

## **Information and Communication Technology (ICT) Service Provision and Acceptable Use Policy**

### **Preamble**

This Policy has been approved by the Deakin College Senior Management Group on 27 April, 2018.

This Policy is consistent with:

- Privacy Act 1988 (Cth)
- Crimes Act 1958 (Vic)
- Copyright Act 1968
- Copyright Amendment Act 2006 (Cth)
- The Spam Act 2003 (Cth)
- Privacy Amendment (Notifiable *Data Breaches*) Act 2017 (Cth)

Information and Communication Technology (ICT) is provided to staff and students for use during the course of study and work. Use of ICT facilities must meet acceptable use standards as detailed in this policy.

### **Purpose**

This policy provides the scope in which provided ICT equipment and services are to be used in a safe, secure and acceptable manner to ensure Deakin College is a safe and supportive learning environment and workplace for staff and students.

### **Scope**

This policy applies to all staff and students who work or study on all Deakin College Campuses and use any ICT equipment and/or services provided.

### **Policy**

#### **1. Principles**

- 1.1.** ICT infrastructure and services are provided to support staff and students in the application of working or studying at the college.
- 1.2.** The range of ICT facilities, services and materials will be reviewed regularly to ensure that they remain relevant.
- 1.3.** Deakin College is committed to the secure management of ICT assets and to reduce risk of any ICT incidents that may impact the confidentiality, integrity and availability of information and necessary protection of the College's people and assets.
- 1.4.** All users of Deakin College ICT infrastructure and services must abide by Common Law, State and Federal Legislation and the Deakin College Codes of Conduct.
- 1.5.** Where Deakin College infrastructure and services are provided by Deakin University (for example email and library) an acceptable use agreement must be accepted. All staff and students must abide by University policies and procedures.

- 1.6. Where Deakin College Infrastructure and services are provided by Navitas, staff must sign the Navitas acceptable use policy agreement and abide by the relevant Navitas policies and procedures.
  - 1.7. The IT Manager will regularly review the range of ICT facilities, services and materials to ensure that the services are provided in accordance with Deakin College plans and meet the core functions of the Deakin College.
  - 1.8. Staff members or students must not initiate a project that has an ICT dependency unless it has been reviewed and endorsed by the IT Manager.
  - 1.9. In order to provide a secure and reliable ICT service and ensure compliance with the Common Law, State and Federal Legislation and Deakin College policy, the IT Manager may authorise monitoring and auditing the use of ICT facilities, services and materials, and may view data stored on these facilities and services, as well as material received or transmitted via these facilities (including email).
  - 1.10. The IT Manager is responsible for receiving and acting upon notifications of alleged breaches of use of ICT facilities, services and materials.
- 2. ICT Equipment and Facilities Provided**
- 2.1. Equipment and Facilities which may be provided to staff and students include, but are not limited to: computers including desktop, laptop, and tablet; mobile phones; network and internet access; Office 365 associated services; Gmail associated services; access to shared network drives; SharePoint access; Software; Accounts to access certain services; student portal and Moodle.
- 3. Security**
- 3.1. Any user accounts and passwords supplied to individual staff members or students must be kept secure and never provided to any other person.
  - 3.2. Any devices provided for individual use (for example, staff laptops and mobile phones) must be looked after and kept secure at all times. Mobile phones will be locked by a PIN or other security measure to keep information and data on them secure. Corporate provided iPhones will have "Find my iPhone" turned on. If you step away from any device, it must be locked to ensure no unauthorised access occurs.
  - 3.3. Any access passes and keys to secure areas shall be kept secure at all times.
  - 3.4. Visitors to secure areas are to be escorted at all times.
  - 3.5. Any loss, breach or potential breach in security is to be reported immediately to either the manager for staff, or to Deakin College reception for students.
- 4. Notifiable Data Breach**
- 4.1. Deakin College has a responsibility to report to the Australian Information Commissioner any data breach that has the potential to cause serious harm and to notify individuals whose personal information is involved in this data breach.
  - 4.2. The overall responsibility for protecting the privacy of all personal information held by Deakin College resides with the College Director and Principal, with the day to day management delegated to the Director Quality and Student Services.

- 4.3.** Breaches of the privacy rights of an individual must be reported to the Director Quality and Student Services who will manage the breach in conjunction with the relevant area.
- 4.4.** Staff members at Deakin College undertake training in the required data breach identification and reporting. The protocol includes:
- Data breaches immediately reported by the staff member to his or her line manager and to the Navitas Australian Regional Data Protection Manager;
  - The staff member then sends an email to the central data breach email account - [dataprotection@navitas.com](mailto:dataprotection@navitas.com);
  - The incident response team will assess the seriousness of the breach, contact the staff member for further information and/or in containing the breach; and
  - The incident response team implements the appropriate reporting action.

## **5. Electronic Data Storage**

### **5.1.** All personal data is:

- securely stored and password protected;
- contains the correct details and required information;
- Not kept any longer than the purpose for which it was processed, and is available to the supervisory authority upon request. See the Deakin College Privacy Policy for more information about use protection and storage of personal information.

## **6. IT Department Support for Students and Staff**

- 6.1.** The IT department monitor a shared email account [dcoll-ithelp@deakin.edu.au](mailto:dcoll-ithelp@deakin.edu.au) available to staff and students.
- 6.2.** Deakin College staff can request IT support through the Navitas IT Service Desk.
- 6.3.** Online Moodle training is provided for academic staff as part of Navitas Learning & Teaching department.

## **7. Non-acceptable Use**

- 7.1.** At no time shall any user access, or attempt to access, any equipment, information or services they are not lawfully required to access as part of their duties or studies.
- 7.2.** Any attempts to access equipment, information or services shall be reported to the Deakin College Senior Management Group for any further action to be taken.

## **Related Policies**

Privacy Policy

Staff Code of Conduct

Student Code of Conduct

Deakin University ICT Policies

Information and Communications Technology Security Policy

Information and Communications Technology Use Policy

Information and Records Management Policy

Information Technology Service Provision policy

Navitas ITC Policies

- IT Risk Policy
- ITC Change Management Policy
- Social Media Policy
- Navitas Global Email Policy
- IT Acceptable Use Policy

IT Security Policy

## Procedure

ICT Service Provision Procedure

Data Breach Reporting Procedure

## Definitions

<b>Key Term or Acronym</b>	<b>Definition</b>
ICT	Information and Communication Technology.
ICT Facilities	All physical spaces (e.g. server rooms, network or communications closets, computer laboratories), hardware and infrastructure (e.g. servers, workstations, laptops, voice and data network, audio visual equipment and portable storage devices) associated with the delivery of ICT services and materials.
ICT Services and Materials	All software and applications, all services (including but not limited to telephony and internet access), and data contained or stored in any ICT facility.
ICT User	Any authorised person with access to the College ICT facilities, services and materials, including but not limited to staff, students, honorary staff members, any authorised visitors (staff, academic, contractors, agents, alumni or students).
Moodle	Deakin College web service learning management system.
Portal	Secure web service provided to staff and students requiring login for accessing news, Google services, communications, and other learning support services.
Data Breach	Occurs when personal information may have been accidentally or unlawfully accessed, lost, disclosed, altered or destroyed.
Personal Information	Includes any information that can identify and individual (students or staff) such as a person's name address phone number email address, bank details, education activities etc

## Status and Details

<b>Status</b>	Current
---------------	---------

<b>Domain</b>	Governance
<b>Effective date</b>	27/04/2018
<b>Review date</b>	30/04/2020
<b>Approval Authority</b>	Senior Management Group
<b>Implementation Officer</b>	IT Manager
<b>Enquiries Contact</b>	Adam Hannan