DATA BACKUP POLICY

Document Id	Data Backup Policy
Sponsor	Laura Gibbs
Author	Huw Michael, Nigel Rata
Date	May 2014

Version Control Log

Version	Date	Change
1.0	11/02/10	Initial draft for review
1.1	12/05/10	Updated
1.2	6/10/10	Updated
1.3	05/05/14	Updated

Document Approval

Name	Approval Date
Laura Gibbs	27.5.14
ITUAG	27.5.14

Introduction

The technology used to facilitate data backup at RHUL has been replaced. The new service allows for data in both our Huntersdale and Computer Centre Data Centres to be stored and then replicated between the sites ensuring that data is present on both sites.

Scope

The service and hence this policy has been designed and implemented with disaster recovery/business continuity (i.e. the ability to recover recent live data in the event of a partial or total loss of data) as key deliverable and is not therefore designed as a method of archiving material for extended periods of time.

The 'data' backups covers all systems managed by the IT department. Data held and managed locally in departments is excluded unless departments have entered into specific arrangements with IT. All staff are reminded that they are individually responsible for data held locally on their desktop or laptop computer and all critical data *must* be stored on the network drives provided or central e-mail services.

Backup Policy

- Full backups of all RHUL data are performed weekly. Full backups are retained for 3 months before being overwritten.
- Incremental backups of all RHUL data are performed daily. Incremental backups are retained for 1 month before being overwritten.
- Where possible backups are run overnight and are completed before 8am on working days.
- Upon completion of backups, media copies are moved automatically to a secure remote site for disaster recovery purposes.
- Backups are stored in secure locations. A limited number of authorised personnel have access to the backup application and media copies.
- Requests for backup data from 3rd parties must be approved by the College Secretary or Principal.
- Backup of data held within Database Systems have data backup routines which ensure database integrity is retained. Currently this means some systems are taken off-line in order to backup the data on a daily basis. Other systems are able to backup data on-line whilst maintaining data integrity.

Backup

- The IT Backup systems have been designed to ensure that routine backup operations require no manual intervention.
- The IT department monitor backup operations and the status for backup jobs is checked on a daily basis during the working week.
- Any failed backups are re-run immediately the next working day.

Restore

- Data is available for restore within a few minutes of a backup job completing on the daily schedule.
- Data will be available during the retention policy of each backup job – which is currently defined as 3 months.
- Recent data is available from this system on completion of the daily backup jobs, which means that there is potential data loss during a working day on some systems. The IT systems at RHUL have been specified to minimise data loss between backup windows by having elements of system redundancy.
- Requests for data recovery should be submitted to the IT Service desk.

This policy will be reviewed on an annual basis and be tabled for approval with ITUAG.