

## **Dropbox and University Information**

### **Information Technology Services**

#### **University of Melbourne**

---

<b>Policy Category</b>	Authorisation
<b>Contact Officer</b>	Stephen Young
<b>Commencement date</b>	1 December 2010
<b>Review date</b>	31 December 2012
<b>Revision no</b>	2

**Web address**

<http://www.unimelb.edu.au/infostrategy/policies/docs/dropbox.pdf>

---

## **PART 1 POLICY STATEMENT**

**Dropbox may be used with University information, subject to the guidelines provided in part 1.7 of this policy.**

### **1.1 Objectives of policy**

To allow use of Dropbox, within the constraints of University IT Security Policy <<http://policy.unimelb.edu.au/UOM0403>>, paragraph 8.4.

### **1.2 Policy rationale**

Dropbox<sup>1</sup> is a convenient and near seamless internet service for synchronising a consistent set of files in Dropbox folders on one or more computers and online storage. The files in a Dropbox folder can be used on any of the synchronised computers and they can be accessed via any modern web browser. The online files can also be accessed from mobile devices like the iPhone and iPad, and there is a facility for sharing subfolders within the main Dropbox folder. This makes Dropbox a most attractive platform for collaboration and sharing amongst colleagues.

Use of Dropbox does pose risks related to IT and records security, privacy, copyright and records retention. A University review of Dropbox, its terms of use and its security, leads to the conclusion that it is appropriate to use Dropbox with University information, subject to the guidelines set out in part 1.7 of this policy.

### **1.3 Scope**

This policy applies to any use of Dropbox with University information. This policy does not authorise any action which would infringe copyright, infringe University Privacy Policy, or any other policy, rule, statute or legislation to which the University and users of its IT facilities are subject.

### **1.4 Related legislation, policies and other documents**

- University of Melbourne Regulation 8.3.R2 <<http://www.unimelb.edu.au/ExecServ/Statutes/pdf/r83r2.pdf>>, particularly section 3 (3) and 10 (1) (c).
- University IT Security Policy, particularly paragraph 8.4: 'Sensitive or confidential University information is not to be stored on third-party facilities without approval of the CIO' <<http://policy.unimelb.edu.au/UOM0403#section-8.4>>.
- University Privacy Policy <<http://www.unimelb.edu.au/unisec/privacy/privacypolicy.html>>.
- *Information Privacy Act 2000* (Vic), particularly Schedule 1, section 9, 'Transborder Data Flows'.
- *Public Records Act 1973* (Vic)

### 1.5 Authority Statement

This policy imposes restrictions and conditions on authorisation to use the Central Facilities. Regulation 8.3.R2, paragraph 3.3, provides that power to the Executive Director (Information Technology) or his or her delegate.

This policy provides guidelines on appropriate security controls in the use of University IT facilities. Regulation 8.3.R2, paragraph 10, provides that the Executive Director (Information Technology) may publish such guidelines and that such guidelines may be taken into account in determining whether a user has done, or omitted to do, any act or practice which constitutes a misuse of any of the facilities.

University IT Security Policy, paragraph 8.4 provides that '[s]ensitive or confidential University information is not to be stored on third-party facilities without approval of the CIO'. This policy provides that approval for use of Dropbox, subject to the guidelines set out in part 1.7.

### 1.6 Definitions

**"Chief Information Officer" or "CIO"** has the meaning given in section 4 of the University IT Security Policy.

**"Dropbox"** means the online file storage, synchronisation and backup facility made available by Dropbox inc of 101 First Street #213, Los Altos, CA 94022, United States of America, and related software provided by that company.

**"Executive Director (Information Technology)"** has the meaning given to 'director (information technology)' by University Regulation 8.3.R2, section 1.

**"iOS"** means the operating system for iPhone, iPad and iPod touch, developed by Apple Inc.

**"mobile device" means an internet access device which is not a personal computer in the traditional sense. iPhones and iPads are mobile devices; desktop and laptop computers are not.**

A **University Record** comprises recorded information in any form (regardless of format), created or received and maintained by the University in the course of conducting its affairs and retained as evidence of such activity.

## **1.7 Guidelines: Dropbox and University Information**

- 1.7.1 Dropbox should not be used with confidential or sensitive information unless there is no alternative method, of comparable immediate availability and ease of use and with better security, to achieve the required functionality.
- 1.7.2 Any Dropbox file sharing is limited to small groups of highly trusted colleagues, using shared folders not public folders.
- 1.7.3 If it is feasible to do so, any confidential or sensitive information stored on Dropbox should be in encrypted form (for example, documents as encrypted PDFs). In this regard, the iOS application 'Goodreader' is suggested as an alternative to the Dropbox iOS application.
- 1.7.4 Files should be left online for no longer than is necessary.
- 1.7.5 Owners of shared folders should frequently review Dropbox events and shared folder membership, and promptly update shared folder membership to reflect changes in colleagues' roles.
- 1.7.6 Participants should not put anything on Dropbox that they would not be comfortable sending as an email attachment.
- 1.7.7 Dropbox is not to be used as the sole storage for any University Record, or as a recordkeeping system.
- 1.7.8 All University users of Dropbox should exercise self-discipline to ensure that passwords are reasonably strong and are changed at reasonable intervals.
- 1.7.9 As with any use of personal computers, those who use and manage the computers should be vigilant against security threats including phishing, viruses, trojan horses and key-logging.
- 1.7.10 Dropbox should not be used on mobile devices connected via unencrypted wifi networks.

## **PART 2. RESPONSIBILITY**

- Initiating the policy: ITS Planning Office
- Approving the policy: Executive Director (Information Technology) and CIO
- Review process: ITS Planning Office

- Compliance with the policy: all people who use Dropbox with University information.

---

<sup>1</sup> Dropbox 2010, Dropbox, USA, viewed 30 July 2010, <<http://www.dropbox.com/>>.