IT Disaster Recovery Plan

Introduction

In order for the School to function well, it is necessary for its critical information systems and networks to operate effectively, without excessive interruption or loss of service.

The School's IT Disaster Recovery Plan sets out the process to enable critical systems to be recovered within agreed timeframes in the event of service disruption, outage or disaster.

For the purposes of this document a disaster is defined as an unplanned event that disrupts the School's computing or telecommunication services, adversely affecting the School's educational or business functions for a period of time.

Disruptions to ICT systems may be mild (e.g., short-term power loss) to severe (e.g., fire). Although it is not possible to eliminate all risks, putting the appropriate technical, administrative and operational controls in place can bring risk to within acceptable limits. The School is committed to ensuring that the systems and networks that are critical to the School are properly maintained and protected against relevant threats, and that the School has the ability to recover systems in a timely and controlled manner.

This Policy sets out the high-level management processes for recovering service following an IT incident.

Disaster Determination and Declaration

The IT Disaster Recovery Plan is used in the event of the loss of any critical system or network, or component of a system or network leading to a hindrance in the effective operation of the School in providing student, academic, administrative or external information services.

The plan becomes effective when a disaster occurs. The Executive Committee are responsible, with input from the Chair of the Learning Resources, Property, Data & IT Committee, Head of Digital, and external suppliers (where appropriate), for declaring a disaster. The Digital team will respond based on the directives specified by the Chief Executive and Executive Committee.

The impact of the loss can be graded as minor, significant, or extreme. The level of impact is based on an assessment of what the impact would be to the core business. The level of impact then determines the level of control of the incident—operational, tactical or strategic. The principle of escalation holds, whereby an incident can be escalated from one category to the next if, for example, it is having its effect over a prolonged period of time, if it is part of a pattern leading to multiple incidents, or if in the process of handling the incident, it becomes clear that the impact is greater than originally assessed.

Minor incidents are identified, assessed and logged routinely by operational staff. In the case that the impact of a minor incident becomes prolonged or more severe, or is part of a pattern, leading to multiple incidents, the operational staff escalate it to Significant and report it as such to the Chair of the Data & IT Working Group.

Significant incidents are determined by the Head of Digital, either directly or as a result of an escalation of a minor incident by his/her team.

Extreme incidents are determined by the Head of Digital in conjunction with the Chair of the Learning Resources, Property, Data and IT Committee and immediately escalated to the Chief Executive and the Executive Committee.

Impact levels and levels of control

Impact of incident	Definition	Level of control required	Description
Minor	Effect on School systems or network is minimal, causing a minor inconvenience to a specific group of users.	**Operational** *(Bronze Command in crisis management terminology)*	Incident dealt with by technical staff (i.e., IT department staff and contractors), without the need to report to higher levels of control. (E.g., resetting of a server or network router to recover service).
Significant	Effect on School systems or network is significant and affects multiple user groups, with significant parts of the network or critical systems are affected.	**Tactical** *(Silver Command in crisis management terminology)*	Head of Digital, alongside Chair of Learning Resources, Property, Data & IT Committee, coordinates and directs operational resources (department staff and IT contractors) to ensure contingency plan properly executed.
Extreme	Entire network is unavailable, central systems have failed, or an incident affects the campus as a whole (e.g., data centre fire).	**Strategic** *(Gold Command in crisis management terminology)*	Incident dealt with at strategic level by CEO and Executive Committee, who determine priorities and deliver instructions to the Head of Digital and Chair of Learning Resources, Property, Data & IT Committee

Regardless of the Disaster Circumstances, or the identity of the persons first made aware of the disaster, the Business Continuity plan will be activated if the School loses two or more of the following services/systems:

- Internet connection/servers (if appropriate)
- Software for teaching and learning incl. Learning Management System
- Business/administrative systems incl. Student Records System, Finance System
- Learning resources and classroom technologies
- Critical staff and student access devices, incl. printers
- Infrastructure, Fibre Optic cabling and network management switches and routers

THE LONDON INTERDISCIPLINARY SCHOOL

Incident Management Process

Stage	Actions
1: Emergency Response	Requires relevant personnel (dependent on impact level) to come together Impact assessed, impact level declared, and plan of action determined. Plan of action to include: • Agreeing and documenting activities needed • Agreeing priorities and estimated timescales • Agreeing communications and reporting arrangements • Identify specialist staff needed (if appropriate) • Identify costs involved for replacement equipment Includes informing and engaging recovery teams, third party vendors and partners to start the recovery effort.
2: Recovery Process	Continuity actions conducted to restart essential operations, including: • Notify suppliers of likely requirements • Obtain approval for purchases and place orders • Manage restoration of each system, keeping relevant campus staff and stakeholders elsewhere informed of the progress of the resumption of services
3: Restoration of Service	Conditions restored to normal. Restoration of a system may include: • Agreeing a suitable new physical location for the system • Install infrastructure • Procurement of suitable new equipment • Obtain software support for re-installation from suppliers of third party applications • Restore data from backups
4: Review	Incident reviewed to identify actions, changes or investments required to reduce risk of recurrence. Risk log is reviewed and updated.

Roles and responsibilities

Chief Executive and Executive Committee (Strategic Control of Extreme Incidents)

In the case of an extreme incident, the role and responsibilities of the Chief Executive and Executive Committee are as follows:

- Communicate with key stakeholders;
- Provide management control and strategic direction, including resolving issues of priority to School;
- Determine whether to implement resolution plans proposed by Head of IT, and any other actions;
- Plan and execute any movement to an alternate site where appropriate;
- Approve emergency equipment purchases;
- Secure financial and human resources as required;
- Communicate with media where required;
- Approve damage assessment and negotiate with insurers.

Head of Digital **(Tactical Control of Significant Incidents)**
In the case of a significant incident, the role and responsibilities of the tactical lead, the Head of Digital, are as follows:

- Escalate, if necessary, to Extreme impact and the passing of control to the Chief Executive and Executive Committee;
- Communicate with key stakeholders;
- Provide management control and tactical direction;
- Determine whether to implement resolution plans proposed by operational staff, or any other actions;
- Secure financial and human resources as required;
- Approve damage assessment and negotiate with insurers.

It is also the responsibility of the Head of Digital, with support from the Learning Resources, property, Data & IT Committee, to provide ongoing advice to the Executive Committee on issues of technological resilience and recovery and information security.

Digital Associate
Someone from the IT/Digital Team, to support the Head of Digital in delivery of role as Tactical Control

Monitoring and Review

This Plan will be reviewed annually by the Head of Digital and Chair of Learning Resources, Property, Data & IT Committee, and any changes agreed by the Learning Resources, Property, Data & IT Committee.

THE LONDON INTERDISCIPLINARY SCHOOL

Version control

Name of policy/procedure:	**IT Disaster Recovery Plan**
Document owner:	**Head of Digital**
Date Originally Created:	**01/2019**
Related documents: (e.g. associated forms, underpinning processes, related policies or overarching policies)	**Risk Management Policy** **Business Continuity Plan**

Version Control			
Version	**Author**	**Date**	**Brief summary of changes**
1	Hannah Kohler (Director of Admissions and Student Support)	13/01/2019	Original draft
2	Jasper Joyce (Director of Finance and Operations)	12/03/2019	Minor wording changes
3	Hannah Kohler (Director of Admissions and Student Support)	05/08/2019	Minor wording change
4	Jasper Joyce (Director of Finance and Operations)	10/08/19	Inclusion of further detail relating to: Disaster Determination and Declaration, and Incident Management Process
5	Executive Committee	08/08/2019	Approved
6	Kestral Gaian Chair of the Data & IT Working Group	20/10/2021	Updating document to reflect new structures and systems.
7	Kestral Gaian, Head of Digital	LRPD&IT Committee 23/11/2022	Updating to reflect change in committee structure