

## Acceptable Use of ICT Policy

<b>Policy Category</b>			
<b>Document Owner</b>			
<b>Responsible Officer</b>	Registrar		
<b>Review Date</b>			
<b>Related Documents</b>	<i>Discrimination, Bullying and Harassment Prevention Policy</i> <i>Fraud and Corruption Control Policy</i> <i>Fraud and Corruption Control Procedure</i> <i>Health and Safety Policy</i> <i>Health and Safety Procedure</i> <i>Learning Technologies Policy</i> <i>Staff Code of Conduct</i> <i>Staff Misconduct Procedure</i> <i>Student Code of Conduct</i> <i>Student Misconduct Procedure</i>		
<b>Version</b>	<b>Authorised by</b>	<b>Approved</b>	<b>Effective Date</b>
1.2			

### 1. Context

This Policy supports Waratah Institute (the 'Institute') commitment to providing a secure and reliable information and communications technology service.

### 2. Definitions

Affiliate: any person appointed or engaged by Waratah Institute to perform duties or functions for the institution other than students and staff, and including members of advisory committees and governing bodies, contractors, consultants, and agency staff.

Information and Communications Technology (ICT) facilities or resources: systems, software, hardware and services, including data files, information systems, and services such as internet access and email.

User: any individual who uses any ICT system, hardware or service owned or leased by Waratah Institute.

### 3. Scope

This Policy applies to Waratah Institute's students, staff and affiliates.

### 4. Policy Principles

The key principles informing this Policy are:

- proper authorisation for use Waratah Institute's ICT facilities;
- responsible, ethical, professional and lawful behaviour of students and staff while using the Institute's ICT facilities; and
- no damage to ICT facilities or intentional disruption to ICT services.

## 5. Policy Details

### 5.1. Authorised Users

Waratah Institute's ICT resources may only be used by authorised users. Unauthorised access to ICT facilities is prohibited and may result in either disciplinary action or criminal prosecution.

Authorised users may use the Institute's ICT resources in the course of discharging their responsibilities as employees, to further their studies as students, to conduct official business, or other sanctioned activities. The Institute expects the following from users of its ICT resources:

- that users only use their own account and password and do not attempt to access any file or program stored under another's ICT account;
- that users do not provide their password or login to others or attempt to obtain unauthorised access to the password of others; and
- that users keep their passwords and login secure and confidential.

### 5.2. Conditions of Use

All users of Waratah Institute's digital communication resources are expected to abide by the relevant *Code of Conduct* and, in particular:

- conduct themselves in a respectful, fair and ethical manner;
- be considerate when using the Institute's resources, property, and facilities;
- use the Institute's resources in a proper and efficient manner;
- use their right to academic freedom in a manner consistent with a responsible and honest search for, and dissemination of, knowledge and truth; and
- use ICT devices appropriately and for learning purposes.

Users must not use the Institute's ICT resources for:

- commercial or private gain;
- preparing, storing, receiving or transmitting any material that is may be considered sexist, racist, obscene, pornographic, discriminatory or intimidating;
- engaging in any behaviour which may be unwelcome or may victimise, offend, humiliate, vilify, or intimidate others regardless of intent;
- disseminating any material that is unlawful;
- disclosing personal information without permission; or
- unlawfully copying software or uploading or downloading material that is licenced or protected by copyright.

All users are required to treat ICT resources at the Institute with care and respect. Users must not:

- vandalise, damage, destroy or tamper with ICT facilities, resources or services;
- use ICT resources to gain unauthorised access to other computers, networks, systems, files or data; or
- subvert or deliberately compromise the integrity and security of ICT resources.

### **5.3. Monitoring**

In the course of providing a secure and reliable ICT service and ensuring compliance with its legislative obligations, Waratah Institute may audit or monitor the use of ICT facilities and services and may view data stored on these facilities and services, as well as material received or transmitted via these facilities, including email.

### **6. Necessary action**

The Chief Executive Officer has the authority to take necessary action that protects computing and information systems and to restrict email, network or software application threats and malware.

The Registrar may authorise access to any Waratah Institute records or block any of the Institute's email addresses without consent of any holder of the email when:

- required by, and consistent with, law;
- the Registrar has substantiated reason to believe that violations of law or the Institute's policy have taken place; or
- in exceptional cases, to meet time-dependent, critical operational needs.

### **1. Breaches**

If a student or staff member is found to be in breach of this Policy, she or he may be subject to disciplinary action in accordance with the relevant *Code of Conduct* and *Misconduct Procedure*, which can be accessed from the Waratah Institute's website.

### **2. Appeals**

Appeals concerning any decision taken in relation to this Policy should be made under the relevant *Complaints and Appeals Policy*, which can be accessed from the Waratah Institute's website. Overseas students may lodge an appeal with the Overseas Students Ombudsman.

### **7. References**

*Copyright Act 1968 (Cth)*

*Crimes Act 1900 (NSW)*

*Cybercrime Act 2001 (Cth)*

*Privacy Act 1998 (Cth)*

*Spam Act 2003 (Cth)*

*Workplace Surveillance Act 2005 (NSW)*

### **8. Acknowledgements**

In developing this policy, Waratah Institute acknowledges:

- *Macquarie University, Acceptable Use of IT Resources Policy and Procedure.*

**Document History:**

Version	Date	Author	Reason	Sections
0.1	29/9/2017		Approved by Management Committee	All
1.0		Julien Marechal	Amended as per the Executive Management Committee's comments at its 03/07/18 meeting	All
1.1	13/08/19	Julien Marechal	Revised in response to TEQSA feedback and approved by the Executive Management Committee 13/8/19.	6.
1.2	17/12/2019	Philippa Ryan	Amended to reflect new trading name 'Waratah Institute'.	All

