ITM001 – IT Acceptable Use Policy

XCL Education Malaysia

Approved by:	[Anthony Partington]	**Date:** [1 August 2024]
Last reviewed on:	[N/A]	
Next review due by:	[1 August 2025]	

Contents

1. Introduction 3
2. Procedures and practice 3
   2.1. Scope 3
   2.2. Ownership and Return of Computing Devices 3
   2.3. Protection of Company issued Computing Device 3
   2.4. Acceptable Use of Computing Devices 4
   2.5. Staff Passwords and User Accounts 4
   2.6. Secure Use of Internet 5
   2.7. Secure Use of Electronic Communication 5
   2.8. Secure Sharing and Storage of Data 5
   2.9. BYOD (Bring Your Own Device) 6
   2.10. Remote Support and Access to Third Parties 6
   2.11. Incident Reporting 6
   2.12. Responsible Digital Citizenship 7
3. Concluding notes 7
   3.1. Monitoring and Review 7
   3.2. Links to other policies 7

1. Introduction

This policy will provide guidelines to ensure that all users of information and communication technology (ICT) at XCL Education Malaysia and its related entities (The Company):

- understand and follow procedures to ensure the safe and appropriate use of ICT at the service, including maintaining secure storage of information.
- take responsibility to protect and maintain privacy.
- are aware that only those persons authorized by the Approved Provider are permitted to access company ICT services.
- understand what constitutes illegal and inappropriate use of ICT facilities and avoid such activities.

This policy provides a governing framework for secure and responsible use of company provided computing devices, services and devices connected to company networks. It is the responsibility of every company staff to be aware of this policy and to conduct their activities in accordance with its recommendations.

2. Procedures and Practice

2.1. Scope

This policy applies to XCL Education Malaysia and all related entities. Throughout this document, all applicable parties have been collectively referred to as "company staff". This policy applies to all aspects of the use of ICT including:

- internet usage
- electronic mail (email)
- electronic bulletins/notice boards
- electronic discussion/news groups
- weblogs (blogs)
- social networking
- file transfer
- file storage (physical, cloud or any form of storage where data resides)
- file sharing
- video conferencing
- streaming media
- instant messaging

2.2. Ownership and Return of Computing Devices

The Company provides computing devices to its staff. This is to support educational and work-related activities. Company provided devices shall continue to be the property of company, unless explicitly documented at the time of allocation.

Upon completion of employment or the contractual term, personnel shall return all computing devices in their custody to the IT department.

2.3. Protection of Company issued Computing Device

Company staff shall adopt reasonable measures to safeguard the company issued equipment in their possession from theft and damage, including but not limited to the following:

- Computing devices shall not be left unattended in meeting rooms or at third-party locations including conferences or hotel rooms.
- Computing devices shall not be checked-in as baggage during travel, unless mandated by the airport security personnel.

Company staff are not authorized to perform self-repairs. Faulty devices shall be handed over to the IT department for repairs and maintenance through authorized service vendors. Costs of repair or replacement will be borne by the person the device was assigned to unless it is due to manufacturer defect.

Staff are required to obtain a Police report for stolen or lost devices. The Company reserves the right to secure erase lost or stolen devices. Incidents related to lost, stolen or damaged computing devices shall be promptly reported to the IT department. Costs of replacement will be borne by the person the device was assigned to unless otherwise agreed by the management of the company.

Computing devices including portable storage devices, containing company business information shall be handed over to IT for disposal in a secure approved manner.

2.4. Acceptable Use of Computing Devices

Company issued computing devices shall be utilized in a manner that is consistent with organizational policies and within the confines of country laws and regulations. Company staff shall not:

- Bypass organization or national security measures through fraudulent use of network protocol address i.e., use of private Virtual Private Networks (VPN) or anonymity networks.
- Download, transmit, store, or create inappropriate material such as extremist or terrorism related materials, pornographic content, malicious software (malware) and pirated copies of software or entertainment media.
- Perform activities that would cause the network, website or applications to stop functioning or result in crashing, deletion, omission, destruction or cause fraudulent transaction i.e., activities classified as hacking or cracking.
- Install applications not authorized and not licensed to the Company or obtained via illegal methods.
- Provide remote or physical access to the computing device, to individuals other than designated IT administrators.
- Reconfigure or tamper with the computing device in any way that could result in failure, degraded performance or limited operations of software and implemented security controls i.e., Anti-Virus, Mobile Device Management, and other software agents.
- Interrupt installation of security patches and operating system upgrades on computing devices through forceful shutdown.
- Company staff other than designated IT staff, shall not hold privileged access / administrator rights on computing devices, to applications or to any other services hosted on company networks.

2.5. Staff Passwords and User Accounts

The Company provisions business tools and online subscriptions to its employees, which is controlled through a combination of user credentials (username and password). Company staff shall exercise due care to prevent misuse of their allocated accounts. Company staff:

- Shall not share their credentials (username password combination) with anyone. This includes colleagues, contractors, senior staff, managers or IT staff.
- Shall not reveal or list passwords over emails, chats, questionnaires, sticky notes, security forms.
- Shall choose passwords that meet the current recommendations, ideally a “pass phrase” (a combination of words) instead of a password if the system allows it. Refer to the document **Microsoft Password Guidance** for best practice.
- Password shall not be listed in hints on “Recover Password” questions.
- Shall be responsible for all activity that occurs, from use of their accounts and allocated computing devices.
- Is strongly encouraged to use Multi-Factor Authentication (MFA) where available via the Microsoft Authenticator mobile app or other similar solutions.

- Shall use biometric of any of Windows Hello method of authentication for company provided devices where available.

2.6. Secure Use of Internet

Internet access provided to the Company staff shall be consistent with their business needs. Company staff shall not utilize Internet access provisioned within premises or provided by the company in external locations to perform activities that could endanger reputation or classified as illegal as per national laws and regulations. Company staff shall not utilize the Internet access provided to:

- Commit fraud, forgery, harassment, intimidation or impersonation.
- Post or share derogatory, libelous or threatening messages or images against an individual, race, religion, organization or community.
- Download, upload or access inappropriate, extremist or terrorism related materials, pornographic content, malicious software (malware) and pirated copies of software or entertainment media.
- Use peer-to-peer or torrent-based applications.
- Use anonymity networks (TOR, VPN) or access dark web without explicit approval from IT department.
- Perform activities that could cause corruption, disruption or result in unauthorized access of data on third-party websites or services on the Internet i.e., activities classified as hacking or cracking.
- Cause "Denial of Service" i.e., Use Internet services in a way that disrupts or blocks the service for others.
- Commit copyright infringement and provide third-parties, unauthorized access to company network or to company issued computing devices through use of Virtual Private Networks.

Connecting to free public Wi-Fi hotspots for Internet access (cafés, hotel lobbies, airports) utilizing company issued devices is not recommended. Personal use of the Internet within company premises during business hours should be minimal and must not affect the individual's ability to perform their assigned responsibilities.

2.7. Secure Use of Electronic Communication

Company staff should use their company email account with due care to avoid misuse. Company staff shall not:

- Company email address to subscribe to mailing lists, external services not related to business.
- Utilize named company accounts for promotional messages or advertisements.
- Share executable programs or scripts to internal or external recipients over any form of electronic communication.
- Generate or forward chain messages containing derogatory, libelous or threatening messages, images against an individual, race, religion, organization or community.
- Remove or modify the system generated disclaimer notice and email signatures.
- Auto-forward company emails to external addresses / domains or personal accounts.

Company staff should exercise caution in responding to requests soliciting user credentials for that claim to come from IT department or service providers over email or telephone calls.

NOTE: Under any circumstances, IT or any service provider will not request validation of user accounts or user credentials (username / password) over an email, URL, SMS or telephone calls. All such requests should be promptly notified to the IT department and should not be complied with.

2.8. Secure Sharing and Storage of Data

Company staff shall exercise due care in handling data in their custody. Company staff shall not share confidential business data through unauthorized channels, i.e., personal email, messenger services, free to

use data sharing and cloud storage platforms, e.g., Gmail, Yahoo mail, WhatsApp, Dropbox, WeTransfer, personal cloud storage accounts among others.

Staff are required to use the company provided OneDrive or designated storage as the default location to store data.

Staff are not permitted to configure data shares on their local computing devices. Company staff shall only utilize Microsoft Office 365 issued Corporate OneDrive cloud account or the company provisioned platform, to share data with relevant external business parties.

Data shares shall be configured only after relevant approvals from data owners / Head of the Department. Access to data shares shall be, explicitly restricted to designated individuals of intended business parties and disabled within 90 days of activation.

2.9. BYOD (Bring Your Own Device)

Staff are permitted to register personal handheld devices for official use under BYOD program; personal devices shall comply with the following standards to be eligible for registration under BYOD program:

- Devices should be running a supported platform:
  - Android
  - IOS / Apple designated Operating System
  - Windows
- Devices should be covered by the manufacturer for security updates and host a supported version of the Operating System or updated firmware. As security is a key factor, the company will take action to remove and remotely delete company data on a registered device if deemed necessary.
- Devices should be secure, free of malware and any jailbroken or rooted devices are not permitted. Only applications from authorized manufacturer app stores are allowed on BYOD devices.
- Devices should be adequately protected via regular software and operating system updates and presences of a security software such as antivirus

The company may change the supported platforms and versions supported depending on current technology trends and risks.

2.10. Remote Support and Access to Third Parties

For troubleshooting or management of applications and computing devices in company network:

- that requires third-party access to company network or computing devices shall be logged and managed through IT department.
- IT staff shall monitor access by third parties to the company network or devices connected to company networks.
- Provisioning access to third parties for computing devices that are connected to company network requires approval from IT to ensure security of the network and information.
- Unregistered or unlicensed software for remote access or to circumvent controls within the network is prohibited.

2.11. Incident Reporting

Company staff shall report all incidents to enable implementation of appropriate corrective actions. Company staff should promptly report any of the following incidents to IT helpdesk:

- Lost / stolen company provided device.
- Loss of personal device registered under BYOD.
- Lost storage device containing company data.
- Compromised credentials.

- Suspicious system behavior.
- Suspicious emails sent from company account.
- Suspected malware.
- System misconfiguration or opportunities to circumvent implemented system controls discovered during the course of daily business operations.
- Suspicious devices attached to systems or network points.
- Suspicious / look-alike wireless networks visible in company premises;
- Any identified violation of this policy;

2.12. Responsible Digital Citizenship

Users should adhere to the school's acceptable use policy and practice respectful and ethical behavior online. Cyberbullying, harassment, or any form of online misconduct will not be tolerated.

3. Concluding notes

3.1. Monitoring and Review

The CTO and IT department is primarily responsible for monitoring the implementation of this policy. This policy shall be reviewed annually to ensure that it stays relevant with the change of technology landscape.

3.2. Links to other policies

This policy should be read in conjunction with the following documents:

- Microsoft Password Guidance