File Restoration Policy

Author: Raymond Scott (ISD)

Date: 9/2/16

Version: 3.0

This document defines the University's policy on the restoration of digital assets held in file storage, and is based on the following principles.

- **End users should manage their 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
2.0	8/11/13	Approved by ISSC
2.1	5/1/16	Reviewed and updated
2.2	15/1/16	Renamed and updated to remove references to email
3.0	9/2/16	Approved by ISSC

Introduction

File digital assets held on centrally-managed systems administered by ISD[1] are backed up daily 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 restoration service, but under exceptional circumstances may be called upon to attempt recovery of items lost in error.

Summary

The options for the recovery of digital assets are summarised in the following table.

Type	Location	Backup	Recovery by user	Recovery by ISD
File	CFS (personal or share)	Daily (overnight)	Yes. Check recycle bin (indefinite) or snapshot (up to 7 days)	Only as an exception

[1] For the purposes of this document, centrally-managed services include those provided by Microsoft Office 365 (e.g. Exchange Online, OneDrive for Business).

Type	Location	Backup	Recovery by user	Recovery by ISD
File	OneDrive for Business (cloud)	BC[2] as defined in SLA	Yes. Check recycle bin (up to 90 days). Items removed from recycle bin are held until 90 days old	None
Email	Office 365 (cloud)	BC as defined in SLA	Yes. Check Deleted Items folder (indefinite). Items removed from Deleted Items are held in Recover Deleted Item for up to 30 days	None

Scope

This policy applies to:

- All users of centrally-provided filestore services, and ISD IT administrators
- The recovery of files 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. ISD is not able to offer an email recovery service.
- Items deleted from storage areas or devices other than the filestore services offered by ISD (central filestore and OneDrive for Business), 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**. A file or email owned or managed by an end user.
- **End user**. A student, member of staff, or visitor issued with a UEA IT account including filestore services.

Aims

The aims of this policy are to clarify:

- Arrangements available to end users to recover their digital assets.
- When deleted digital assets are subject to disclosure under Freedom of Information 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 digital assets held on centrally-provided systems administered by ISD are 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.

[2] Business continuity

- (Staff only). Deletion of items should be in line with the department's records retention schedule.
- (Staff only). Items subject to legal hold must not be deleted (e.g. for compliance with Freedom of Information or Data Protection requests or other legal processes).
- Once deleted, items may be held in a Deleted Items folder (e.g. Outlook for email) or Recycle Bin (e.g. Windows or OneDrive 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. Note that files in the OneDrive recycle bin are held for 90 days before being automatically deleted.
- 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 30 days after deletion. Beyond this period, ISD cannot offer a service to aid their restoration.
- On occasions when files held in UEA filestore have been deleted permanently in error, end users may be able to recover their own files via snapshot backups. 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.
- For OneDrive for Business, deleted items are held in a Recycle Bin from which they can be restored by the end user. When items are emptied from this Recycle Bin a second-stage recycle bin is provided. Both recycle bins automatically remove items older than 90 days. Ten previous versions of files contained in OneDrive for Business are retained for self-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 end user attempts to recover their files, but fails, they may request help from IT support. Requests for help shall be handled in the following way:

- Requests for file restoration should be handled promptly as backup data is held for up to 30 days. Delays in acting may mean that the files are not available for recovery from backup or, in the case of OneDrive for Business, from the recycle bin.
- 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 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 (to help ISD recover it from backup)
    - description of the contents of the file
- ISD attempts to restore the file and informs the end user of the outcome.

Responsibilities

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

Responsibility	Owner
Permanently delete items no longer required (and, staff only, where appropriate according to records retention schedules)	End users
Restore items which have been deleted in error	End users
Ensure digital asset management is in compliance with Freedom of Information and Data Protection legislation	End users
Provide a snapshot backup service to aid users' recovery of files from central filestore	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 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. https://portal.uea.ac.uk/information-services/strategy-planning-and-compliance/regulations-and-policies/it-regulations-and-policies/business-continuity-and-disaster-recovery
- Microsoft Office 365 service continuity. https://technet.microsoft.com/en-us/library/office-365-service-continuity.aspx
- 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://portal.uea.ac.uk/is/online-wiki-helpdesk/-/wiki/Main/How+to+rescue+deleted%3CSLASH%3Emodified+items+from+UEA+file+store+on+a+Windows+7+PC
- ISD Helpsheet on Office 365 quotas, limits and file retention. https://portal.uea.ac.uk/documents/6207125/7752191/10.+Quotas-limits-Retention-v2.pdf/
- Conditions of Computer Use. https://portal.uea.ac.uk/information-services/strategy-planning-and-compliance/regulations-and-policies/it-regulations-and-policies/usage-policies
- Department records retention schedules (RRS). https://portal.uea.ac.uk/information-services/strategy-planning-and-compliance/regulations-and-policies/information-regulations-and-policies/records-management/rrs-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).