

**Centurion International School, Bangkok**

# CISB ICT Acceptable Use Policy - 2025-2026

## Purpose

This ICT Acceptable Use Policy sets out the rules and guidelines for the appropriate use of all ICT resources at Centurion International School of Bangkok. Its aim is to ensure that students, teachers, staff and guests use ICT services safely, securely and in a manner consistent with CISB's educational mission, values and legal obligations.

## Scope

*This Policy applies to:*

- All users of CISB's ICT resources, including students, faculty, administrative staff, contractors and visitors
- All ICT equipment, systems, software and network services owned, leased or otherwise provided by CISB, whether on-campus or accessed remotely

## Definitions

- ICT Resources: Hardware (computers, tablets, servers, network devices), software, data, email, internet access, cloud services and peripherals
- Users: Anyone authorized to access or use CISB ICT resources
- Confidential Data: Personal or sensitive information about CISB students, staff or operations

## User Responsibilities

1. **General Obligations**
    a. Use CISB ICT resources for educational, administrative or authorized research purposes only
    b. Exercise care to protect login credentials; sharing accounts is prohibited
    c. Lock or log off devices when unattended, and if applicable

2. **Security and Privacy**
    a. Protect confidential data by following CISB's Data Protection Policy
    b. Report any suspected security breaches or lost/stolen devices immediately to the ICT Helpdesk

c. Do not attempt to bypass network security (e.g., firewalls, content filters, anti-virus)

**Respect and Ethical Conduct**

- Treat other users with respect; do not engage in harassment, hate speech or cyberbullying
- Credit all sources and respect copyright, intellectual property and software licensing terms.

**Prohibited Uses**

*Users must not:*

- Access, download or distribute illegal, obscene or inappropriate materials
- Use ICT resources for commercial gain or political campaigning
- Introduce malicious software (viruses, worms, spyware) or attempt unauthorized access to any network or system
- Engage in phishing, spamming or mass-mailing unrelated to CISB's educational mission
- Install unauthorized hardware or software on CISB devices or network
- Share personal data about others without proper authorization

**Internet and Email**

- Web browsing is subject to CISB's content filters; attempts to circumvent them are prohibited
- School email is to be used for school-related communications; personal use must be limited, lawful and inoffensive
- Emails must carry the standard CISB signature (name, role, school contact details)

**Monitoring and Privacy**

- CISB reserves the right to monitor, log and review network traffic, email and data stored on its systems to ensure compliance
- Users have no expectation of privacy when using CISB ICT resources

**Enforcement and Sanctions**

- Violations of this Policy may lead to disciplinary action consistent with CISB codes of conduct, up to suspension of ICT access, disciplinary review or termination of employment/enrollment
- Serious or illegal activities will be reported to law enforcement or relevant authorities

**Date of Last Review:** July 2025
**Next Review:** July 2026