# Information and Records Management procedure

# Section 1 - Preamble

(1) This Procedure is effective from 7 November 2018.

# Section 2 - Purpose

(2) This Procedure documents requirements for the control of University data and information.

# Section 3 - Scope

(3) This Procedure applies to all University data, information and records, whether received, created, maintained, copied, disseminated or disposed of by the University in the course of its operations.

# Section 4 - Policy

(4) This Procedure is pursuant to the Information and Records Management policy.

# Section 5 - Procedure

### Information Management Framework

(5) The Information and Records Services Team, in collaboration with other organisational units of the University as required, will facilitate awareness and training activities for staff in relation to information and records management, including information classification and recordkeeping requirements.

(6) Information Owners will implement information and records management practices for their organisational unit, including determining appropriate information classification.

(7) Managers will ensure that their staff members, including consultants and contractors, are aware of and educated about information and records management, including the information classification and recordkeeping requirements appropriate to their role. (Refer to the Information and Records Services website for further information.)

### Information classification

(8) Staff will undertake the information classification and recordkeeping requirements required by their role, to preserve the confidentiality, integrity and availability of information, and will not damage, conceal or give unauthorised access to information.

(9) If classification of information is unclear, the information must be protected in a manner consistent with the more secure of the possible classification levels until the information owner can apply the correct classification, which must

be done within 20 working days of creation or receipt.

(10) All Relevant Documents and files must be clearly labelled with one of the following designations:

a. strictly confidential
b. restricted to staff
c. restricted to staff and students
d. public.

(11) The classifications will be applied as follows:

a. strictly confidential
    i. used for highly sensitive information; access strictly limited to a selected group or process
    ii. access, distribution, retention and/or destruction of information is subject to restrictive regulatory obligations
    iii. if compromised, would place the University in breach of its legal and regulatory responsibilities.
b. restricted to staff:
    i. information available to Deakin staff who need access to fulfill their operational duties, but not for public disclosure; commercial and competitive in nature
c. restricted to staff and students:
    i. information available to Deakin staff and students to enable operations, but not for public disclosure
d. public:
    i. available to the general public; no adverse effects are expected to result from the wide circulation of this information.

## Information storage

(12) All confidential, personal and proprietary Information will be stored, in the first instance, in primary storage devices.

(13) Where there is a clear business requirement, copies of confidential, personal and proprietary Information may be temporarily stored on portable storage devices administered by the University, but only where the storage device is physically secured to prevent unauthorised access and, if electronic, the files containing the Information are password protected.

(14) Where there is a clear business requirement to have copies of confidential, personal or proprietary Information on devices provided by an external service provider, staff will submit requests to the University Information Manager or nominee as stated in the Data Use Agreement and/or Privacy Impact assessments, who will determine whether to approve the request.

(15) All data and information held electronically will be stored and secured according to technology standards defined by the Chief Digital Officer.

## Access

(16) The Head of Organisational Unit that is responsible for devices or applications in which information is managed or stored, will ensure that access to those devices or applications is given on a needs basis and that access rights are reviewed at least annually.

### Disposal

(17) Staff will not dispose of a record except:

a. in accordance with the Deakin University Retention and Disposal Authority, and
b. with the prior approval of the Information and Records Services Team.

(18) Staff will not destroy information where the information:

a. is, or is reasonably likely to be, required in evidence in a legal proceeding, or
b. is the subject of a request for access received by the University under the Freedom of Information Act 1982 (Vic).

### Archives

(19) The Information and Records Services Team will assess and manage records judged to be of archival value or requiring long-term storage and preservation.

### Breaches

(20) All members of the University should immediately report any suspected or perceived breach of the Information and Records Management policy, Procedure or Guidelines, or associated legislation, to their relevant Head of Organisational Unit in the first instance, the University Information Manager or as appropriate under other legislative and policy provisions.

(21) Breaches will be investigated, and disciplinary action will be taken as appropriate.

## Section 6 - Definitions

(22) For the purpose of this Procedure:

a. data: as defined in the Information and Records Management policy.
b. information: as defined in the Information and Records Management policy.
c. Information Owner: as defined in the Information and Records Management policy.
d. portable storage device: any device that is small, lightweight and capable of storing data and information; including but not limited to CDs, DVDs, floppy discs, removable hard drives, USB flash drives and memory sticks, laptops, tablet computers, PDAs, mobile phones, iPods and MP3 players, and other devices.
e. primary storage device: any device which is capable of storing data and information and which is a fixed storage device owned and administered by the University.
f. record: as defined in the Information and Records Management policy.
g. Relevant Document: any document or file produced by an employee of Deakin University in the course of their duties containing personal or commercial information.

## Status and Details

| | |
|---|---|
| **Status** | Current |
| **Effective Date** | 7th November 2018 |
| **Review Date** | 7th November 2023 |
| **Approval Authority** | Vice-Chancellor |
| **Approval Date** | 6th November 2018 |
| **Expiry Date** | To Be Advised |
| **Responsible Executive** | Liz Johnson<br>Deputy Vice-Chancellor Education<br>+61 3 92468303 |
| **Implementation Officer** | Craig Anderson<br>University Librarian<br>+61 3 92517180 |
| **Enquiries Contact** | Information and Records Services Team<br>+61 3 52278566 |