Cybersecurity Policy

1. Purpose

The purpose of this policy is to ensure the protection of digital information, safeguard personal data, and promote responsible online behavior among students, staff, and parents. The school is committed to maintaining a safe and secure digital environment that supports teaching, learning, and communication.

2. Scope

This policy applies to all **students, staff, and parents/guardians** who use the school's digital systems, including:

- School-provided devices (computers, tablets, projectors, servers).
- Personal devices connected to the school's Wifi and local network.
- AI tools, cloud platforms, and EdTech apps (Century Tech, Raz Plus, Lexia, etc.).
- School communication platforms (emails, portals, apps).
- Online learning platforms and third-party educational tools.

3. Key Principles

1. **Data Privacy & Security:** Protect student/staff records with encryption and confidentiality.
2. **Responsible Use:** Use school digital systems responsibly and ethically.
3. **AI & Emerging Tools:** Ethical, transparent, and age-appropriate usage, with parental awareness.
4. **Monitoring & Compliance:** IT Department to track usage, filter content, and maintain logs.Report any suspicious activity, cyber threat, or breach immediately.
5. **Incident Response:** Immediate reporting of suspicious activities, cyberbullying, or breaches.
6. **Positive Environment:** Promote digital citizenship and online safety within the school community.

4. Policy Guidelines

For Students

- Use only approved BYOD devices; no mobile phones.
- Follow surrender & in-class usage rules.
- Do not share login credentials with others.
- Never bypass security filters, use VPNs, or access unauthorized sites.
- Avoid accessing, downloading, or sharing inappropriate or harmful content.
- Report cyberbullying, phishing, or suspicious messages to teachers or the school counselor.

- Respect digital ethics: no plagiarism, piracy, or AI misuse (e.g., ChatGPT without teacher approval).
- Respect intellectual property—no plagiarism, piracy, or unauthorized software downloads.

For Staff

- Protect student and staff data in line with school confidentiality standards.
- AI and EdTech use must align with curriculum and safeguarding standards.
- Use strong, unique passwords and change them regularly.
- Do not install unapproved applications on school systems.
- Ensure safe handling of electronic communication with students (use official school channels only).
- Report incidents within 24 hours to IT and SLT.

For Parents

- Support children in responsible online behavior at home.
- Avoid sharing sensitive school-related information on social media or unsecured platforms.
- Use only official school communication channels (school portal, official emails, and newsletters) for queries or concerns.
- Report any suspected cyber risks that may affect the school community.
- Monitor children's device use and encourage healthy digital habits.

5. Prohibited Conduct

- Unauthorized access to school systems or data (hacking)or use of VPNs.
- Sharing false, misleading, or harmful information online.
- Using school devices or accounts for illegal or unethical activities.
- Circumventing BYOD security rules or school internet filters or security measures.
- Misuse of AI tools for cheating, harmful deepfakes, or plagiarism.
- Cyberbullying, harassment, or online defamation of students, staff, or parents.

6. Grounds for Violations and Consequences

For Students

- **Minor Violations**: Misuse of devices, sharing passwords.
    - Warning, parental notification, temporary loss of device privileges.
- **Moderate Violations**: Accessing restricted sites, repeated misconduct.
    - Device confiscation, suspension from online platforms, mandatory counseling.
- **Severe Violations**: Hacking, cyberbullying, data theft.

- Suspension or expulsion, referral to legal authorities (as per UAE Cybercrime Law).

For Staff

- **Minor Violations**: Weak password practices, unintentional breaches.
  - Warning, refresher training.
- **Moderate Violations**: Unauthorized sharing of school/student data.
  - Formal HR disciplinary action.
- **Severe Violations**: Data leaks, cyber harassment, intentional breach of trust.
  - Termination of employment, legal referral.

For Parents

- **Minor Violations**: Sharing school updates in unsecured groups.
  - Reminder and written warning.
- **Moderate Violations**: Spreading false information, unauthorized sharing of student data.
  - Meeting with school leadership, suspension of school communication privileges.
- **Severe Violations**: Cyber harassment of staff, students, or parents; data breaches.
  - Restriction from school facilities, legal referral.

7. Cyber security Education

- The school will provide regular training and awareness sessions for students, staff, and parents on:
  - Students: Digital citizenship, safe passwords, ethical AI use.
  - Staff: Data privacy, AI integration, safeguarding compliance.
  - Parents: Home device safety, monitoring apps, responsible AI support.
  - Annual awareness week and refresher workshops.

Type of Document	Cyber security Policy
Date Written	Sept 2025
Review Date	Sept 2026