ANZSOG

PROVISION AND ACCEPTABLE USE OF ITC POLICY

Table of Contents

1. OBJECTIVES

The objectives of this policy are to:

a) outline the principles that apply to the management and use of computing and network facilities across ANZSOG – through a positive and empowering frame;
b) support efficient processes and enhance staff and stakeholder experience with ITC tools;
c) define the expectations of users of ANZSOG information technology systems and restrictions on use; and
d) provide authority for ANZSOG to investigate and act on allegations of misuse.

2. SCOPE

2.1 This policy applies to the provision of, and all users of, ANZSOG information technology services, equipment and connectivity, including:

a) participants
b) staff
c) contractors and consultants
d) visitors.

2.2 This policy applies to all uses of ANZSOG networks or connectivity services, including using a user-owned device to connect to the system.

3. DEFINITIONS

Term	Definition
Appropriate and responsible manner	Broadly considered in the context of 'Authorised use' and 'Misuse'. Common sense should also prevail, for example: it is not acceptable to spend hours viewing streaming services for personal use during work hours: users should be aware of potential cost implementation such as leaving on data roaming when travelling abroad. **Refer also to the Social Media Policy**.
Authorised use	means purposes associated with work or study at ANZSOG, provision of services to or by ANZSOG, which are approved or authorised by the relevant officer or employee of ANZSOG in accordance with ANZSOG policies and procedures or pursuant to applicable contractual obligations, limited personal use, or any other purpose authorised by the relevant authority.
Bring Your Own Device (BYOD)	Any electronic device owned, leased or operated by an employee, contractor or affiliate of ANZSOG that is capable of storing data and connecting to a network, including but not limited to mobile phones, smartphones, tablets, laptops, personal computers and netbooks.
Computing and network facilities (facilities)	means computers, computer systems, data network infrastructure, dial-in network access facilities, email and other communications and information facilities together with associated equipment, software, files and data storage and retrieval facilities, all of which are owned or operated by ANZSOG.
Corporate Device	A device owned or leased by ANZSOG.
Data	Data owned, originating from or processed by ANZSOG systems, including any such data stored or processed through a BYOD.

Device (can also be referred to as an Endpoint)	Computing device that communicates back and forth with a network to which is it connected. Examples of endpoints include: desktops; laptops; smartphones; and tablets.
External provider	means an external entity that provides computing and network facilities to ANZSOG.
Information Communication Technology (ICT)	Covers all IT, and all forms of communication including telephony, mobiles, wireless networks, other enterprise softwares, audio visual systems that enable movement or manipulation of data.
Information Technology (IT)	Covers all forms of computers, networks, and information.
Misuse	Use for any purpose other than an authorised purpose is considered to be misuse, for example: use that causes or contributes to a breach of any provision of a law or code of practice or conduct applying to ANZSOG, or to which users are subject use that contravenes an ANZSOG rule or terms and conditions, policy or process creating, transmitting, storing, downloading or possessing illegal material the deliberate or reckless creation, transmission, storage, downloading, or display of any offensive or menacing images, data or other material, or any data capable of being resolved into such images or material, except in the case of the appropriate use of facilities for properly supervised ANZSOG work or study purposes use which constitutes an infringement of any intellectual property rights of another person communications which would be actionable under the law of defamation communications which misrepresent a personal view as the view of ANZSOG, including unauthorised use of the ANZSOG brand deliberate or reckless undertaking of activities resulting in: the imposition of an unreasonable burden on an ANZSOG facility

	corruption of or disruption to data on an ANZSOG facility, or to the data of another person disruption to other users introduction or transmission of a virus into the facilities Loss or damage of ICT equipment, or repeated loss or damage of ICT equipment. Engaging in inappropriate online activities on work devices which compromise the ANZSOG values e.g. hate speech, viewing pornography. NOTE: the policy acknowledges that unintentional human error might be considered misuse but this will be discovered per procedural principles below.
Mobile Device Management (MDM)	Solution that manages, supports, secures and monitors mobile devices.
Partner University	A University with whom ANZSOG has a formal agreement, who may confer ANZSOG's long courses such as the EMPA.
Provider	means ANZSOG department which provides and manages any part of the facilities, in most cases **ANZSOG IT** which is a unit within ANZSOG.
User	means any member of staff, or any other person, who is authorised to use the computing and network facilities.

4. POLICY

Provision of ANZSOG information technology

4.1 ANZSOG computing and network facilities support and enable research, learning and teaching, and engagement, through provision of cost-effective world class infrastructure and customer services.

4.2 Computing and network facilities and related services are responsive to the needs of users.

4.3 ANZSOG computing and network facilities complement and inter-operate with other information technology in the lives of users.

4.4 ANZSOG will only provision an endpoint asset to staff, and not consulting firms or contractors for example.

4.5 Corporate smart phone setup

4.6 ICT will setup each Corporate Devices to ensure all relevant policies are applied.

Use of ANZSOG information technology

4.7 All users are expected to use facilities and services in an appropriate and responsible manner, and make themselves aware of ANZSOG's related ICT policies as and when they become available or updated.

4.8 Users may be exempt from aspects of this policy where it is required for their role, studies or research. Permission from the CIO must be obtained.

4.9 Users must not misuse (see Definitions) ANZSOG computing or network facilities, see below for procedures relating to alleged misuse.

Use of Bring Your Own Device (BYOD)

Users have responsibility for:

- ensuring no other person has access to ANZSOG software or data stored on your BYOD.
- abiding by all licence terms and conditions applicable to any software, apps, data or information provided by ANZSOG to your BYOD.
- reporting your BYOD as lost or stolen as soon as practicable to the IT Service Desk

- backing up and restoring the data and configuration settings of your BYOD. Personal data is not to be backed up or stored by ANZSOG. ANZSOG is not responsible for any personal loss or damage.
- ensuring ANZSOG information is not stored on BYODs and/or unapproved cloud-based services.
- Taking reasonable steps to separate work from personal correspondence and data.
- Installing the app(s) required to access data, and granting permissions required by the app(s) on the BYOD.
- Limited support will be provided for any ANZSOG computing and network facilities:

Support	**BYOD**
Physical provisioning	Device owner
Replacement of defective / damaged device	Device owner
Operating system support including licensing	Device owner
Application support of device including licensing	Device owner
ANZSOG provided / supported mobile applications	IT Service Desk

Device connectivity / access	**BYOD**
Mobile internet	Device owner
Home internet / broadband	Device owner
ANZSOG wireless	IT Service Desk

ANZSOG will apply the following technical controls on BYOD devices for data protection purposes:

- Restrict the apps that can be used to access ANZSOG data.
- Restrict the movement of data. Following are examples of some prevention measures that may be utilised: attachment downloading; the forwarding or sharing of data; blocking data access if staff are located in a high-threat country; controlling access to data using advanced artificial intelligence that defects anomalies.
- ANZSOG will not install services onto the BYOD to apply these controls.
- ANZSOG will have the ability to wipe data (see definitions).

ANZSOG is not responsible for:

- any costs incurred by your use of your BYOD. ANZSOG will not reimburse any voice or data charges, software or application acquisition fees, and support or insurance

costs associated with your device. ANZSOG will replace your own device if it is lost or damaged whilst travelling for work.

- any inconvenience that you may experience in connection with using ANZSOG ICT services on your BYOD.
- any personal loss or damage you may suffer by actions undertaken by ANZSOG to protect ANZSOG data stored on your BYOD.

ANZSOG will not monitor:

- the phone call or text message history of a BYOD. Where needed (for example, in the case of a disciplinary matter) the call and text messages may be requested.
- the web browser history on your BYOD when not connected to ANZSOG's network(s), unless the web traffic is directed through ANZSOG's network infrastructure.

ANZSOG may:

- restrict access to internet websites, services or other elements for operational or policy reasons while your BYOD is connected to ANZSOG networks including either wireless or cabled connections.
- monitor your use of your BYOD while it is connected to ANZSOG network. This information may be collected and archived.
- at its own discretion, de-register any BYOD at any time without warning thereby preventing the BYOD from accessing ANZSOG information.
- through MDM capabilities of Office 365, enforce certain policies on mobile devices, including BYOD, to ensure the security of ANZSOG data. This includes, but not limited to, enforcing screen locks, pin codes and in extreme circumstances, the ability to remotely wipe ANZSOG data.

5. PROCEDURAL PRINCIPLES

ANZSOG provision of services

5.1 ANZSOG IT supports ITC environments which are consistent with agreed standards.

5.2 Support for non-standard environments may be subject to additional charges.

5.3 ANZSOG does not necessarily provide user support or funding for software licensing for a proposed non-standard use of facilities.

5.4 Departments must not make purchases or commitments which have the effect of hindering or preventing transition to common ITC products and services.

5.5 For ANZSOG-owned devices, physical security and protective items such as a secure carry case will be provided.

Lost, Stolen or Damaged Computer Equipment

5.6 In case of loss, theft or damage, the guardian of the asset should immediately notify the Information Technology Services Helpdesk.

5.7 ANZSOG acknowledges that devices can be lost or damaged, and may seek reimbursement from the employee to cover the cost of replacement or repair if deemed misuse.

Privileges and responsibilities of users

5.8 Facilities may be used only for authorised use, in an appropriate and responsible manner per definitions.

5.9 No user may engage in any act or practice, or omit to do any act or practice, which constitutes a misuse of any of the facilities.

5.10 Users are responsible for the physical security and care of their device(s), and for bringing their device into work as a replacement will not necessarily be available.

Specifically prohibited activities

5.11 Users may not:

a) circumvent user authentication or access control measures, security or restrictions on the use of any facilities or account, including the unauthorised distribution or use of tools for compromising security

b) engage in unauthorised reserving of, or exclusion of others from using, any facilities

c) use any facilities for the purposes of any private business whether for profit or not, or for any business purpose other than ANZSOG business, unless allowed for in relevant contract(s).

Removal of material

5.12 ANZSOG IT or a provider may at any time, without prior notice, remove or disable access to any material stored on or accessible via any facilities which it considers constitutes or may constitute, or be in furtherance of, misuse or possible misuse of any facilities.

5.13 Where a person is aggrieved by a decision to remove or disable access to material under this section:

a) they may provide to the CIO a written submission in response to the decision

b) the CIO, or delegate, must consider any such submission in discussion with the affected user's relevant Director and investigate the matter and decide, as soon as

practicable, whether to uphold, revoke or alter the decision, and advise the aggrieved person of that decision

c) in making a decision, the CIO, or delegate, must have regard to the purpose of this policy and the interests of ANZSOG.

Investigation

5.14 In this section, 'investigator' means an authorised representative of a provider or the CIO, or delegate.

5.15 If an investigator considers that an allegation of misuse which is brought to their attention would, if substantiated, constitute a significant and unacceptable abuse of any facilities, then they must do one of the following:

a) investigate the allegation under this section, or

b) if the user is a member of staff, recommend that the allegation be dealt with under the appropriate policy, or

c) recommend that the allegation be dealt with under the provisions of any applicable contract.

5.16 An investigator may, at their discretion, investigate or refer any other allegation of misuse which is brought to their attention, for example to a law enforcement agency.

Outcomes of investigation - reporting

5.17 If, as a result of an investigation under 5.15, an investigator is satisfied on the balance of probabilities that misuse of any facilities has taken place, they must:

a) prepare a written report setting out particulars of the misuse and of the investigation undertaken, and any action taken by the investigator

b) if the investigator is a person other than the CIO, provide a copy of that report to the CIO

c) if the allegation of misuse was made against a member of staff or an honorary, provide a copy of that report to the CEO, the affected user's Director and the Director Human Resources.

Outcomes of investigation - penalties

5.18 If, as a result of an investigation under 5.15 an investigator is satisfied on the balance of probabilities that there has been misuse of any facilities by any staff user, they may, at their discretion, do one or more of the following:

a) decide to take no further action on the alleged misuse

b) counsel the user on appropriate use of the facilities

c) Recommend that the allegation be dealt with under the appropriate code of conduct.

d) if the user is an external user, recommend that the allegation be dealt with under applicable provisions of any contract or otherwise as determined by the CFO, or CEO
e) require the user to indemnify or compensate ANZSOG or a provider for the reasonable loss and damage occasioned by reason of the misuse
f) if the misuse results in a breach of privacy, refer to the relevant privacy breach process.

User responses and appeals

5.19 Where a decision has been made regarding an allegation of misuse:

a) the investigator must notify the affected user, in writing, as soon as practicable, of the decision, with reasonable particulars, and of the right of appeal
b) the investigator must provide the CIO with a copy of the notice as soon as practicable or, if the investigator is the CIO, they must provide the notice to the role in charge of the relevant work unit/team, if relevant.

5.20 If the affected user is a staff member:

a) the affected user may, within seven business days of receiving the notice, provide to the CIO, or, in the case of the CIO being the investigator, provide to the CFO a written submission in response to the decision.
b) the CIO or the CFO, as appropriate, must consider the decision and such submission in response and decide, within seven days of receipt, whether to uphold, revoke or alter the decision, and advise the affected user of his or her decision as soon as practicable.
c) a decision by the CIO or CFO, or delegate is final. Where an allegation of misuse has been made against a member of staff, the Director, Human Resources, or delegate, will be consulted before making a decision if practicable to do so.

6. ROLES AND RESPONSIBILITIES

Role/Decision/Action	Responsibility	Conditions and limitations
Use all ITC facilities appropriately, lawfully and in compliance with this and other relevant policies and rules of ANZSOG	Users	
Provide reliable, secure access to the ITC services or facilities in their control Ensure they and their staff do not access data or information passing through the system except as required by policy, rule or law Perform all required maintenance on systems, including imposing restrictions on use to facilitate maintenance Investigate, or cause to have investigated, allegations of system misuse Impose penalties or refer to other disciplinary processes if misuse is substantiated Report on all investigations to the CIO	Providers	
Establish, publish and maintain ITC standards which prescribe standard services Establish, and publish, conditions of information technology system use Investigate, or cause to have investigated, allegations of system misuse Impose penalties or refer to other disciplinary/breach processes if misuse is substantiated	CIO, or delegate	Where an allegation of misuse has been made against a member of staff or an honorary, the Director Human Resources, or delegate, must be consulted before making a decision if practicable to do so

Hear submissions from users who have been found to have committed misconduct in an investigation by the CIO Determine whether the decision of the CIO should be upheld, modified or reversed	CEO or delegate	Where an allegation of misuse has been made against a member of staff or an honorary, the Director Human Resources, or delegate, must be consulted before making a decision if practicable to do so

7. LINKS TO RELATED POLICIES

- Code of Conduct Policy
- Disciplinary Procedure Policy
- Social Media Policy

8. FURTHER INFORMATION

Category: ICT

Review due by: 2/7/2020

Version: 1

Policy Steward: CIO

Status: Published

Further information and advice on this policy can be obtained from the CIO.

9. VERSION HISTORY

Version	Authorised by	Date Approval	Effective Date	Sections modified
1	CEO and Dean	2/7/2019	2/7/2019	