P.11	**IT SERVICES ACCEPTABLE USE POLICY**		
APPROVED BY	**STRATEGIC LEADERSHIP TEAM**	VERSION	**2017-v1**
REVIEW STAKEHOLDERS	▪ HEAD OF OPERATIONAL SERVICES	Last reviewed	2017
	▪ DEAN	Published	2017
	CLICK HERE TO ENTER TEXT. TITLE	Review period	3 YEARS
	CLICK HERE TO ENTER TEXT. TITLE	Next review	2020
PURPOSE	Bethlehem Tertiary Institute's (BTI) information systems, including (but not limited to) electronic devices, computers, computing software, photocopiers, printers, voicemail, email and access to the Internet, are provided as tools in support of the programmes at BTI. This policy is designed to guide students and staff in the acceptable use of computer systems, networks and other information technology resources at the institute.		

1 PURPOSE

Bethlehem Tertiary Institute's (BTI) information systems, including (but not limited to) electronic devices, computers, computing software, photocopiers, printers, voicemail, email and access to the Internet, are provided as tools in support of the programmes at BTI. This policy is designed to guide students and staff in the acceptable use of computer systems, networks and other information technology resources at the institute.

2 SCOPE

This policy applies to any user (staff, student or other) of BTI's Information Technology (IT) resources, whether initiated on or off the institute's premises. This includes any electronic device, telephone, digital service, computer and information system or resource, means of access, networks (including internet and WiFi), and the data residing on BTI's internally and externally hosted systems. This policy applies to the use of all IT resources.

3 POLICY PRINCIPLES

Telephones, electronic devices, digital services, computers and networks provide access to resources on and off BTI's campus, as well as the ability to communicate with other users worldwide. Users must respect the rights of other users, respect the integrity of the systems and related physical resources and observe all relevant laws, regulations, contractual obligations and behavioural guidelines that exist in relevant or associated polices.

The BTI community is encouraged to make innovative and creative use of information technologies in support of educational, scholarly and administrative purposes. BTI supports access to information representing a multitude of views for the interest, information and enlightenment of students, faculty and staff. Consistent with this policy, BTI supports the use of information technology resources in a manner that recognises both the rights and the obligations of academic freedom.

The institute recognises the importance of copyright and other protections afforded to the creators of intellectual property. Users are responsible for making use of software and other information technology resources in accordance with copyright and licensing restrictions and applicable institute policies.

BTI cannot completely protect individuals against the receipt of some potentially offensive material. Those who use electronic communications occasionally may receive material that they might find offensive. Those who make personal information available about themselves through the Internet or other electronic media available at the institute may expose themselves to potential invasions of privacy.

Users should remember that information distributed through the institute's information technology resources may be considered a form of publication. Although BTI does not take responsibility for

material issued by individuals, users should recognise that third parties
may perceive anything generated at the institute as in some manner having been produced under BTI auspices. Users are reminded to exercise appropriate language, behaviour, and style in their use of information technology resources.

Information technology resources are provided to support BTI's scholarly, educational, and administrative activities. Information technology resources are limited and should be used wisely and with consideration for the needs of others.

4   POLICY

Authorised Use:
1. Access and use of BTI's IT resources is granted to staff and students in support of their studies, instruction, and duties as employees or official businesses with the institute, and other approved activities.

2. For approved purposes or projects and for other brief activities that are clearly reasonable and do not conflict with any of the points of this policy, employees and students of BTI are permitted to use the equipment for occasional non-institute related purposes with this caveat: Use of BTI's IT resources may not be transferred or extended by members of BTI's community to outside individuals or groups.

3. It is important that the use of the institute's IT resources is dedicated to its educational purpose. Because of this, use which involves hosting or serving unauthorised commercial activities, personal or political gain, private business, fundraising, or uses otherwise unrelated to BTI are not permitted.

4. Gaining access to BTI's IT resources does not imply the right to use those resources. Unauthorised access and use could subject the user to possible civil charges, criminal charges or institute disciplinary actions.

User Responsibilities:
1. Users are expected to use all IT resources in a responsible manner. Users should take appropriate precautions to ensure the security of their usernames and passwords, preventing others from obtaining access to their computer resources.

2. Users may not encroach on others' use of IT resources. Such actions include, but are not limited to, tying up IT resources unnecessarily; sending frivolous or excessive messages including chain letters, junk mail (spam), electronic chat and other similar types of broadcast messages; using excessive internet bandwidth such as downloading large multimedia files; streaming movies for entertainment; and/or using excessive amounts of storage or data.

3. Responsible use also means avoiding some activities which are specifically prohibited while using Institute IT resources, including computers and networks owned or operated by BTI, or to which BTI is connected. These include:
    *   Modifying system or network facilities, or attempting to crash systems or networks;
    *   Using, duplicating or transmitting copyrighted material without first obtaining the owner's permission, in any way that may reasonably be expected to constitute an infringement, or that exceeds the scope of a license, or violates other contracts;
    *   Tampering with software protections or restrictions placed on computer applications or files;
    *   Sending messages that are malicious or that a reasonable person would find to be harassing;
    *   Subverting restrictions associated with computer accounts;
    *   Using information technology resources to obtain unauthorised access to records, data, and other forms of information owned, used, possessed by, or pertaining to the institute or individuals;
    *   Accessing another person's IT resource or digital account without authorisation;
    *   Altering electronic communications to hide one's identity or to impersonate another individual. All email, news posts, chat sessions, or any other form of electronic communication must contain the sender's real name and/or user ID (except where these communications are explicitly anonymous, as for example with online course evaluations);

- Intentionally introducing computer viruses, worms, Trojan Horses, malware or other rogue programs into information technology resources;
- Installing software or running any unauthorised software from an external source;
- Physically damaging IT resources;
- Using or encouraging others to use IT resources in any manner that would violate this or other Institute policies or any applicable New Zealand law; and
- Falsely reporting or accusing another of conduct that violates this policy, without a good faith basis for such an accusation.

Data Privacy and Policy Implementation:
1. The institute encourages all members of its community to use electronic resources in a manner that is respectful of others. While respecting users' privacy to the fullest extent possible, BTI reserves the right to access any BTI IT resource or examine any electronic data stored in or transmitted through its systems. BTI reserves this right for bona fide purposes, including, but not limited to:
   - Enforcing polices against harassment and threats to the safety of individuals;
   - Protecting against or limiting damage to institute information technology resources;
   - Complying with a court order, subpoena or other legally enforceable discovery request;
   - Investigating and preventing the posting of proprietary software or electronic copies of texts, data, media or images in disregard of copyright, licenses, or other contractual or legal obligations or in violation of law;
   - Safeguarding the integrity of computers, networks, software and data;
   - Preserving information and data;
   - Upgrading or maintaining information technology resources;
   - Protecting the Institute or its employees and representatives against liability or other potentially adverse consequences.

Internet filtering and email restrictions:
1. BTI reserves the right to block certain categories of internet content as well as specific sites.

2. BTI reserves the right to send electronic communications, including large group or broadcast email messages, to its own users. The institute also reserves the right to limit the size of individual messages and attachments being transmitted through the network resources.

Policy Enactment Processes:
1. An individual's use of IT resources and/or network connection privileges may be suspended immediately upon the discovery of a possible non-compliance with these policies. This suspension does not reflect an assumption of guilt but the need to protect the integrity of BTI's IT resources and systems.

2. The BTI Dean will determine whether the policy non-compliance is evidenced.

3. Non-compliance with these policies will be dealt with in the same manner as breaches of other institute policies and may result in disciplinary review.

4. Suspected violations of this policy should be reported to BTI's Head of Operational Services, who will, in consultation with BTI's IT support staff and other relevant staff, decide on appropriate action. BTI's Head of Operational Services must be notified for all non-compliance.