Stratford College London

IT Disaster Recovery Plan

Policy Version Number	SCL/ITDRP/APR2026/02
Member of Staff Responsible for Policy	Jonathan Omani

Record of Revisions to Policy

Date	Details	Approved by
28 MAY 2018	Published	BoD
23 Mar 2024	Reviewed	BoD
23 Mar 2025	Reviewed	BoD
23 Apr 2026	Reviewed	BOD

Date of Current Policy	23 Apr 2026
Policy Review Date	23 Apr 2027
Review to be approved by	BOD

IT Disaster Recovery Plan

Objectives/Constraints

A major objective of this document is to define procedures for a contingency plan for recovery from disruption of computer and/or network services. This disruption may come from total destruction of a server room or from minor disruptive incidents. There is a great deal of similarity in the procedures to deal with the different types of incidents however special attention and emphasis is given to an orderly recovery and resumption of those operations that concern the critical business of running the College including providing support to curriculum activities relying on computer systems. Consideration is given to recovery within a reasonable time and within cost constraints.

Assumptions

This section contains some general assumptions, but cannot include all possible particular situations that can occur. Particular decisions for situations not covered in this plan needed at the time of an incident will be made by appropriate staff members on site.

This plan will be invoked upon the occurrence of an incident. The senior staff member on site at the time of the incident or the first one on site following an incident will contact the College Principal and/or IT & Technical Services Manager for a determination of the need to declare an incident. The Director of Studies will also be notified.

The IT & Technical Services staff member on site at the time of the incident will assume immediate responsibility. The first responsibility will be to see that people are evacuated as needed. If injuries have occurred as a result of the incident, immediate attention will be given to those persons injured. If the situation allows, attention will be focused on shutting down systems, turning off power, etc., but evacuation and individual safety are the highest priorities.

Once an incident which is covered by this plan has been declared, the plan, duties, and responsibilities will remain in effect until the incident is resolved and proper College authorities are notified.

Invoking this plan implies that a recovery operation has begun and will continue to be the top priority until workable computer support to the College has been re-established.

Incidents Requiring Action

The IT disaster recovery plan will be invoked when there is an actual or threatened circumstance that will result in “significant impairment‟ of the curriculum and/or administrative systems that the IT & Technical Services team manages. This could include:

1. An incident which has disabled or will disable, partially or completely, the curriculum network facilities for a period exceeding one business day.
2. The loss of data that significantly exceeds the normal day to day restoration of student/staff files.
3. An incident that has significantly impaired the use of computers and networks managed by IT & Technical Services due to circumstances which fall beyond the normal processing of day-to-day operations.
4. The threat of significant loss of data, systems or facilities.

5. An incident which was caused by problems with computers and/or networks managed by IT & Technical Services and has resulted in the injury of one or more persons.

Possible Contingencies: Areas of Risk

General situations that can destroy or interrupt the computer network usually occur under the following major categories:

- Power/Air Conditioning Interruption
- Fire
- Water ingress
- Weather and Natural Phenomenon
- Malicious damage (sabotage, hacking)
- Denial of service or virus attack

There are different levels of severity of these contingencies necessitating different strategies and different types and levels of recovery. This plan covers strategies for:

- Partial recovery - operating at an alternate site.
- Full recovery - operating at the current main college site possibly with a degraded level of service for a period of time.

Types of Computer Service Disruptions

This document includes hardware and software information, emergency information, and personnel information that will assist recovery from most types and levels of disruptive incidents that may involve networking facilities.

Some minor hardware problems do not disrupt service; maintenance is scheduled when convenient for these problems. Most hardware problems disrupting the total operation of the computers are fixed within a few hours.

Fire

All floors are equipped with manual CO_2 fire extinguishers, which will adequately protect the equipment from fires starting in the room itself. If a fire starts, the equipment could be used to limit damage to the affected piece of equipment and possible minor damage to equipment in the immediate vicinity. This would be handled as described in the preceding section:

In the event of a catastrophic fire involving the entire building, we would most likely have to replace all our hardware. Our critical servers are backed up daily and tapes are stored in the IT & Technical Services office and off site.

Security Strategies

The college employs standard security strategies. For example by adopting the use of standard software and hardware, local and wide area networking components. This includes Microsoft software on all PCs and laptops, Microsoft Office 2010 and Windows Server software, switches and also routers. This industry standard approach will in itself permit reasonable mitigation of outage through market reliability and knowledge.

Individual users shall be made aware of their responsibilities with regard to how they can contribute to the overall security level. Guidance on good practice shall be provided to all users (curriculum and administrative, staff and students) and correspondingly special efforts shall be directed to those who are handling particularly sensitive information such as student record information, personnel information and financial information.

A system is in place to ensure the prompt removal of access rights, and the removal of data, of staff and students on leaving.

The College shall ensure that business continuity plans are in place to ensure that all systems and networks have appropriate plans and recovery strategies for major breakdown, loss of network facilities or data. This includes plans to recover data, test our restore systems, source replacement servers, network and other critical components.

IT Disaster Recovery Team

Possession of IT Disaster Recovery Plan

The primary copy of the IT Disaster Recovery Plan is held in the IT & Technical Services folder on the public drive on the College Network. Soft and hard copies of the Plan will be kept by the Principal, DOS, HoD. Copies are also held by all members of IT & Technical Services.

IT Disaster Recovery

In the event of a disaster the recovery team will meet as follows:

1. If The Hub is usable, the recovery team will meet in the office of The IT & Technical Services

2. If The Hub is not usable, the recovery team will meet in an appropriately safe location.

3. If the college facilities are not usable then it is presumed that the disaster is of such proportions that recovery of IT facilities will take a lesser priority. The IT & Technical Services will make suitable arrangements.

Preparations for a disaster

This section contains the steps necessary to prepare for a possible disaster and as preparation for implementing the recovery procedures. An important part of these procedures is ensuring that the off-site storage facility contains adequate and timely computer backup tapes and documentation for applications systems, operating systems, support packages, and operating procedures.

General Procedures

Responsibilities have been given for ensuring each of following actions have been taken and that any updating needed is continued.

The IT & Technical Services is responsible for

- maintaining, reviewing and updating the IT disaster recovery plan.
- Ensuring that all members of the IT & Technical Services receive copies of the Plan and are given the opportunity to discuss its implications.
- Ensuring that procedures are in place to ensure the scheduled rotation of backup media including the movement of weekly backup tapes.
- Maintaining and periodically updating IT disaster recovery materials, specifically documentation and systems information (electronically and manually).
- Maintaining a current asset register of equipment.
- Ensuring that the College is aware of appropriate disaster recovery procedures and any potential problems and consequences that could affect their operations.
- Ensuring that the proper environment is maintained in server areas.

Recovery Procedures

This portion of the disaster/recovery plan will be set into motion when an incident has occurred that requires use of the alternate site, or the damage is such that operations can be restored, but only in a degraded mode in a reasonable time.

It is assumed a disaster has occurred and the Critical Incident Plan is to be put in effect. This decision will be made by the Principal / DOS upon advice from the IT Team.

In case of either a move to an alternate site, or a plan to continue operations at the main site, the following general steps must be taken:

- Determine the extent of the damage and if additional equipment and supplies are needed.
- Obtain approval for expenditure of funds to bring in any needed equipment and supplies.
- Notify local vendor marketing and/or service representatives if there is a need of immediate delivery of components to bring the computer systems to an operational level even in a degraded mode.
- If it is judged advisable, check with third-party vendors to see if a faster delivery schedule can be obtained.
- Notify vendor hardware support personnel that a priority should be placed on assistance to add and/or replace any additional components.
- Notify vendor systems support personnel that help is needed immediately to begin procedures to restore systems software.
- Order any additional electrical cables needed from suppliers.
- Rush order any essential technical supplies that may be needed.

In addition to the general steps listed at the beginning of this section, the following additional major tasks must be followed in use of the alternate site:

- Coordinate moving of equipment and IT support personnel into the alternate site.
- Bring the recovery materials from the off-site storage to the alternate site.
- As soon as the hardware is up to specifications to run the operating system, load software and run necessary tests.
- Prepare backup materials and return these to the off-site storage area.
- Set up operations in the alternate site.

- Work out plans to ensure all critical support will be phased in.
- Keep SMT and staff informed of the status, progress, and problems.
- Coordinate the longer range plans with SMT of continuing support and ultimately restoring the overall system
- To ensure that if a breach of security has occurred that any access points are secured and passwords changed.

Degraded operations
In this event, it is assumed that an incident has occurred but that degraded operations can be set up. In addition to the general steps that are followed in either case, special steps need to be taken.

- Evaluate the extent of the damage, and if only degraded service can be obtained, determine how long it will be before full service can be restored.
- Replace hardware as needed to restore service to at least a degraded service.
- Perform system installation as needed to restore service. If backup files are needed and are not available from the on-site backup files, they will be transferred from the off-site storage.
- Work with the various vendors, as needed, to ensure support in restoring full service.
- Keep the SMT informed of the status, progress and problems.

Appendix 1 – Data Back Ups and Restoration

There are a variety of reasons for file server failure including hardware/software conflicts and failure, accidental or deliberate damage, hacking and inexplicable failures normally called „Act of God failures'.

The following documentation gives details of our backup procedures and will enable the recovery of data in circumstances where a catastrophic loss of data has occurred due to file server failure. All our backups are run with a verification option and test restorations are performed

Appendix 2 – Testing Procedures

It would be impractical to simulate an actual disaster on the entire college network as this would require the creation of a temporary server room with enough servers to recover the main college systems. This would be expensive and very time consuming. A more suitable approach would be to simulate a disaster in one particular area of the college network. The network can be sectioned into eight separate areas.

They are:

- Internet Access
- Staff E-Mail
- Student Data
- Staff Data
- Core Network Servers
- Print Services
- Wireless
- CIS

Therefore approximately every six weeks one of these areas would be restored fully from backup onto a disaster recovery server. This would simulate a disaster in part of the college network without the requirement of taking the area offline.

However, after a disaster has occurred it would be necessary to resort from backup anyway and therefore this test will adequately provide a suitable testing platform for our services.