

POLICY			
Information and Communications Technology			
Date of approval	December 2015	Approved by	EMG
Date of effect	December 2015	Current to	December 2018
Registered no	SCS010	Version	v1.2 2015
Policy Owner	Executive Director, Strategic and Shared Services		
Contact Officer	Manager ICT		

1. Outline

This Information and Communications Technology (ICT) policy is intended to support the achievement of the Batchelor Institute of Indigenous Tertiary Education (the Institute) Strategic Objectives by encouraging the best practice use of ICT; minimising risks, including those of inappropriate use of ICT; and minimising real and potential loss or harm to the Institute, staff, students and stakeholders.

2. Summary

This policy applies to all users and uses of Institute ICT and outlines the relevant responsibilities.

3. ICT Policy

3.1 The Institute provides staff and students access to ICT to support employment and study. This may not necessarily require the issue of ICT to individuals. Where ICT is issued to individuals this will be on the basis of a 'Standard Issue' as outlined in the ICT Equipment and Costing Guideline. Standard issue ICT will be funded from the Corporate ICT Cost Centre. ICT above, or in addition to, the standard issue or Standard Operating Environment (SOE) will require the approval of the respective Executive Director and funding from the Business Unit Cost Centre.

3.2 Access to reasonable personal use of ICT is provided to Institute staff, students and visitors as a privilege, not a right, and may be withdrawn at any time. The personal use of Institute ICT resources and time must not:

3.2.1 Interfere with Institute operation of ICT;

- 3.2.2 Burden the Institute with incremental costs;
 - 3.2.3 Interfere with the user's employment or other obligations to the Institute,
 - 3.2.4 Infringe any other condition of employment, and
 - 3.2.5 Be used for personal benefit, outside employment with the Institute.
- 3.3 Institute ICT must not be used in any way that:
- 3.3.1 Breaches any applicable laws or other Institute policies and specifically must not contain any offensive or disruptive content about culture, race, gender, age, sexual orientation or explicit material, religious or political beliefs, national origin, disability or pornography.
 - 3.3.2 Risks or results in a financial, reputational or capacity (including health and environmental) loss or harm to the Institute, its staff or students.
 - 3.3.3 Breaches employment conditions, or
 - 3.3.4 Breaches the Staff or Student Codes of Conduct.
- 3.4 All users of Institute ICT must comply with relevant Institute policies, guidelines and procedures, specifically, but not limited to, Codes of Conduct, ICT security and operations, data quotas, resource management, procurement, Work Health and Safety, bullying and harassment, Privacy, Intellectual Property (including copyright).
- 3.5 All ICT resources purchased by the Institute, irrespective of the funding source, remain the property of the Institute. In addition:
- 3.5.1 All new ICT purchased must be registered in the ICT Asset Register before use.
 - 3.5.2 With the exception of 'standard issue' ICT all new hardware, software, network or device purchases must be approved by the Manager ICT, or delegate, before the Purchase Order or Credit Card is used.
 - 3.5.3 Installation of software requires the permission of the Manager ICT, or delegate, before proceeding.
 - 3.5.4 Mobile Apps do not require permission before installation, however they must not interfere with the operation of Institute ICT Resources nor incur cost to the Institute.
 - 3.5.5 ICT resources purchased through a grant or project must be returned to the Manager, ICT, or delegate, at the end of the grant or project and added to the ICT resources loan pool.
 - 3.5.6 All ICT resources issued to a staff member, student or contractor must be returned to the Manager ICT, or delegate, on resignation, completion of contract or studies, or prior to starting Long Service, maternity/paternity or extended Leave.
 - 3.5.7 All transfers of ICT resources between personnel, projects or business units must be facilitated through the Manager ICT or delegate.

- 3.6 A user is not permitted to provide another person with their access details for any facility protected by user identification or password. This includes allowing non-staff members access through the Northern Territory Government firewall or to shared network drives.
- 3.7 Only authorised system administrators may alter, adjust or otherwise configure the ICT network, add a device to the network, add or remove software, firmware or hardware, or grant access to the system.
- 3.8 Staff and students are personally responsible for any loss or harm suffered by any party as a result of their inappropriate use of Institute ICT or resources. The Institute is not responsible for any loss or harm suffered by any party as a result of the inappropriate use of ICT resources by a user.
- 3.9 While staff and students may be granted reasonable use of Institute ICT for personal communications, this does not convey any additional right or expectation of privacy, and, subject to applicable laws of Australia and the Northern Territory, authorised persons may, but are not obligated to, record any use of Institute ICT (including personal communications made using Institute ICT resources) and the recording may be stored, accessed, reviewed, copied and tended as evidence for legitimate purposes, including disciplinary or legal proceedings, by persons with a right to do so.
- 3.10 The Institute reserves the right to (without notice):
- monitor the use of any device or application,
 - inspect any data residing on any Institute-owned resource (regardless of data ownership and including electronic mail and other forms of communication),
 - capture and inspect any data in any ICT infrastructure owned or controlled by the Institute,
 - copy or backup data in any networking infrastructure,
 - with prior permission of the data owner delete or modify any data in any networking infrastructure, and
 - re-image devices as and when required.
- 3.11 All managers and staff are responsible for the management of information security risks relevant to their duties and areas of responsibility. Managers at all levels are required to create an environment where managing information security risk is accepted as a personal responsibility of each member of the Institute.
- 3.12 The Institute will adopt an ICT Governance structure to provide advice to Institute management on the development of the Institute's ICT systems, including issues related to infrastructure, services, procurement, applications and risk.
- 3.13 All staff and students must report any instance of an apparent breach of this policy to the Manager ICT.
- 3.14 Breach of this policy may result in disciplinary action by the Institute, including termination of employment or enrolment, in addition to any other private or criminal legal action.

4. Responsibilities

Executive Management Group

Oversight of Institute ICT Operations, and
Approval of the ICT Strategic Plan.

Executive Director, Strategic and Shared Services

Policy Owner of the ICT Policy, and
Senior Executive responsible for approving ICT and related Guidelines and Procedures.

Executive Directors

Approval of any non-standard issue ICT, and
Funding of any non-standard issue ICT.

Manager ICT

Management, and provision of advice, regarding the ICT operations and resources of the Institute,
Management of ICT contracts,
Development of the ICT Strategic Plan,
Identification and advice regarding ICT risks and mitigation strategies, and
Investigation of breaches, or allegations, to ICT security and inappropriate or unacceptable use of Institute ICT resources.

All Users

Responsible for the appropriate use of ICT resources and compliance with this policy, and
Responsible for all activity initiated from their account.

5. Acronyms & Terms

Acronym/Term	Definition/Description
ICT	<p>Information and Communications Technology (ICT) and includes All ICT resources and facilities operated by the Institute whether owned, leased, used under licence or by agreement - including, but not limited to:</p> <ul style="list-style-type: none">• telephones (including mobile devices) and telephone equipment, voice mail, SMS;• mobile data devices;• desktop, laptop, tablet or other portable computing devices,• cameras, video and audio visual devices,• email, chat, facsimiles, mail; social media,• any connection to Institute networks, or use of any part of

Acronym/Term	Definition/Description
	<p>those networks to access other networks;</p> <ul style="list-style-type: none"> • connections to the Internet or mobile networks that are intended to fulfil information processing and communications functions; • all software; • communication services; • all hardware, including printers, scanners, facsimile machines; storage devices or RAID, • laboratories or other facilities; • any off-campus computers and associated peripherals and equipment provided for the purpose of Institute work or associated activities; • usage of remote systems accessed via ICT facilities; or • the use of information that may be accessed via ICT resources
Mobile App	A computer program designed to run on smartphones, tablet computers and other mobile devices.
User	<p>Any person using any of the Institutes ICT resources or facilities, including, but not limited to:</p> <ul style="list-style-type: none"> • staff, • students, • adjuncts, associates, honoraries and visiting staff, • alumni, • consultants or contractors, • third parties, • those persons using the Batchelor library, • other users who are authorised by the Institute to access its systems and/or network, or • anyone connecting non-Institute owned equipment (e.g. laptop computers) to the Institute network. <p>A member of the public reading public Institute web pages from outside the Institute is not by virtue of that activity alone considered to be a user.</p>
Unacceptable Use, or Inappropriate Use	Any action that contravenes the provisions of the ICT Policy set out in Section 3.

6. Supporting Documents

- ICT Equipment Issue and Costing Guideline
- Staff Code of conduct

- Student Code of Conduct
- Privacy Policy
- Intellectual Property Policy
- Copyright Policy
- Communications Standards Policy

7. Related documents

- *Information Act (NT)*
- *Fair Work Act 2009*

8. Modification history

<i>Date</i>	<i>Version</i>	<i>Sections modified</i>	<i>Authority</i>	<i>Details</i>
Nov 14	1	New policy	EMG	
Sep 15	1.1	Logo, Heading, S6, S7		Change to new logo Change of titles due to organisational change Separation of supporting & related documents
Dec 15	1.2	3.1; 4	EMG	Clarifying issues and funding of ICT Adding responsibilities of Executive Directors

9. Feedback

If you have any comments or feedback about this Policy, please contact the Manager ICT.