ليـــوا للتعليم
Liwa Education

Responsible Technology Usage Policy

Policy Document

2024-2025

Policy Reference	IT-02
Version	V1
Date of Creation	01082024
Policy Owner	IT Manager
Date of Approval	01082024
Effective Date	01082024
Date of Review	01082026
Reviewed by	Director of Schools
	Deputy CEO
Approved by	CEO

A. Rationale

This policy ensures that Liwa Education Schools adhere to the requirements set forth by the Abu Dhabi Department of Education and Knowledge (ADEK) while maintaining a secure and responsible digital environment for students, staff, and stakeholders. As technology plays a vital role in education and administration, this policy establishes clear guidelines for cybersecurity, responsible technology use, and data protection. It reflects the school's commitment to creating a safe, ethical, and secure online environment in alignment with regulatory requirements.

B. Purpose

The purpose of this policy is to establish a clear and structured approach for managing and responding to cybersecurity incidents that may impact Liwa Education Schools' technology systems, student and staff data, or daily operations. The policy outlines procedures for identifying, containing, eradicating, and recovering from cybersecurity incidents. This is crucial to protect the school community and ensure compliance with relevant regulations.

C. Policy Overview

Liwa Education Schools is committed to:

1. Preventing user access to, or transmission of, inappropriate material via the Internet, electronic mail, or other forms of electronic communications.
2. Preventing unauthorized access and other unlawful online activities.
3. Preventing unauthorized online disclosure, use, or dissemination of personal identification information of minors.
4. Complying with the Child Protection Policy (CPP).

All users must adhere to the Liwa Education Schools Internet Responsible Use Policy and cybersecurity procedures outlined in this document.

D. Guidelines and Procedures

1. Availability of Access

1.1. Internet access is provided for instructional and administrative purposes only.

1.2. The network is a privilege, not a right. Misuse may result in disciplinary actions, including revocation of access privileges.

1.3 The school reserves the right to monitor, access, and disclose any user's files, activities, or communications to ensure compliance with this policy.

2. Security

2.1 Users are required to maintain confidential login credentials, such as usernames and passwords. Sharing login information or using another user's credentials is strictly prohibited.

2.2 Internet filtering systems are in place to block access to inappropriate or harmful content. Users encountering questionable content must report it to the administration immediately for review and action.

3. Internet Safety

Liwa Education Schools prioritizes internet safety and has implemented measures to:

3.1 Prevent access to inappropriate or harmful online content, especially for minors.

3.2 Safeguard minors when using email, messaging platforms, and other online communication tools.

3.3 Provide age-appropriate training on online safety, including privacy protection, cyberbullying awareness, and responsible online behavior.

Authorized Exceptions: The principal is authorized to designate certain individuals to temporarily disable the blocking or filtering measures for bona fide research or other lawful purposes.

4. Inappropriate Use of Technology

The following activities are prohibited and will result in disciplinary action:

4.1 Sharing or posting materials that are defamatory, obscene, profane, threatening, or inconsistent with the school's values.
4.2 Engaging in harassment, bullying, or other abusive behaviors.
4.3 Using the network for unauthorized commercial activities or financial gain.
4.4 Downloading, installing, or using unauthorized software or programs.
4.5 Attempting to bypass network security or circumvent filtering systems.
4.6 Gaining unauthorized access to restricted data or systems.
4.7 Introducing harmful software, such as viruses, to the network.
4.8 Altering or tampering with network or computer configurations.
4.9 Using the school network for illegal activities, including downloading copyrighted materials without permission.

5. Cybersecurity Incident Response

Liwa Education Schools has established an incident response protocol to address cybersecurity threats:

5.1 **Identification**: Detecting and assessing potential cybersecurity incidents.
5.2 **Containment**: Isolating affected systems to minimize damage.
5.3 **Eradication**: Addressing the root cause and eliminating threats.
5.4 **Recovery**: Restoring normal operations and ensuring data integrity.

The IT Department will lead this process, with support from relevant stakeholders, to ensure swift resolution and reporting.

E. Enforcement and Disciplinary Actions

Violations of this policy will result in:

1. Revocation of access privileges.
2. Consequences as outlined in the school's Code of Student Conduct and Discipline.
3. Legal action as per UAE laws and regulations, if necessary.

F. Review and Amendments

This policy will be reviewed regularly and updated as necessary to reflect changes in technology, regulatory requirements or the school's educational practices.

By following this policy, Liwa Education Schools ensures the safe and responsible use of technology for educational purposes while safeguarding the security and privacy of all users.

Policy Owner Department

IT Department

Key Stakeholders		
Policy Owner:	Hari Devicharan	IT Manager
Reviewed by:	Margaret Haynes	Director of Schools
	Kevin Wallis	Deputy CEO
Approved by:	Dr. Shereen Gobran	Chief Executive Officer