1. **Purpose of Policy**

The purpose of this policy is to outline the obligations of Employees and Apprentices with regards to information technology usage. This document will provide Employees and Apprentices with a code of practice relating to the use of electronic equipment, services and applications.

1. **Scope**

This policy will apply to all employees and apprentices of the College.

1. **Policy Statement**
	1. **Authorisation of Use**

Employees and Apprentices of the College are authorised to use computer equipment and/or software supplied by the College, subject to compliance with the following protocols:

* Prior notice to the Business Services Department that a Employee has

been officially employed by the College and a Apprentice has been officially enrolled by the College;

* A request or authorisation for access to equipment or software (including the College’s corporate network) has come from a member of the EMT or HR;
* The Employee and Apprentice is made aware of which computers, software and such other IT equipment they are entitled to use and for what purposes; and
* The Employee and Apprentice is made aware that usage of computers, services and software is monitored to identify any breaches of this policy.

Once the above requirements have been met, the Employee and Apprentice then have access to College’s computer equipment and software for:

* The conduct of official business;
* Professional or Educational duties;
* Limited personal use (See section 4.8).
	1. **Security, Privileges and Passwords**

It is the responsibility of the Business Services Department to:

* Provide, maintain and monitor the necessary hardware and software e.g. Anti-virus to minimise risks.

Employees and Apprentices with access to computer equipment and software must comply with the following security requirements:

* Network passwords must not be shared with any other parties, including other Employees and Apprentices. The Business Services Department must be consulted should any problems arise concerning data or program access;
* Passwords should not be retained in written form for any reason;
* Employees and Apprentices must not attempt to install or remove software or hardware onto a computer without prior approval and direction from the Business Services Department;
* Employees and Apprentices must not attempt to access, copy, damage, delete, insert or alter any information held on a computer unless authorised by the Business Services Department;
* Employees must not attempt to compromise the security, integrity or availability of the College’s IT systems, or bypass security measures in place.
* Employees and Apprentices must not attempt to obscure their identity when using a computer (E.g. An Employee or Apprentice must not send email using another person’s email account);
* Employees and Apprentices must not attempt to obscure any identifying features of information sent (e.g. Altering the time on an email message);
* Any information from outside sources including, but not limited to, CD-ROMS, floppy discs and email, must be scanned for viruses using the scanning software supplied by the College for that purposes before being exposed to the network; and
* Employees and Apprentices must protect their access to the network and ensure their workstation is locked when unattended at any time;
* Suspicious emails should not be opened. Instead, the IT Department should be contacted for advice on how to proceed.
* Any loss or theft of a College-issued device must be reported promptly to the IT Department for immediate action. Time is often a critical factor in securing or recovering a missing device, and often makes the difference between a successful or non-successful resolution.
* Should an employee become aware of a security risk or breach, they must immediately report it to the IT Department.
* Employees and Apprentices must log out of the network and shutdown their workstation at the completion of the day’s work without fail, and within any timeframes that may apply from time to time.

Persons who are not employed by the College must not be given access to the College’s network under any circumstances, unless approval is first sought and obtained from the Business Services Department. This includes work experience Apprentices, volunteers, temporary staff etc.

Where approval to access equipment and software is conditionally given, such persons are not permitted to use an existing user’s login or password. In such circumstances, the Business Services Department will arrange a guest account with the appropriate security privileges.

* 1. **Email**

With respect to Email messages sent via the College’s internal network, or via Internet email, Employees and Apprentices must not;

* Send defamatory, harassing and discriminatory messages;
* Disseminate jokes, pictures or any other form of communication which may be considered offensive or pornographic;
* Disseminate messages without authority that may cause people to fear for their safety or for the safety of others; and
* Disseminate any information, messages or the like of any kind which would in any way to be likely to bring the College’s name into disrepute.

Employees and Apprentices must not access or attempt to access, another Employee or Apprentices email file without authorisation from the Chief Executive Officer.

The Business Services Department will not allow themselves access, or give anyone access to other Employee’s email files unless one of the following conditions are met:

* The Employee is aware that his or her email file is to be accessed and have given permission, whether written or verbal, to the Business Services Department or the Chief Executive Officer or
* The request comes directly from the Employee’s supervisor and the Chief Executive Officer is aware of the situation and have given approval or
* The request comes directly from the Chief Executive Officer.

Employees and Apprentices are reminded of the College’s policies and procedures concerning sexual harassment, anti-discrimination, harassment and bullying which are identified in the College’s Sexual Harassment and Discrimination Policy, Harassment and Bullying Policy and Equal Opportunity Policy. These documents are available for inspection by all Employees and Apprentices, either via the Intranet, or by contacting the Human Resources Officer.

Employees and Apprentices are reminded that the dissemination of inappropriate material by email or from the Internet can constitute sexual harassment and defamation, and breach anti-discrimination and associated legislation.

Staff and students should refer to their Code of Conduct Policy and Procedure for guidance on appropriate behaviours which includes the use of social media.

* 1. **Internet Access**

The following rules apply when using the College’s network or internet services;

* Employees and Apprentices must not use the Internet to obtain personal gain/profit, either directly or indirectly. This includes advertising or selling of personal equipment, or the purchases of items via online stores;
* Employees and Apprentices must not use the Internet to solicit, discuss, advertise, sell, trade or otherwise deal in illegal materials or activities;
* Employees and Apprentices must not access, download, store or distribute pornography of any kind;
* Employees and Apprentices must not use the Internet for gambling purposes;
* Employees and Apprentices must not access, download or transmit defamatory, harassing and/or discriminatory website material or files;
* Employees and Apprentices must not use the Internet to access Internet chat & messaging clients or Internet Relay Chat (IRC) networks including but not limited to IRCnet and Freenode; and
* Employees and Apprentices must not use the Internet to access streaming radio & media clients or streaming media networks including but not limited to internet radio and TV stations such as ABC iView when not business related; and
* Employees and Apprentices must not use the Internet to access social networking sites of any kind including but not limited to Ebay, Facebook, My Space, Bebo; and
* Employees and Apprentices must adhere to copyright laws as they pertain to information distributed on the Internet.
	1. **Ownership of Information**

State and Federal copyright and intellectual property legislation must be adhered to when using College equipment and software. This applies to information, page design, graphics or photos, documents and software downloads, and any other items or information which may be copyrighted. Permission must be sought from the appropriate authority before downloading or copying information where copyright permission is unclear.

Employees and Apprentices must not:

* Download from the Internet or otherwise obtain information resulting in breach of copyright;
* Intentionally copy unauthorised copyright protected material or infringe licence agreement and/or other contracts;
* Undertake any unauthorised use, such as unauthorised preproduction of a cartoon in a presentation or having a copy of a computer programs, or part thereof or documentation that would normally require payment of a fee for its use; and
* Represent personal opinions as those of the College, or otherwise fail to comply with College’s practices concerning public statements about its position.

Any information created, received or stored on a computer, locally or on the network, is the property of the College, and Employees and Apprentices cannot claim any right of confidentially or privacy in relation to such information.

* 1. **Occupational Health and Safety**

It is the Business Services Department’s responsibility to ensure:

* Employees and Apprentices are aware of any relevant issues pertaining to the correct handling and usage of computer hardware;
* That cabling is arranged tidily so as not to present a health or operational hazard;
* That monitors are low radiation; and

It is the Employees and Apprentice’s responsibility to ensure equipment is used in accordance with guidelines stipulated by this policy, such other protocols and best practice procedures as required and adopted from time to time

* 1. **Education and Training**

It is the responsibility of the Business Services Department to:

* Ensure Employees and Apprentices are made aware of the contents and purpose of this policy, and compliance requirements of the policy;
* Train Employees and Apprentices to use communication and information devices (including new devices and new methods of using existing devices) in a way that is consistent with this policy;
* Provide Employees and Apprentices with training in new technology as and when it is required and/or where particular circumstances warrant.
	1. **Limited Personal Use**

Limited personal use is available to College Employees only. Apprentices are prohibited from accessing College Equipment and Software for personal use.

Employees undertaking an approved work-related study course are permitted to use computer equipment and software, including access to the Internet, for limited personal use related to their area of study. This usage will be monitored for misuse in terms of accessing illegal or offensive material (including pornography, illegal substances, or other objectionable topics).

Limited personal use is defined as usage which:

* Incurs minimal additional expense to the College;
* Generally is expected to take place during the Employee’s non-work hours;
* Does not interfere with the operation of the College; and
* Does not violate any State or Federal legislation and regulations.

Employees must be aware of the following in relation to limited personal use of the College’s computer equipment, services and software:

* Employees have a responsibility to be ethical and efficient in their use and management of all College resources at all times;
* The privilege of using College Equipment and Software for personal use may be revoked or limited at any time for a breach of this policy by an Employee.
* Authorised Officers may revoke or limit, permanently or temporarily, such personal use; and
* Employees must not use College Equipment or Software to maintain or support a private business of any description.
	1. **Monitoring and Auditing of Equipment and Software**

Employees and Apprentices should be aware that:

* Computer usage including Internet access and Internet email will be monitored by the Business Services Department to identify any breaches of this policy. This includes monitoring personal use of Computer Equipment and Software continuously;
* Logs will be kept indicating Internet sites Employees and Apprentices have visited. Authorised Officers will be the only Employees access/and or analyse these logs;
* Authorised Officers will reserve the right to recommend to the Chief Executive Officer that an Employee has their Internet Access discontinued on the basis of any findings from these logs;
* Authorised Officers can access the content of Employee’s electronic files or email only if permission is obtained from the Employee or the request is approved by the Chief Executive Officer (see section 4.3 for more information on this process);

# Definitions

**College** means Tec-NQ Ltd.

**Computer Equipment and Software**

Any electronic equipment or computer software whatsoever, provided to Employees and Apprentices for use in the performance of their duties, either in general or specific terms, including, but not limited to:

* A computer, including PC’s, laptops/notebooks and handheld computing devices;
* A printer;
* A fax;
* A USB “stick” or thumb drive;
* A scanner;
* A mobile phone;
* A digital camera or any other digital imaging equipment;
* All software and programs provided to facilitate work needs;
* Network operating systems;
* Electronic mail (all forms including use of Internet Email);and
* Internet access

**Employees**

All persons engaged, whether on a permanent, temporary, or fixed term basis, as well as contractors engaged to work for or on behalf of the College. For the purpose of this policy, Employees includes company Directors and Board members of the College.

**Apprentices**

All Apprentices enrolled at the College.

**Authorised Officer(s)**

Are allthe following positions; Chief Executive Officer; Members of the Executive Management Team and Members of the IT Department.

# Legislation

* Copyright Act 1968 (Cth)
* Freedom of Information Act 1982 (Cth)
* Libraries and Archive Act 1988 (Qld)
* Criminal Code Act 1995 (Cth)
* Anti-Discrimination Act 1991 (Qld)
* Anti-Spam Act 2003 (Cth)

# Related Documents

* Child Protection Policy and Procedure
* Staff Code of Conduct Policy and Procedure
* Student Code of Conduct Policy and Procedure
* Board Code of Conduct Policy and Procedure
* Harassment and Bullying Policy and Procedure
* Access and Equity Policy and Procedure
* Privacy Policy and Procedure
* Complaints Policy and Procedure
* Selection, Recruitment and Enrolment Policy and Procedure
* Sexual Harassment and Discrimination Policy and Procedure
* Information Technology Acceptable Use Policy
* Digital Marketing Policy and Procedure

# Related Systems

* Tec-NQ Document Management System
* Tec-NQ Support Desk

# Publication

Distributed to all staff and students via the Tec-NQ DMS.

# Policy Release Details

Date of Policy Release: 25/2/2022

Review Date: 25/2/2024

Recommended by: Stacey Cox - Business Compliance & Projects Mgr

Approved by: Julie Hyde, Chief Executive Officer

Approval Date: 25/2/2022

Version: 2

CIR Number: 4698