

CYBER SECURITY POLICY

Policy Revised By	Department of IT	Policy Reviewed & Monitored By	SLT and HODs	CEHS/CSP/2026-27
Date of Review	17/03/2026	Approved by	Principal	
Academic year	2026-2027	Next Review	16-03-2027	

1. Introduction

Crescent English High School is committed to safeguarding the confidentiality, integrity, and availability of its digital systems and data. This Cybersecurity Policy outlines the procedures and responsibilities for protecting the school's information technology resources and ensuring safe, secure digital practices for students, staff, and stakeholders. The policy complies with KHDA guidelines and applicable UAE cyber laws.

2. Purpose

The purpose of this policy is to:

- Protect the school's digital infrastructure from cyber threats.
- Promote safe and responsible use of technology within the school community.
- Ensure compliance with UAE Federal Decree Law No. 34 of 2021 on Cybercrime and relevant KHDA regulations.

3. Scope

This policy applies to:

- All staff, students, contractors, and third parties accessing or using Crescent English High School's IT systems.
- All devices connected to the school's network (desktops, laptops, tablets, smartphones, etc.).
- All data processed, stored, or transmitted via the school's digital platforms, including administrative and academic information.

4. Roles and Responsibilities

4.1 IT Manager

- Implement and maintain cybersecurity infrastructure.
- Monitor systems for threats and vulnerabilities.
- Conduct cybersecurity awareness and training programs.
- Manage incident response and disaster recovery planning.

4.2 Staff and Faculty

- Use school IT systems for official educational and administrative purposes only.
- Follow best practices in password security and data handling.
- Immediately report any suspected security incidents or breaches.

4.3 Students

- Use school devices and internet responsibly and ethically.
- Avoid accessing or sharing inappropriate content.
- Participate in digital safety and cybersecurity education programs.

4.3.1 Prohibition of Smart Wearables, Recording Devices & Hidden Cameras

A. Prohibition of Smart Wearable & Recording Devices on School Premises

Students are **not permitted to wear, carry, or use** smart wearable devices **anywhere on school premises**, including but not limited to:

- Classrooms
- Examination halls
- Laboratories
- Libraries
- Corridors, playgrounds, and common areas

Prohibited devices include:

- Smart glasses (e.g., camera-enabled or AI-assisted eyewear)
- Smart watches, fitness bands, smart rings
- Wireless earbuds or listening devices
- Any device capable of **recording, storing, transmitting, or receiving audio, video, images, or data without permission of supervisor.**

B. Prohibition of Hidden Cameras & Disguised Recording Devices

The use or possession of **hidden or disguised recording devices** is **strictly prohibited** on school premises. This includes, but is not limited to:

- Pen cameras
- Button cameras
- Keychain cameras
- Spectacle-embedded cameras
- Any concealed or covert recording equipment

C. Privacy & Data Protection

Recording or attempting to record **students, teachers, staff, or school activities** without explicit authorization is a **serious violation of privacy**. Such actions may:

- Breach personal data protection and cyber safety laws
- Create unsafe and hostile learning environments
- Result in legal consequences beyond school disciplinary action

D. Academic Integrity & Misconduct

Possession or use of prohibited devices during instructional time or assessments will be treated as:

- **Cyber misconduct**
- **Violation of student code of conduct**
- **Academic dishonesty** (if during tests or exams)

Disciplinary actions may include:

- Confiscation of the device (as per school policy)
- Written warning or suspension
- Cancellation of assessments or exams
- Further action as deemed appropriate by school authorities

E. Declaration, Inspection & Confiscation

Students may be required to:

- Declare electronic or wearable devices upon request
- Submit such devices for safekeeping during school hours

The school reserves the right to **inspect items** where there is reasonable suspicion of policy violation, while maintaining student dignity.

F. Assistive & Medical Device Exception

Exceptions apply only to **medically necessary or approved assistive devices**.

Such devices must:

- Be declared in advance
- Be approved in writing by school administration
- Be used strictly for the approved purpose under supervision

G. Emerging Technology Clause

This policy applies to **all current and future technologies**, including devices not explicitly listed, that pose risks to:

- Student privacy
- Cyber safety
- Academic integrity

5. Acceptable Use Policy

- Use of the school's internet and devices must support teaching, learning, and administration.
- Users may not install unauthorized software or access blocked websites.
- Passwords must be kept confidential and changed regularly.
- Use of personal devices (BYOD) is permitted only with prior approval and in accordance with school guidelines.

6. Data Protection and Privacy

- All student and staff data must be stored securely and accessed only by authorized personnel.
- Personal data must not be shared without consent.
- Cloud storage services must be compliant with UAE data protection standards.

7. Network and System Security

- Firewalls, antivirus software, and endpoint protection tools must be active and updated regularly.
- Systems must use strong authentication (e.g., passwords, two-factor authentication).
- Regular backups and security audits will be performed.

8. Incident Response and Reporting

In the event of a cybersecurity incident, the following reporting and response procedures shall be followed:

- **Reporting by Students or Staff:** Any student or staff member who becomes aware of cyberbullying, online abuse, or any cybersecurity-related concern must report the incident immediately to the designated Child Protection Officer (CPO).
- **Child Protection Officer (CPO):** The CPO will document the incident, provide immediate support to the affected individual, and escalate the matter to the School Principal.

- **Principal:** The principal will coordinate with the IT Department for technical support and ensure appropriate measures are taken.
- **IT Department:** The IT team will investigate the incident, contain any threats, and take corrective action to restore safety and security.
- **Regulatory Reporting:** Where required, a formal incident report will be submitted to the KHDA and/or other relevant authorities in compliance with regulatory obligations.

9. Training and Awareness

- Annual cybersecurity training will be conducted for staff.
- Students will be educated on responsible digital behavior and online safety.
- Parents will be engaged through awareness sessions on supporting digital safety at home.

10. Compliance and Disciplinary Action

Violations of this policy may result in:

- Suspension of IT privileges.
- Disciplinary action in line with the school's Code of Conduct.
- Legal action if applicable under UAE law.

11. Policy Review

This policy will be reviewed and updated annually or whenever significant changes occur in technology, regulations, or risk assessments.

DR. SALEEM JAMALUDHIN
(Director)

Signed _____

Date: 20/03/2026



DR. SHARAFUDEEN THANIKATT
(Principal)

Signed _____

Date: 20/03/2026

