Cloud Computing Service Audit

1. Introduction

Following the review and approval of the Information Security Policy and Processes document at the IT Policy Committee, issues surrounding the use of cloud based services were identified as needing further investigation, discussion and recommendations. Anecdotally, the use of cloud based services is widespread at the institution; people are concerned and eager to have direction on the safe use of such services.

In an attempt to provide a consistent and clear set of guidelines on the use of cloud based services, this document presents the findings of an initial audit (in July 2012) of a few of the cloud based services known to be in use.

2. iCloud

Service Name	iCloud
Description	Synchronisation mechanism between iTunes, Mac computers, iPads and iPhones. Ensures the availability 'anywhere' of selected file types, including music files, mail messages, and documents.
Terms and Conditions URL	http://www.apple.com/legal/icloud/en/terms.html
Issues	• Terms and Conditions, or nature of service can change without notice. • No guarantee that data stays within the EU and US • The right to change data in transmission is reserved
Appropriate Usage	**Personal Data: Not permitted** **Restricted: Not recommended** **Confidential: Permitted** **Ordinary: Permitted** Note that caution is recommended in the use of iCloud for any data, as it is not always clear when the service is being used. For example, opening an attachment to a piece of mail within 'Pages' will implicitly move it to iCloud if Pages synchronisation is activated.

3. Gmail

Service Name	Gmail
Description	Google's cloud based email system. Mail from other accounts is often forwarded to a single Google mail (Gmail) account to allow someone to see all their email in a single location, with access from any web browser. Note that Google has one global set of terms and conditions which covers Google's other services, not just Gmail. The recommendations provided here should be extrapolated to cover the use of Google's other services.
Terms and Conditions URL	http://www.google.com/intl/en/policies/terms/

Issues	• "When you upload or otherwise submit content to our Services, you give Google (and those we work with) a worldwide license to use, host, store, reproduce, modify, create derivative works (such as those resulting from translations, adaptations or other changes we make so that your content works better with our Services), communicate, publish, publicly perform, publicly display and distribute such content." • Terms and Conditions, or nature of service can change without notice. • No reference to where data is stored, hence no guarantee it remains in EU or under safe harbour.
Appropriate Usage	**Personal Data: Not permitted** **Restricted: Not recommended** **Confidential: Permitted** **Ordinary: Permitted** Although personal data must not be transmitted via email within the institution, automatic forwarding to Google mail would exacerbate any break of that policy, given the terms and conditions above.

4. Evernote

Service Name	Evernote
Description	"Accessibleanywhere" notes: cloud-based storage of notes, documents and images, which can then be accessed through a web browser or from a mobile device.
Terms and Conditions URL	http://evernote.com/tos/
Issues	• Terms and Conditions, or nature of service can change without notice. • No guarantee that data stays within the EU and US • A superseding agreement can be negotiated
Appropriate Usage	**Personal Data: Not permitted** **Restricted: Not recommended** **Confidential: Permitted** **Ordinary: Permitted** It is easier to identify when Evernote is being used than it is with iCloud, but caution is still recommended to ensure that personal data is not inadvertently moved into an Evernote account. If the institution wanted to pursue the use of a particular cloud-based service for use with Personal and Restricted data along with Confidential and Ordinary, it may be possible to draft an agreement with Evernote for a superseding agreement which ensures that data stays in the EU.

5. Dropbox

Service Name	Dropbox
Description	Ubiquitous filestore available via a web browser or from a mobile device. Allows some folders to be available to other Dropbox users while others remain 'private'.
Terms and Conditions URL	https://www.dropbox.com/terms
Issues	• 'If you are using the Services on behalf of an organization, you are agreeing to these Terms for that organization and promising that you have the authority to bind that organization to these terms.' • 'We may also remove any content from our Services at our discretion.' • Terms and Conditions, or nature of service can change without notice. • No guarantee that data stays within the EU and US, though does claim to adhere to the US Safe Harbor laws.
Appropriate Usage	**Personal Data: Not permitted*** **Restricted: Not recommended** **Confidential: Permitted** **Ordinary: Permitted** *As dropbox is simply filestore, it is easier than with some other cloud based services to apply further levels of security to files and still make them accessible via Dropbox. Hence, if there were unavoidable circumstances in which personal data needed to be stored on Dropbox, that, though not recommended, may be permitted as long as the file containing the data is separately encrypted. There have been security issues with Dropbox, which are worthy of note: http://www.economist.com/blogs/babbage/2011/05/internet_security http://dereknewton.com/2011/04/dropbox-authentication-static-host-ids/

6. Generic Advice

Across the relatively small number of services which have been audited, the following advice remains the same and would probably apply to the use of other services.

Given the changeable nature of terms and conditions which will likely apply unless the University makes an explicit agreement with a provider:

- Do not use cloud-based services to hold personal data unless it is independently encrypted, using a recommended encryption mechanism.
- Do not assume that your right to the Intellectual Property of documents held in the cloud is unchanged by storing the information there—many claims are made that you forgo certain rights through your use of certain cloud services.

- As with advice on the use of mobile devices, do not rely on cloud-based services to provide more than a secondary copy of data; ensure that primary copies are held on University systems that offer suitable backup provision.

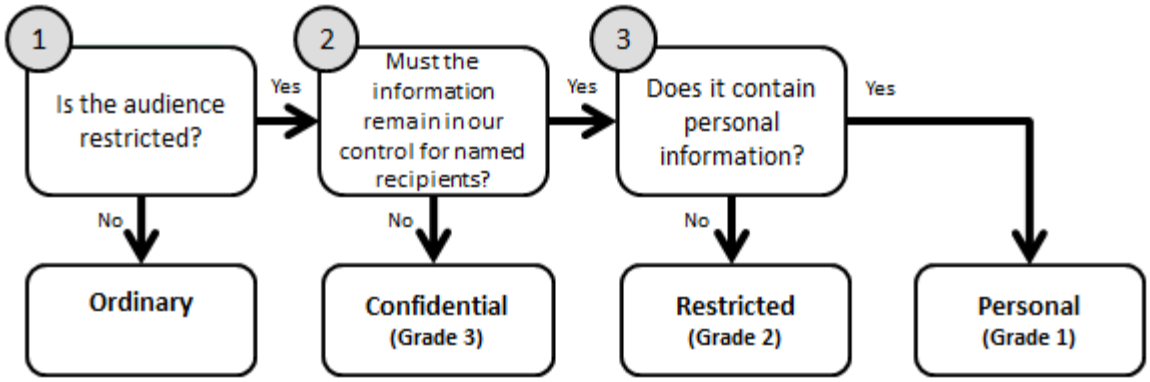
7. Conclusion

The services audited to date are believed to be in wide use across the institution; whether that usage represents risk to information security is dependent on the category of information being shared. There are many additional cloud-based services which could be audited, but, given the potential changes to terms and conditions over time, it may be difficult to ensure that audit results remain up-to-date.

It is worth underlining the potential implications of Dropbox's claim that someone in an organisation accepts liability for the use of the service on behalf of the organisation; this requirement challenges the University to have an explicit policy about the use of their service. Though there is a degree of disparity between the terms and conditions of the different services there is also some commonality (and commonality of issues not addressed, like data location).

To date, no cloud-based service has been identified which is appropriate for Personal or Restricted data (based on their public terms and conditions). Caution is advised in all cases, and especially in the cases where it is not obvious when a cloud based service is being used (e.g. iCloud and Google mail with automatic forwarding).

8. Appendix – Data Classification



Ordinary	Information that has no constraints on its publication. Available to all including external parties.
Confidential	Information of internal interest or being prepared for publication. Recipients may forward to others within the control of the University. For example, forwarded internally or outside the University with a confidentiality agreement, such as to contractors.
Restricted	Information which is for circulation to named recipients only. Any further distribution to be explicitly approved by the author. Must not be downloaded or copied to mobile devices unless the device is capable of appropriately encrypting the information.

Personal data	Personal information is protected by the Data Protection Act. Access should be by relevant staff only and the information can be circulated to named recipients only. Any further distribution to be explicitly approved by the author and must represent permitted processing under the Data Protection Act.