INFORMATION COMMUNICATION TECHNOLOGY POLICY

Authorised By:	President (CEO)	Revision: 1.11
Last Amendment Date:	Revision Date: 02 Jun 2021	
Review Due Date:	Next Review: 02 Jun 2026	
Responsible Officer:	Registrar	
Review:	Executive Director - Digital Learning and Innovations Team	

Any person who requires assistance in understanding any aspect of this document should contact the Responsible Officer.

1. Overview

The purpose of the Information Communication Technology (ICT) Policy is to ensure the effective protection and proper usage of the computer systems within Tabor College Inc. The ICT Policy will assist in maintaining systems at operational level and ensure the integrity of data,

2. Scope and Applications

This policy applies to all staff members and volunteers of Tabor.

3. Policy Principles

3.1. Tabor will uphold the integrity and reliability of its ICT structure and all associated data

4. Procedures

4.1. Network

4.1.1. Network management, administration and maintenance within the College are the responsibility of the Digital Learning and Innovations Team (DLIT)/ICT Services Provider. Access to, and usage of, the Servers is restricted to authorised staff.

4.2. Hardware and Software

4.2.1. The requirement for IT equipment and Software will normally be identified within the context of an IT strategy for the College and more specifically within a planned programme of PC replacement.

4.2.2. The purchase, installation, configuration and maintenance / support of computer equipment and Software are the responsibility of the DLIT / ICT Services Provider. Software, including screensavers, must not be installed or downloaded from the Internet by users without prior authorisation from the DLIT / ICT Services Provider

4.2.3. Software that is placed on the desktops of data-projector units by lecturers must be removed when the lecture is over, this includes PowerPoint presentations.
4.2.4. Software licence and computer equipment registers will be maintained by the DLIT / ICT Services Provider to ensure full tracking of equipment and compliance with legislation.
4.2.5. The ICT Administrator will liaise with the Chief Operating Officer to ensure adequate insurance cover for computer equipment.
4.2.6. Software disks will be kept securely by the DLIT.
4.2.7. Requests for modifications, enhancements and upgrades of existing software applications should be discussed with the ICT Administrator.
4.2.8. Requirements for new hardware, new software or software applications must be discussed in advance with the ICT Administrator to assess the detailed specification and implications.
4.2.9. The deployment of new equipment or re-deployment of existing equipment is undertaken by the DLIT after consultation with Deans of Faculties / Departments.
4.2.10. The relocation of hardware within or out of Tabor College premises must be discussed with the ICT Administrator in advance to ensure good reason for relocation, determine the most appropriate means of relocation and that computer equipment registers and insurance policies are updated.
4.2.11. The security and safekeeping of portable and other equipment used outside the College premises is the responsibility of the member of staff using it.
4.2.12. All members of staff are responsible for the proper use, care and cleanliness of the computer equipment they use.
4.2.13. Problems with hardware or software are to be reported to the DLIT via email / phone / helpdesk ticket.

4.3. Electronic Information

4.3.1. Deans of Faculties / Heads of Departments are responsible for maintaining the quality of the computer-held data processed by their staff.
4.3.2. The individual user is responsible to their line manager for the quality of the computer data they have personally processed.
4.3.3. All information / data held on the organisation's systems is deemed the property of Tabor College Inc.
4.3.4. As a condition of employment, staff consent to the examination of the use and content of all data / information processed and / or stored by the staff member on the organisation's systems as required.
4.3.5. The DLIT is responsible for ensuring the implementation of an effective back-up strategy for server-held software and data.
4.3.6. Data stored on networked desktop PCs on the local hard drives may be lost if a problem develops with the PC, and the DLIT may not be able to assist in its recovery. Data should therefore, be stored within the file directory (folder) structure used by the office, i.e., Sharepoint.

4.4. Security

4.4.1. The DLIT/ICT Services Provider is responsible for the implementation of an effective virus security strategy. All machines, networked and standalone, will have up-to-date anti-virus protection.
4.4.2. The installation of anti-virus software on all machines is the responsibility of the DLIT.
4.4.3. The DLIT will ensure the upgrade of the anti-virus software on networked desktop PCs.
4.4.4. Staff members are required to virus-scan all media (including USBs and CDs) prior to first use. The DLIT will provide assistance and training where required.
4.4.5. On detection of a virus, staff must notify the DLIT immediately which will provide assistance.
4.4.6. Under no circumstances must staff attempt to disable or interfere with the virus scanning software.

4.5. Usage

4.5.1. It is the responsibility of Deans of Faculties / Departments to ensure appropriate computer training for their staff is identified. The DLIT can assist with computer-related training issues.

4.5.2. Deans of Faculties / Departments should notify the HR Manager of new members of staff in advance to allow the creation of network and e-mail accounts and system permissions.

4.5.3. New staff member accounts will not be created unless an request is received by the DLIT via the online New Staff Form.

4.5.4. Deans of Faculties / Departments should notify the DLIT of the departure of staff to allow the deletion of network and e-mail accounts.

4.5.5. The DLIT will ensure password protection is part of the security strategy of the Tabor Adelaide IT system. All new computers, both desktop and laptop, supplied to staff will have a password set by default.

4.5.6. Passwords must be specific to each staff member; as such staff must change their password after an account is established. Staff members are responsible for the security of their password and must not divulge this to others including colleagues.

4.5.7. Problems with passwords should be reported to the DLIT.

4.5.8. Users are to ensure their computers are fully shut down and turned off at end of day.

4.5.9. Computers must have screen savers set to activate after no more than 10 minutes of absence and require a password to resume. Laptops are to be stored securely when not in use.

4.5.10. Lecturers and visitors are required to bring presentations on usb memory sticks.

4.5.11. Deans of Faculties / Departments will determine the top-level folders/directories and associated permissions for their department and inform the DLIT. The DLIT will create or modify the folders accordingly.

4.6. Email and internet

4.6.1. The Tabor e-mail system is a core business application. It should not be used for political, business or commercial purposes not related to the College.

4.6.2. The e-mail system and Internet must not be used to send or access illegal or inappropriate material such as pornographic or other improper material. Any such behaviour will lead to disciplinary action which may include termination.

4.6.3. Limited personal use of email and Internet is permitted. Managers must ensure there is no abuse of this privilege.

4.6.4. Global distribution lists should be used appropriately. All staff emails should be used only for business purposes.

4.6.5. Staff members are responsible for minimising the number of messages in their email in-box to ensure maximum efficiency of the delivery system. Folders can be set up and messages filed accordingly.

4.6.6. An automated archiving facility has been set up by the DLIT for staff use.

4.6.7. Archive folders should be kept to a maximum of 750MB to prevent accessing problems from occurring.

4.6.8. Caution must be exercised in sending confidential material by e-mail and must be so marked.

4.6.9. Tabor retains the right to access and view all Emails sent and received by the Email system. This right is exercised solely through the DLIT on the instructions of the Executive.

4.6.10. Staff must not subscribe to chat rooms, dating agencies, messaging services or other on-line subscription Internet sites unless they pertain to work duties.

4.7. Tabor Website

4.7.1. Faculty administrators will communicate with the marketing team regarding any changes to the College's website that the faculty would like to see implemented.

4.7.2. Marketing will check the changes ensuring the required marketing standards are met.

4.7.3. The Registrar will check the changes for compliance and accuracy, and publish to the website

5. Definitions

See **Global Definitions**

6. Communication / Training

6.1. All staff, upon request, will be given appropriate training and offered professional development opportunities in relation to their roles and responsibilities.

6.2. The communication of this policy is the responsibility of Deans of Faculties / Departments