ISC13D007

Title:	***File and Email Restoration policy review***
Author:	Raymond Scott (ISD)
Date:	24 October 2013
Circulation:	ISSC - 8 November 2013
Agenda:	ISC13A001
Version:	v1.1 DRAFT
Status:	Open

Issue

To seek the committee's approval for proposed changes to the File and Email Restoration policy.

Recommendation

Recipients are invited:

- To approve the revised policy.

Resource Implications

No change to service is required and therefore there is no impact on resources.

Equality and Diversity

New services will be subject to Equality Impact Assessments as they are implemented.

Timing of decisions

Once approval is obtained the revised policy can be put into effect and published.

Further Information

- Raymond Scott (ISD), x3561, r.scott@uea.ac.uk

Background

The File and Email Restoration policy is subject to bi-annual review. This paper contains the proposed changes to the policy, which are clearly highlighted.

File and Email Restoration Policy

Author: Raymond Scott (ISD)

Date: ~~10/11/11~~1/10/13

Version: 1.1~~0~~

This document defines the University's policy on the restoration of digital assets such as files and emails, and is based on the following principles.

- **End users should manage their email and files so that items no longer needed are deleted**
- **ISD provides backup services only to restore service in the event of system failure**
- **Users are responsible for the recovery of their own items deleted in error**

Version history

Version	Date	Note
0.1	18/10/11	First draft
0.2	26/10/11	Updated following review by ISDMT
1.0	10/11/11	Approved by ISSC
1.1	1/10/13	Reviewed and updated

Introduction

File and email digital assets held on centrally-provided systems administered by ISD are ~~regularly~~ backed up daily (overnight) to ensure service resumption following disaster in line with Disaster Recovery and Business Continuity (DR & BC) planning. End users of these systems are encouraged to delete items no longer required, but responsibility for the recovery of items deleted in error rests with the end user. In general, ISD does not offer a file and email restoration service, but under exceptional circumstances may be called upon to attempt recovery of items lost in error.

Scope

This policy applies to:

- All users of centrally-provided email and filestore services, and ISD IT administrators
- The recovery of files and emails deleted in error by end users

This policy does not apply to:

- Files owned by UEA staff or students managed through systems other than the central filestore service delivered by ISD, e.g. the loss of files on systems such as Blackboard or CMS.
- Emails sent or received by UEA staff or students managed through systems other than those delivered by ISD~~, e.g. local email servers, Gmail, Yahoo, or Windows Live~~.
- Items deleted from storage areas or devices other than the central filestore service delivered by ISD, e.g. local file servers, USB sticks, external hard drives, cloud storage, or local hard drives.

Definitions

The following definitions apply to this policy:

- **Digital asset**. An email or file owned or managed by an end user.
- **End user**. A student, member of staff, or visitor issued with a UEA IT account including filestore and email services.

Aims

The aims of this policy are to clarify:

- ~~What~~ A~~a~~rrangements ~~are~~ available to end users to recover their digital assets.
- When deleted digital assets are ~~still~~ subject to disclosure under F~~f~~reedom of I~~i~~nformation legislation.
- Responsibilities of end users in recovering items deleted in error.
- Responsibilities of ISD in aiding the restoration of files deleted in error.

Policy statements

- File and email digital assets held on centrally-provided systems administered by ISD are ~~regularly~~ backed up daily (overnight) to ensure service resumption following disaster in line with Disaster Recovery and Business Continuity (DR & BC) planning.
- End users of these systems are encouraged to delete items no longer required.
- (Staff only). Deletion of items should be in line with records retention schedules.
- (Staff only). Items subject to legal hold (for compliance purposes) should not be deleted.
- Once deleted, items may be held in a Deleted Items folder (e.g. Outlook for email) or Recycle Bin (e.g. Windows for files). A user can then choose to recover these items from the appropriate location should the item still be required, and the deletion was conducted in error.
- However, it should be noted that advice from the Information Commissioner's Office (ICO) states that items which have been deleted but remain in a Deleted Items folder or a Recycle Bin are held by the ~~Public Authority~~University for the purposes of the Freedom of Information Act 2000 or Environmental Information Regulations 2004. This means they should be considered for release subject to a relevant request for information. ~~However,~~ ~~w~~When intentionally removed from these temporary deleted items stores, they are permanently deleted and no longer considered to be held. In general, information that is capable of being overwritten and has been intentionally deleted will not be held.
- On occasions when emails have been deleted permanently in error, end users may be able to recover their own email via the 'Recover Deleted Items' option.~~-~~Items are held in this folder for up to 15 days after deletion. Beyond this period, ~~I~~in general, ISD will not offer a service

to aid their restoration. It is the end user's responsibility to ensure that they only permanently delete emails which are no longer required.

- On occasions when files have been deleted permanently in error, end users may be able to recover their own files via snapshot backups operating on centrally-~~-~~managed filestore. Snapshots can be used to recover files up to seven days after deletion. Beyond this period, in general, ISD will not offer a service to aid their restoration.
- Under exceptional circumstances, for example to support security investigations or where business critical information has been lost, ISD can be called upon to attempt to recover files.

Exception handling

Where the ~~E~~end user attempts to recover their files, but fails ~~and~~they may request help ~~requests help~~ from IT support. ~~Exceptions to this policy shall~~Requests for help shall be handled in the following way:

Formatted: Normal

- Requests for file restoration should be handled promptly as backup ~~hold~~ data is held for up to 30 days. Delays in acting may mean that the files are not available for recovery from backup.
- ~~End user attempts to recover files, but fails and requests help from IT support.~~
- IT support confirms that the file cannot be restored by the end user, and also asks the user to check whether others may have copies of the file (e.g. emailed to a colleague).
- IT support collects the following information from the user and ~~sends this through to ISD Strategy, Policy and Compliance team (via email or the call logging system), who will~~ provides authorisation for the restoration of the file from backup:
  - Reasons why the file needs to be restored (reflecting its value to the user’s work and the institution)
  - reasons why the end user is not able to restore it themselves (e.g. manner of deletion, or snapshots not working or beyond seven day limit)
  - full path and filename of the deleted file
  - date when the file was last seen ~~and its full network share path~~ (to help ISD recover it from tape)
  - description of the contents of the file
- ~~If approved,~~ ISD attempts to restore the file and informs the end user of the outcome.

Formatted: List Paragraph, Bulleted + Level: 1 + Aligned at: 0.63 cm + Indent at: 1.27 cm

Formatted

Formatted: List Paragraph, Bulleted + Level: 1 + Aligned at: 0.63 cm + Indent at: 1.27 cm

Responsibilities

Within this policy, the following individuals have the following responsibilities:

Responsibility	Owner
Permanently delete items no longer required (and, staff	End users

Responsibility	Owner
only, where appropriate according to records retention schedules)	
Restore items which have been deleted in error	End users
Ensure digital asset management is in compliance with ~~freedom~~ Freedom of I~~i~~nformation legislation	End users
Provide a snapshot backup service to aid users' recovery of files from central filestore[1]	ISD
Backup systems to ensure their recovery in the event of disaster as defined by DR & BC documentation	ISD
Provide a file restoration service to recover files under exceptional circumstances ~~aid~~ such as security investigations or the loss of business critical information	ISD

References

This policy is supported within the context of the following pieces of legislation, professional standards, and University documents:

- ICT Contingency Plan – Top Level. http://www.uea.ac.uk/is/itregs/businesscontinuitydisasterrecovery
- ICO Line to Take on deleted electronic information. http://www.ico.gov.uk/foikb/PolicyLines/FOIPolicyDeletedelectronicinformation.htm
- ICO guidance on determining whether information is held. http://www.ico.org.uk/for_organisations/guidance_index/~/media/documents/library/Freedom_of_Information/Practical_application/determining_whether_information_is_held_foi_eir.ashx
- ISD Helpsheet on How to rescue deleted/modified items from UEA filestore ~~https://intranet.uea.ac.uk/is/ithelpsheets/filemanagement/f3~~ https://intranet.uea.ac.uk/is/ithelpsheets/filemanagement/f3
- Conditions of Computer Use. http://www.uea.ac.uk/is/itregs/usepols
- Department records retention schedules (RRS). https://intranet.uea.ac.uk/is/strategies/infregs/Records+management/RRS%3a+department+policies

Review

ISD will undertake a review of this policy every two years. Revisions will be presented for approval to the Information Strategy and Services Committee (ISSC).

[1] As at October 2013, snapshots are not available to UEA London users.