

1. Introduction

L&IS take backup copies of all data held on the University's corporate systems. This includes the Student System, Agresso Finance, Timetabling, Archibus, Sharepoint, Moodle, Cardiff Met Web Server and iTrent.

These backups help ensure that Cardiff Met's data is not lost in the event of a hardware failure, software malfunction or major incident. Full details, including the frequency and retention of backups, are included in this document.

Please note that Staff Email (which is being migrated to Office 365 Email) will be compliant with the terms detailed in this document from their next version upgrade. If you require any further clarification, then please contact IT Helpdesk.

2. Backup Frequency and Retention

2.1 Corporate systems hosted at Cardiff Met

The following three levels of backup are in place for corporate systems.

2.1.1 Replication

Data is replicated on to storage in the backup computer room in line with Cardiff Met's agreed recovery timescales. This enables services to be quickly restarted in the event of a major incident or disaster.

Replication is only in place for Cardiff Met's most critical systems i.e. those systems with a maximum data loss of less than one day.

2.1.2 Regular Backups

Daily, Monthly and Biannual backup cycles are in place for all corporate systems hosted at Cardiff Met. The data is backed up to a local backup device and is then copied to a backup device in the backup computer room.

Daily backups are performed Monday to Friday. Data can be restored from any weekday in the last 4 weeks.

Monthly backups take place on the last Sunday of each 4-week period. Data can be restored from as far back as 12 weeks.

6 Monthly – every year a full backup is taken in March and September. These backups are kept for a full year.

2.1.3 Tape Backups

A backup to tape is also taken on a weekly basis to facilitate archiving requirements and as a backup of last resort. This covers Archibus, iTrent, Moodle, ABW, Smart Cards, Timetabling and the Student System. Tapes are retained on a

rolling basis for periods of up to one year. Tapes are stored in fireproof safes which are located remotely from the main and backup computer rooms.

Information Custodians may request tape backups are retained for a longer period where it is necessary to archive data from corporate systems.

2.2 Cloud hosted systems

2.2.1 Ex Libris (Library)

Ex Libris has a well-developed backup plan consisting of multiple daily snapshots and including a full daily backup. The full daily backups are also stored in a remote secured location.

On a regular basis, Ex Libris also performs a system backup to back up application files, database files, and storage files. A 10-week retention policy is in place for backups. For full details please see [Ex Libris Cloud Services Business Continuity Plan](#).

2.2.2 Office 365 - Microsoft Onedrive for Business

Backup of Onedrive is undertaken by Microsoft and is not user accessible. There are, however, a number of features which can assist with the security of the content.

Item Recovery

Unless you specifically request a permanent deletion then any items you delete will be retained in the **Recycled Bin** for 90 days and will also be recoverable by a System Admin for a further 90 days after that.

Content Synchronisation

It is possible to backup content by synchronising it to a local device and then backing it up from there. Contact IT Helpdesk for further information.

[eDiscovery](#) and In-Place Hold

These features can be used to place Onedrive sites or documents that meet specific search criteria on hold. These may be applied to sites and documents of staff members who are still in-post with Cardiff Met or those that have left.

[Preservation Hold](#)

Content that is placed on hold is preserved, but users can still change it. The state of the content at the time of preservation is recorded.

Third party products, such as [Clouddaily SharePoint Online and OneDrive for Business Backup](#) can also be used to provide full backup features on an individual user or group basis.

2.2.3 Office 365 – Email (Staff Email)

Backup of Office 365 Email is undertaken by Microsoft and is not user accessible. There are, however, a number of features which can assist with the security of the content.

Mail Item Recovery

Unless you specifically request a permanent deletion then any mail items you delete will be retained in the **Deleted Items** folder for 365 days. This means you can easily recover a deleted item.

If mail items are purged from **Deleted Items** or deleted by pressing **shift+delete** they are retrievable for up to 30 days using the Recover Deleted Items feature; after that period, they will be lost.

Mailbox Recovery

Deleted mailboxes are recoverable for up to 30 days after they are deleted, by default, however it is possible to keep mailboxes indefinitely on request (by making the mailbox inactive).

Litigation Hold and In-Place Hold

These features can be used to place mailboxes on hold and preserve specific mail items for set durations (from the date of receipt or creation).

Third party products, such as [Cloudally Office 365 Exchange Backup](#) can also be used to provide full backup features on an individual user or group basis.

2.2.4 Data on other cloud services

Data backup and recovery of other Software as a Service /Cloud based systems is specific to each individual service. Please be aware that backup policies are generally non-negotiable however there are sometimes additional services which can be utilised to supplement retention.

For further information, please refer to the relevant terms and conditions or contact the provider.

2.3 Data on personal computers or laptop

No corporate backups are in place for personal computers or laptops. All data should be stored on corporate systems to ensure it is covered by the backup arrangements identified in this document.

If you do store any data outside of the corporate systems, then please ensure you have relevant security and data backup measures in place.

Should you require any help or advice with this then please contact IT Helpdesk.