

File and Email Restoration Policy

Author: Raymond Scott (ISD)

Date: 10/11/11

Version: 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

Introduction

File and email digital assets held on centrally-provided systems administered by ISD are regularly backed up 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 items deleted in error rests with the end user. ISD does not offer a file and email restoration service.

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 arrangements are available to end users to recover their digital assets.
- When deleted digital assets are still 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 and email digital assets held on centrally-provided systems administered by ISD are regularly backed up 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 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, when removed from these temporary deleted items stores, they are permanently deleted and no longer considered to be held.
- On occasions when emails have been deleted permanently in error, 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 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, ISD will not offer a service to aid their restoration.
- Under exceptional circumstances, for example to support security investigations, ISD can be called upon to attempt to recover files.

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	End users

Responsibility	Owner
freedom of information legislation	
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 aid security investigations	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>
- ISD Helpsheet on How to rescue deleted/modified items from UEA filestore
<https://intranet.uea.ac.uk/is/ithelpsheets/filemanagement/f3>
- Conditions of Computer Use. <http://www.uea.ac.uk/is/itregs/usepols>

Review

ISD will undertake a review of this policy every two years.