CONTENTS:

1 General Policy ............................................................................................................... 2
   1.1 Introduction .............................................................................................................. 2
   1.2 Scope ......................................................................................................................... 2
2 Data Backup .................................................................................................................... 2
   2.1 Best Practice Backup Procedures .............................................................................. 2
   2.2 Responsibility for Data backup ................................................................................. 3
   2.3 Legal Requirements .................................................................................................. 3
   2.4 Desktop Backups ...................................................................................................... 3
3 Disaster Recovery ............................................................................................................ 3
   3.1 Best Practice Disaster Recovery Procedures ............................................................ 3
   3.2 Network Managers, System Administrators, Application Administrators .......... 3
   3.3 Users ........................................................................................................................ 3
1 General Policy

1.1 Introduction

Back-up procedures, ensuring that both data and software are regularly and securely backed-up, are essential to protect against the loss of that data and software and to facilitate a rapid recovery from any IT failure. This document outlines guidelines for Trinity College staff and students on backing up College Data.

1.2 Scope

The data backup element of this policy applies to all Staff, students and third parties who use IT devices connected to the Trinity College network or who process or store information owned by Trinity College Dublin.

All users are responsible for arranging adequate data backup procedures for the data held on IT systems assigned to them.

The disaster recovery procedures in this policy apply to all Network Managers, System Administrators, and Application Administrators who are responsible for systems or for a collection of data held either remotely on a server or on the hard disk of a computer. Information Systems Services are responsible for the backup of data held in central College databases.

2 Data Backup

2.1 Best Practice Backup Procedures

All backups must conform to the following best practice procedures:

- All data, operating systems and utility files must be adequately and systematically backed up (Ensure this includes all patches, fixes and updates)
- Records of what is backed up and to where must be maintained
- Records of software licensing should be backed up.
- At least three generations of back-up data must be retained at any one time (grandfather/father/son)
- The backup media must be precisely labelled and accurate records must be maintained of back-ups done and to which back-up set they belong.
- Copies of the back-up media, together with the back-up record, should be stored safely in a remote location, at a sufficient distance away to escape any damage from a disaster at the main site
- Regular tests of restoring data/software from the backup copies should be undertaken, to ensure
that they can be relied upon for use in an emergency

2.2 **Responsibility for Data backup.**

Only critical systems are routinely backed up by Information Systems Services and the other relevant IT managers and systems administrators in the current model. The responsibility for backing up data held on the workstations of individuals regardless of whether they are owned privately or by the College falls entirely to the User

If you are responsible for a collection of data held either remotely on a server or on the hard disk of a computer, you should consult your departmental system administrator or Information Systems Services about local back-up procedures. If you do not use the facilities provided by Information Systems Services or those of your department you should put in place your own procedures.

2.3 **Legal Requirements**

Users when formulating a backup strategy should take the following legal implications into consideration:

- Where data held is personal data within the meaning of the Data Protection Act, there is a legal requirement to ensure that such back-ups are adequate for the purpose of protecting that data
- Depending on legal or other requirements, e.g. Financial Regulations, it may be necessary to retain essential business data for a number of years and for some archive copies to be permanently retained
- Depending on legal or other requirements, e.g. Data Protection Act, Software Licensing, it may be necessary to destroy all backup copies of data after a certain period or at the end of a contract.

2.4 **Desktop Backups**

The responsibility for backing up data held on the workstations of individuals regardless of whether they are owned privately or by the College falls entirely to the User.

All network users using personal workstations/laptops should ensure that their data is backed up using one or a combination of the following methods:

- Backing-up to a local device e.g. floppy disk, Zip Drive, CD-Rom.
- Copying critical data on a regular basis to a remote server that is properly backed up by the College.
- Backups should be scheduled regularly.
- All users should backup their data before updating or upgrading software on their computer.
3 Disaster Recovery

3.1 Best Practice Disaster Recovery Procedures

A disaster recovery plan can be defined as the on-going process of planning, developing and implementing disaster recovery management procedures and processes to ensure the efficient and effective resumption of vital College functions in the event of an unscheduled interruption.

All disaster recovery plans must contain the following key elements:

- Critical Application Assessment
- Backup Procedures
- Recovery Procedures
- Implementation Procedures
- Test Procedures
- Plan Maintenance

3.2 Network Managers, System Administrators, Application Administrators

Network Managers, System Administrators, and Application Administrators who are responsible for systems or for a collection of data held either remotely on a server or on the hard disk of a computer must ensure that they have comprehensive, documented and tested disaster backup procedures covers in line with the best practice guideline in section 3.1 of this policy document.

3.3 Users

In the case of the loss of a system and data users need to:

- Procure replacement hardware. This can be done by purchasing it from a suitable hardware vendor or by using spare capacity on a colleague's computer in other building/site.
- Reload the data/software from the back-up media.
- Users may also need to re-licence the software, because often the licence manager keys on hardware-specific attributes e.g. size and type of hard disk, MAC address and/or host-id.