IT – Disaster Recovery Plan

1. Purpose

1.1 This IT Disaster Recovery Plan (IT-DRP) has been developed to provide key information, processes and appropriate responses to major incidents and disruption of IT services.

1.2 It aims to clarify Recovery Time Objectives (RTO) and Recovery Point Objectives (RPO) and to provide a clear path both during and after an incident to ensure that there is minimum downtime, data loss or impact to NMITE.

1.3 In order to be effective, this IT-DRP should:

i. be read by all employees of NMITE so that they understand any role or responsibility they have during a designated incident

ii. be reviewed and updated on a regular basis – at least annually - but also with any change in delivery or service provision

iii. cover all essential services, infrastructure, organisational devices, organisational shared data, organisational personal data, email & communications

iv. consider third party capabilities and functionality including external DR policies

v. be underpinned by a formal Risk Assessment

vi. operate cost effectively to a defined budgetary control

vii. be tested periodically to ensure success and rapid deployment during an on-going incident

1.4 In addition to this document being electronically stored and accessible to all staff, physical copies must also exist which are available in strategic locations.

2. Scope

2.1 The IT-DRP provides an IT risk and mitigation reference in addition to technical and operational information. Any processes and actions described are only applicable during a designated major incident which is to be determined in conjunction with NMITE's Business Continuity Plan.

2.2 This document is intended as a high-level approach and does not specifically itemise all of the steps required during response/recovery for any individual system.

2.3 This IT-DRP should consider all technologies used within NMITE including new and emerging ones. The top-level areas of consideration are:

2.3.1 Physical Infrastructure

i. Internet connectivity

ii. Network – all technologies (LAN, Wi-Fi, RF, Bluetooth, IoT, Proprietary, etc)

iii. Servers & Storage

iv. Client devices & peripherals (Computer, USB devices, etc)

v. Organisational and Support Devices (Dedicated systems, Printing, etc)

vi. Telephony and Communications

vii. Building Management & Digital Signage

viii. Security Systems (Door Access, CCTV, etc)

2.3.2 Software Systems – Cloud provisioning

i. Infrastructure-as-a-Service (IaaS)

ii. Platform-as-a-Service (PaaS)

iii. Software-as-a-Service (SaaS)

iv. Data Storage

v. Databases

2.3.3 Software Systems – Operational Line-of-Business applications

i. Student Records, Information Systems & Management

ii. Virtual Learning Environment / Learning Management System

iii. Organisational Applications

- Site Wide Applications
- CRM
- Finance
- HR

2.3.4 Software Systems – Educational Resources & Software

i. Applications utilised during course delivery

3. IT Emergency Response Team & Contacts

3.1 Internal Contacts

Name	Paul Guest	**Landline**	01432 804552
Title	Head of IT	**Mobile**	07803 551976
Company	NMITE	**Alternative**	
Email address	paul.guest@NMITE.ac.uk		
Roles & Responsibilities	**PRIMARY CONTACT** IT DR Lead Main IT Admin		
Contact Reasons	Any urgent IT requirements including Disaster, Failure, Compromise, Virus	**Hours / Availability**	24 x 7
	Non-urgent data loss requiring recovery	**Hours / Availability**	8:00 – 17:00
Notes			

Name	Graeme Ferguson	**Landline**	01432 804542
Title	IT Technical Lead	**Mobile**	07721536685
Company	NMITE	**Alternative**	
Email address	graeme.ferguson@NMITE.ac.uk		
Roles & Responsibilities	IT Technical Lead		

Contact Reasons	Non-urgent access for System Administration	**Hours / Availability**	8:00 – 17:00
Notes			

Name	James Newby	**Landline**	01432 804525
Title	COO	**Mobile**	
Company	NMITE	**Alternative**	
Email address	james.newby@NMITE.ac.uk		
Roles & Responsibilities	Chief Operating Officer		
Contact Reasons	Authority control during major incident	**Hours / Availability**	8:00 – 17:00
Notes			

3.2 External Contacts

Name	Mark Lindley	**Landline**	01432 60 78 72
Title		**Mobile**	07444 361267
Company	PC Logix	**Alternative**	
Email address	mark@pclogix.co.uk		
Roles & Responsibilities	Acts as Business Relationship Manager for NMITEs outsourced IT Service Desk		
Contact Reasons	Any serious IT Service Desk issue (e.g. users can't access the Service Desk)	**Hours / Availability**	8:30 – 17:00

Notes	

Name	Microsoft Office 365 Support	**Landline**	0117 332 3072
Title		**Mobile**	
Company	Provided through Softcat Ltd	**Alternative**	
Email address			
Roles & Responsibilities	Technical help with Microsoft cloud provision		
Contact Reasons	Assistance with recovery Restore requests for SharePoint	**Hours / Availability**	24 x 7
Notes	Account Mangager – Adam Dolan Tenancy Name: NMITE.onmicrosoft.com Microsoft 365, Office 365, SharePoint Online, OneDrive, Azure Online Link to Microsoft Online Services SLA for UK here		

Name	Jack Webb	**Landline**	0161 227 1000
Title	Customer Success Manager	**Mobile**	
Company	ANS Ltd	**Alternative**	
Email address	jack.webb@ansgroup.co.uk		
Roles & Responsibilities	Technical support for Student Records		
Contact Reasons	Manages the Service Delivery for ANS	**Hours / Availability**	24x7
Notes			

Name	Lauren Foster-Turner	**Landline**	0203 318 8635
Title	Customer Success Manager	**Mobile**	07795 694046
Company	Instructure Global Ltd	**Alternative**	
Email address	lfosterturner@instructure.com		
Roles & Responsibilities	Customer Liaison for Canvas LMS/VLE		
Contact Reasons	Tier 1 support for both students and staff	**Hours / Availability**	8am-6pm weekdays
Notes	Support and issues raised through support portal SLA part of contract terms and conditions (99.9%)		

Name	Toby Yeung	**Landline**	
Title	Senior Business Development Manager	**Mobile**	07805 149723
Company	JISC	**Alternative**	
Email address	toby.yeung@jisc.ac.uk		
Roles & Responsibilities	Service provider and Technical support for fibre internet and Janet Network including Managed Router Service		
Contact Reasons	Escalation point	**Hours / Availability**	9 – 5 weekdays
Notes	Blackfriars, Gardner Hall Online link to JISC network SLA here Online link to Janet Acceptable Use Policy here		

Name	No designated individual	**Landline**	01453 827700
Title	Support Team	**Mobile**	
Company	Connexus	**Alternative**	

Email address	service@connexusuk.com		
Roles & Responsibilities	Service provider for fibre internet into Miller Court Service provider for lift emergency call PSTN line		
Contact Reasons	Sales and account contact only weekdays Broadband/telephone failure 24x7	**Hours / Availability**	9 – 5 weekdays (urgent 24x7)
Notes	SLA part of contract terms and conditions Account number NEW002		

Name	No designated individual	**Landline**	0121 423 5600
Title		**Mobile**	
Company	BT/ BT Local Business / BTnet	**Alternative**	0800 800 152
Email address			
Roles & Responsibilities	Service provider for fibre internet into 6a St Peters Square BT Cloud Phone – provider of main number 01432 371111		
Contact Reasons	BT Faults	**Hours / Availability**	9 – 5 weekdays
Notes	SLA part of contract terms and conditions D2 Communications Ltd (BTLB Hereford to Birmingham)		

Name	No designated individual	**Landline**	01432 276393
Title	Thorne Widgery (Accounts – Xero agent)	**Mobile**	
Company	Xero	**Alternative**	
Email address			
Roles & Responsibilities	Provider and technical support for Xero financial software system		

Contact Reasons	Support	**Hours / Availability**	9 – 5 weekdays
Notes	Main accounts software, SLA part of contract terms and conditions		

Name	No designated contact	**Landline**	01403 288701
Title		**Mobile**	
Company	Breathe HR	**Alternative**	
Email address	support@breathehr.com		
Roles & Responsibilities	Cloud provider and technical support for Breathe HR software system		
Contact Reasons	Support, sales, and accounts	**Hours / Availability**	9 – 5:30 M-Th 9 – 4:30 F
Notes	HR software		

Name	No designated contact	**Landline**	
Title		**Mobile**	
Company	Capsule CRM	**Alternative**	
Email address	support@capsulecrm.com		
Roles & Responsibilities	Cloud provider for and technical support for Capsule CRM database software		
Contact Reasons	Support	**Hours / Availability**	9 – 5 weekdays
Notes	CRM used in Partnerships, Fundraising, Marketing & Faculty		

Name	Bob Williams	**Landline**	01684 296 551
Title	Account Manager	**Mobile**	

Company	Pulsonix	**Alternative**	
Email address	sales@pulsonix.com		
Roles & Responsibilities	Technical support for Pulsonix electronic circuit design software*		
Contact Reasons	Support	**Hours / Availability**	9 – 5:30 weekdays
Notes	Circuit design software		

Name	Ryan Rose	**Landline**	01865 954300
Title	Account Manager	**Mobile**	07891 627234
Company	One PLM	**Alternative**	Support
Email address	support@oneplm.com		01865 954301
Roles & Responsibilities	Technical support for Solid Edge application		
Contact Reasons	Support	**Hours / Availability**	8:30-5:30 weekdays
Notes	CAD suite and FEA simulation		

Name	Rebecca De Rafael	**Landline**	01223 226704
Title	Education Account Manager	**Mobile**	
Company	Mathworks	**Alternative**	
Email address	Rebecca.derafael@mathworks.co.uk		
Roles & Responsibilities	Sales and support for MatLab for both cloud and client installations		
Contact Reasons	Support	**Hours / Availability**	9 -5 weekdays

Notes	service@mathworks.co.uk technical support for teachers, installation support for students

Name	Shreya Sarker	**Landline**	0203 325 5520
Title	Customer Success Manager	**Mobile**	
Company	Adobe	**Alternative**	
Email address	shrsarka@adobe.com		
Roles & Responsibilities	Cloud provider for Adobe products – Creative Cloud, Acrobat		
Contact Reasons	Presales, sales, and renewals	**Hours / Availability**	9 – 5 weekdays
Notes	PDF & document handling, graphics suite		

Name	Susannah Cooke	**Landline**	01223 218022
Title	Development Manager for Education	**Mobile**	
Company	CES	**Alternative**	01223 518895
Email address	Granta.education@ansys.com		
Roles & Responsibilities	Software provider for Material Library software		
Contact Reasons	Sales, support elevation	**Hours / Availability**	9 – 5 weekdays
Notes	Granta Design Ltd		

This form has been intentionally left empty

Name		**Landline**	
Title		**Mobile**	

Company		**Alternative**	
Email address			
Roles & Responsibilities			
Contact Reasons		**Hours / Availability**	
		Hours / Availability	
Notes			

4. Definition of Services & Systems

4.1 From an IT perspective, NMITE aims to operate as a 100% cloud-based organisation. This means that (wherever possible) applications, data & facilities are leveraged wholly through offsite mechanisms.

4.2 This approach enables an extremely light-weight and versatile infrastructure with no requirement for on-site servers or data centres, thus reducing maintenance and upgrade requirements in addition to reducing the organisational attack surface and number of risk area touch points. The implementation and operation of a zero-trust network further mitigates against certain types of risks.

4.3 Although currently NMITE does not operate servers or a data centre there may be a point in the future where this becomes a necessity and for this reason risks, mitigations and procedures should be mentioned and expanded upon when appropriate.

4.4 Telecommunications within NMITE are also provided through cloud services using IP connectivity.

4.5 Use of IT within NMITE is broadly attributable to two primary categories

i. Operational Services

Organisational and Administrative functionality delivered by employees, contractors, and agents of NMITE.

ii. Educational Services

Learning and participatory functionality received by students, whether enrolled on a fulltime course, degree apprenticeship, CPD or other NMITE organised or sponsored activity.

4.6 By operating as a 100% cloud-based organisation NMITE have a very high degree of being able to continue functioning and providing these primary IT services through many physical disaster scenarios including total loss of buildings. The ability to utilise services from “any internet connection” provide a huge benefit in terms of both business continuity and educational delivery.

4.7 With this model, the emphasis for IT-DRP is therefore shifted to the appropriate protection of cloud services and internet provision.

5. Definition of Risks

Infrastructure	Description	Risk	Mitigation Measure
Internet Connectivity	Various fibre connections to buildings	Service provider failure	Secondary service provision
		Damage to fibre cabling	Resilient diverse connectivity Secondary service provision
		Local hardware failure (routers, switches etc)	Multiple device utilisation Overcapacity / Redundancy
		Natural Disaster / Loss of building integrity	Alternate location/Inherent ability
		Electrical failure Over/under voltage and surges Environmental changes	Uninterruptable Power Supply Emergency Generator
		Malicious attack (Denial of Service, Hacking etc)	Intrusion detection Conditional Access Appropriate permissions
		Vandalism / Sabotage / Terrorism	Physical protective measures Door Access Security
Data Centre & Servers	Virtual Machine Estate PaaS provision	Service provider failure VM failure or corruption	Backup & Replication Secondary service provision High availability
Wi-Fi & LAN Estate	IaaS provision	Hardware failure Interference Overloading Electrical failure	Multiple device utilisation Overcapacity / Redundancy Secondary service provision Resilient diverse connectivity

Infrastructure	Description	Risk	Mitigation Measure
Email & communication Primary Data Storage Operational Applications Faculty Applications	Various SaaS providers	Service provider failure Communication failure Corruption of data Loss of data Data Exposure / Compromise Commercial exploitation Sabotage / Internal attack Erroneous or neglectful activity Inability to operate / application failure	Backup & Replication Litigation Hold Policy Retention Policy Secondary service provision Conditional Access API integration
Organisational Devices Personal Devices	Laptops Tablets Desktops Phones Wearable technology BYOD Home PC	Hardware failure Data exposure / Password compromise Loss / Theft Inability to operate External devices (USB stick) Virus / Malware / Attack	Overcapacity / Redundancy Local drive encryption Conditional Access Password policy Remote Wipe capability Device restriction policy Advanced threat protection Active monitoring Appropriate use policy
Support Devices	MultiFunction Printers Scanners Desktop Printers	Hardware failure	Overcapacity / Redundancy
Building Management Digital Signage	BMS, HVAC Environmental monitoring	Hardware failure Communications failure	Manual operation / override Resilient diverse connectivity
Faculty Devices	3D Printing	Hardware failure	Resilient diverse connectivity

Infrastructure	Description	Risk	Mitigation Measure
	CNC Dedicated resources IOT	Vandalism / sabotage	Multiple device utilisation Physical protective measures
Security	Door Access CCTV	Hardware failure Vandalism / sabotage	Manual operation / override Physical protective measures

6. Definition of Mitigation Measures

6.1 Secondary Service provision

6.1.1 Where possible, a secondary service provision should be utilised to enable failover (whether automatic or manual) from one service to another.

6.1.2 For Internet Connectivity this would be in the form of multiple Fibre ISPs. The primary ISP for NMITE is JISC providing access to the Janet network through infrastructure from BTnet and Openreach. In order to be fully effective at the service provider level, a secondary service provision would need to leverage non-BT orientated infrastructure or services such as 4G/5G.

6.1.3 For Cloud Applications, Software-as-a-Service delivery and Virtual Machine environments, this would be in the form of multiple vendor Cloud provision. The primary Cloud vendor for NMITE is Microsoft utilising the Azure platform and Office 365.

6.2 Resilient diverse connectivity

6.2.1 The process of providing connectivity through at least 2 diversely routed pathways allowing for localised damage or failure.

6.2.2 For Internet Connectivity this would be provided by active-active or active-passive fibre connections, however within Hereford there is only partial resilience due to limited Point-of-Presence connectivity within the city.

6.2.3 For internal networks, wi-fi and LAN estates this employs multiple diverse cable routing.

6.3 Multiple device utilisation / Overcapacity / Redundancy / High Availability

6.3.1 The use of numerous identical devices to deploy services enables equipment to be swapped out and exchanged. This is an important facility during issue diagnosis and hardware failure but also allows for rapid resolution in critical areas over less important ones.

6.3.2 Overcapacity planning provides an opportunity to redeploy resources in the event of an issue and helps to mitigate against unexpected peaks in utilization.

6.3.3 For mission critical or key hardware, redundant replacement devices provide the quickest resolution time scales.

6.3.4 All of these processes should be utilised in conjunction with appropriate cost analysis.

6.3.5 High Availability is provided by a combination of the above and is particularly relevant in cloud orientated service deployment. By provisioning server farms, access gateways and load balancers, workloads can be distributed between facilities and in the event of a failure, can be directed, often seamlessly, to the remaining working component parts. These high availability components can be separated geographically to help mitigate against widespread incidents.

6.4 Alternate Location (Inherent ability)

6.4.1 The inherent ability to operate from an alternate location is a key concept in the mitigation against many physical location-based incidents. By operating with a cloud-first philosophy and running a zero-trust network model with extensive wi-fi

implementation, many of the core administration and operational functions of NMITE benefit from this inherent ability.

6.5 UPS / Electrical Generator

6.5.1 Uninterruptible Power Supplies should be used on critical devices and networks to provide short term operation during power outages and controlled shutdown where appropriate.

6.5.2 For longer term protection against electrical failure, localised electrical generators can be utilised, however this raises several other considerations such as hazardous/flammable material storage.

6.5.3 Certain environmental conditions (such as air conditioning in server rooms) may necessitate the implementation of generators.

6.6 Intrusion Detection, Conditional Access, Active Monitoring & Appropriate permissions

6.6.1 An important capability of the zero-trust network model is that of connection monitoring. This is used in a number of ways such as to provide information into utilisation, load and distribution, but also to assist with intrusion detection and to ensure that only approved devices that have gone through an onboarding process are able to work on NMITE networks.

6.6.2 Conditional Access is constantly run on every request for information from the array of cloud services – whether email, document storage, records, etc – the assessment of a devices security status, location, operating system, antivirus status etc in conjunction with the requesting users status, and key metrics such as atypical behaviour and impossible travel are used to form a real-time conditional accept/reject decision. Data is only return to the requester providing all criteria are satisfied.

6.6.3 Appropriate permissions and restrictions must be set according to users job roles and organisational requirements. No default open access should exist.

6.7 Physical protective measures

6.7.1 Cable locations – whether internal or external to buildings – should be physically protected with suitable conduits and covers and where possible located out of reach.

6.7.2 Wireless access points (WAP), CCTV and other surface mounted equipment should be ceiling mounted or at high level on walls, and where appropriate enclosed in tamper/vandal proof enclosures.

6.7.3 Although not necessary in all locations, it should be assessed whether network ports in dado/trunking or wall boxes should have lockable capability to guard against accidental or malicious removal, or attempted access to the network infrastructure. Door Access Security

6.7.4 It is important to ensure that areas containing key infrastructure components have controlled access.

6.7.5 All network cabinets should be lockable, and keys should be kept in at least 2 places to ensure availability in the event of emergency access being required.

6.7.6 Wiring closets, server rooms and areas with communication infrastructure should have suitable door access systems in place. If these door access systems are electronically or centrally controlled, a suitable policy must be in place for automatic locking/unlocking in the event of a triggering event.

6.8 Backup & Replication

6.8.1 An appropriate backup plan must be implemented for all systems. This is the primary resource that will be used during the recovery process and in order to hit RTO and RPO criteria this must be tested regularly.

6.8.2 There are numerous types of backup process, but it is vital to ensure that chosen methods do not create a new vulnerability or exposure of information.

6.9 Policy

6.9.1 There are policies such as the Acceptable Use Policy that determine appropriate regulation and control of passwords, restrict access/functionality on devices.

6.10 API Integration

6.10.1 Many cloud-based applications are provided with little or no actual control of the underlying data backup and retention. Where these third-party providers are holding data on our behalf, suitable Service Level Agreements (SLA) are required to ensure that operational continuity is achieved. This is not, however, sufficient for a full DRP.

6.10.2 By ensuring that all cloud applications and services engaged with by NMITE have a detailed and well documented Application Programming Interface, it is possible to ensure that we not only have visibility of data stored outside of our immediate control, but that we also have a path to retention and backup of that data.

6.11 Encryption

6.11.1 The encryption of data both in transit and at rest is a critical requirement for the security of NMITE data and is documented in the NMITE Security and Data Storage policy. During a recovery process, due care must be taken to ensure that data security and integrity is maintained, especially around encryption.

6.12 Remote Wipe

6.12.1 The ability to remotely wipe a device, block or control access to content is built into many mobile devices. This ability can be leveraged to ensure data security during an incident.

6.13 Advanced Threat Protection / Anti-Virus

6.13.1 NMITE leverages Advanced Threat Protection to actively monitor and report on devices as part of Conditional Access. For stand alone, dedicated devices or non-internet connected devices, suitable antivirus software is installed and updated in line with the Data Security policy.

6.14 Manual operation / override

6.14.1 The ability to switch certain electronically controlled devices into a manual control mode is important to ensure

7. Service Level Agreements / Insurance

7.1 SLAs are sought from all primary providers and are either referenced within the contact details section of this document or held with the contract to supply. Insurance policies held by both NMITE and service providers should be checked prior to the financial commitment of any large-scale recovery operation to ensure any requirements are not overlooked which would invalidate such insurance policies.

8. Backup & Replication

8.1 The backup and replication processes for each of the services used by NMITE are documented in the Security and Data Backup policy.

9. Recovery Strategies

Items marked with an asterisk are documented in the Security and Data Backup policy.

Impact	Short term strategy	Short term method	Long term strategy	Long term method
Loss of building Inability to use building Total loss of internet	Relocate to alternative building	Cloud services not affected, high IT availability with immediate effect	Rebuild building/infrastructure	Cloud services not affected during re-occupancy, very low relocation timescale
Partial loss of internet capability	Immediate resilient connection failover Manual failover to secondary provider	Automatic for resilient circuits and routers with multiple WAN (cable,4G/5G)	Engage alternative provider Repair original connectivity	Supplier repair, reinstallation, or new provision. Add resilience.
Loss of internal connectivity	Diagnose and replace equipment Reconfigure devices from backups	Reinstall / reset devices	Consider secondary network, additional redundancy	Procure additional equipment and services
Total loss of Microsoft Tenancy in Data Centre Corruption of loss of Azure admin data/logins	Implement recovery from Backup (AAD)*	Involve Microsoft Perform attribute recovery Perform account recovery	Consider Long Range geographic resilience Consider alternative tenancy provider	Additional data centre accounts
NMITE Data loss from cloud or data centre Loss of VM	Implement recovery from Backup (Data)*	File, Library or Environment recovery	N/A	N/A
Third Party data loss where provider recovery possible	Implement recovery from Backup (3rd party) *	Instigate service provider recovery	N/A	N/A

Impact	Short term strategy	Short term method	Long term strategy	Long term method
Third Party data loss with NO provider recovery	Implement recovery from Backup (API)	Liaise with service provider to ensure recovery	Develop additional API integration	Engage further software development
Device failure, loss, corruption	Implement recovery from Backup (Device)*	Device repair, reset, localised file recovery	Replace device	Procure new equipment

10. Recovery Time Objectives / Recovery Point Objectives

10.1 For each service or data source, there are two parameters that determine the amount of time it takes to recover a service or data to the required operational state (RTO) and the potential maximum amount of data that will be lost as a result of the incident (RPO)

10.2 These two-time parameters are a property of the backup and replication processes that are undertaken and therefore in order to meet organisational requirements, there may be more than one type of process defined and implemented.

10.3 The RPO for a service is concerned with the allowable amount of data loss in the event of a disaster. If the RPO is 24 hours, then all data produced by the service must be backed up (including the time taken for the backup) at least every 24 hours to ensure that this objective is met.

10.4 RPOs are data only based and are generally automated. There is usually a direct cost relationship.

10.5 The RTO for a service or data is concerned with how long a service or data can be unavailable before causing irreparable damage to the organisation. If the RTO is 24 hours, then the service must be restored within that time in order be within requirement.

10.6 Since the RTO is generally associated with a whole operational capability rather than just the data, there is a higher cost relationship with more demanding RTO. The process is nearly always manual and due to the fact, that restore times can vary depending on the time of day and other business loads, it is important to ensure that an RTO is achievable. If an RTO is 2 hours and it takes 4 hours to restore a service at peak times, then it will never be achievable.

10.7 The RTO and RPO parameters for each service are documented in the Security and Data Backup Policy.

11. Security, Permissions and Authority

11.1 Overriding security access & permissions are set according to job role within NMITE and practices are documented in the Security and Data Backup policy.

11.2 During a disaster recovery incident, the authority to action recovery of systems and data lies with the Head of IT/DR Team Leader. In certain severe cases where the impact to NMITE is high it may be necessary to elevate authority to the Senior Leadership Team following assessment and evaluation of the costs and timescales involved in the recovery.

12. Prioritisation, Action & Communication

12.1 The Head of IT/DR Team Leader is responsible for setting the prioritisation and co-ordination of recovery tasks and has overriding control on the actions that are carried out on behalf of NMITE by any third parties.

12.2 Communication of relevant DR information throughout NMITE will also be provided by the Head of IT/DR Team Leader and during severe instances to the Senior Leadership Team for appropriate communication to all staff, students and

contractors. It is essential that accurate information regarding expectations and realistic recovery timescales is conveyed through proper channels.

12.3 In some events such as that of personal data compromise or loss, the Data Controller for NMITE must be informed in order to discharge the legal obligations of informing relevant authorities such as the Information Commissioners Office.

12.4 Press releases or external communication is strictly under the control of the Senior Leadership Team through the appropriate channels in the Marketing Department. Dissemination of information by other paths will be viewed as inappropriate and may well instigate disciplinary action.

13. Validation of Recovery

13.1 The responsibility for validating successful recovery of services and data lies with the Head of IT/DR Team Leader and as such an incident will not be considered to be closed until the Incident Report has been submitted and approved by the Senior Leadership Team.

13.2 Recovery performed by service providers on behalf of NMITE will also be validated by the Head of IT/DR Team Leader and reported on in the same manner as internally handled recovery.

14. Reporting & Incident Analysis

14.1 Full documentation of the incident must be completed in an appropriate timescale. The following must be included in the report:

i. Date & Time of initial incident occurrence
ii. Method and details of notification
iii. Steps leading to identification of the problem
iv. Assessment criteria used to formulate a level of response
v. Third Party / Service Provider involvement
vi. Description of causes
vii. Events record for each step/action/process undertaken including outcomes
viii. Resources involved
ix. Effectiveness of solution and analysis of target objectives/actuals
x. Possible list of mitigations
xi. Lessons to be learned

15. Testing

15.1 In order to be effective, regular testing of the disaster recovery plan should be undertaken. It is only during testing that parameters such as the RTO and RPO can be confirmed as appropriate and to ensure that the data backups are wholly capable of providing the required level of recovery. It is not sufficient to assume that just because data is being backed up that it will be recoverable.

15.2 There may be certain elements that are difficult to fully test in this situation, but these will also only be identified during testing.

16. Policy Status

16.1 This policy is not part of any contract of employment and does not create contractual rights or obligations. NMITE reserves the right to alter at any time although we will notify you of any future amendments.