# Data Back-Up Policy

## 1 INTRODUCTION

Whilst the University expects its employees and staff to comply with this policy, it does not confer contractual rights or form part of any contract of employment and may be amended by the University or replaced at any time following appropriate consultation and negotiation with recognised trade unions. Breach of this policy may be addressed via the University's Disciplinary Policy and Procedure and Code of Conduct.

This policy will be reviewed by the IT Services and Human Resources department on a 3-year basis or amended in response to changes in future legislation and/or case law.

## 2 OWNERSHIP

The IT Services and Human Resources department owns and manages this policy on behalf of The University of Northampton.

## 3 ORGANISATIONAL SCOPE

This Data Back-Up policy is a corporate policy and applies to all employees (and workers, as applicable) and students of The University of Northampton including any wholly owned subsidiaries, unless an alternative policy exists, subject to any qualifying conditions.

## 4 POLICY STATEMENT

Student and business information is a primary asset to the UoN. As our information is subject to an increasing number of threats, it is important that we at the UoN continue to mitigate against the risk and maintain data integrity. For example, laptops could be stolen or the data could become irreparably corrupted.

In addition to virtual threats, data still needs protecting from environmental damages, such as floods and fire.

Accidents can happen, from discarding a document or overwriting a file by mistake.
In order for IT Services at the UoN help recover your files, it is essential that staff and students store their files in a secure, backed-up facility. Consequently, it is essential back-ups are available to help reduce the impact of information loss could have on any UoN teaching, research or business activities.

## 5 DEFINITIONS

**Data Owner**
The individual(s) who creates and possesses the data, who also has the ability to then edit, modify, share and restrict access to the data.

**One Drive**
One Drive is Microsoft's service for hosting files in the 'cloud'. OneDrive is a simple way to store, sync and share files.

**SharePoint**
A browser-based collaboration and document management platform from Microsoft.

**Removable Media**
Removable media is any type of storage device that can be removed from a computer while the system is running. Examples of removable media include CDs, DVDs and USB drives.

**Encryption**
Encryption is the process of converting data to an unrecognizable or "encrypted" form. It is commonly used to protect sensitive information so that only authorized parties can view it. This includes files and storage devices, as well as data transferred over wireless networks and the Internet.

## 6 KEY PRINCIPLES

### 6.1 Responsibilities

Users are responsible for ensuring that any information you create or modify as part of your work is stored in a University managed system where it will be automatically backed up; or, if you are working with information outside University managed systems, you are responsible for ensuring that appropriate backup controls are in place.

Retention schedule (Classification and Retention of University records) defines how long data types are retained for, this period will include the amount of time the information is only stored on a back-up.

Data Owners are additionally responsible for determining what backup and resilience arrangements are required to protect the information for which they are responsible.

- Ensure that the information you are working with is saved into the University storage which has appropriate back-ups in place.
    - One Drive or SharePoint
    - UoN network storage or UoN shared network storage.
- If your information cannot be saved to the UoN managed storage for example, information created in the field where you are unable to connect to University systems, ensure your information is saved locally on your device and transfer to University systems as soon as possible.

6.2 Constraints

- Refrain from using removable media where possible. If it is essential to use it, according to the classification of information contained, you should consider encrypting your device.
- Do not leave back-up media in devices after back-ups have completed.
- Do not keep back-up data in the same physical location as the original data.
- Do not use cloud storage not provided by UoN IT Services (such as GoogleDrive or DropBox).

## 7 PROCEDURE

a. Simultaneously on your keyboard press the ‘Windows key’ and the ‘e’ key.

b. Just below Desktop, Documents, Downloads, you will see 'OneDrive'.
c. Select 'One Drive'.
d. You should store all your files on your OneDrive rather than being stored on your laptop laptop/desktop or R:\ Drive.

One Drive enables you to store your own work and other files in a way that provides full access, providing you have an internet connection. Ensuring that your data is stored in the corrective location will mean that is secure and backed up (in other words, in case you need it later or your device is lost or damaged).

## 8 ASSOCIATED DOCUMENTS

Acceptable Use Policy
BYOD Policy
GDPR Policy

## 9 EQUALITY IMPACT ASSESSMENT

There is no adverse equality impact within this policy. All responses to breaches of rights will be dealt with in accordance with this Policy, Procedure and relevant Appendices irrespective of an individual's specific characteristics.

## 10 VERSION CONTROL

| **Version Control** | 1.0 | **Approval record** | |
|---|---|---|---|
| Author: | IT Services | Approval: | TU Liaison – 18/09/2018<br>UMT – 10/10/2018<br>Board – 11/12/2018 |
| Date written: | | August 2018 | |
| Current status: | | Live | |

| **Record of Amendments** | | | |
|---|---|---|---|
| Date | Version number | Details of Change | Approval |
| | | | |