

The New School at West Heath

Policy on Information Systems - Disaster Recovery and Business Continuity Plans

Introduction

The New School at West Heath makes use of information systems and technology for both the administration of the school and directly for educational purposes. This policy relates to both these functions. The school has a variety of IT and paper based systems.

Aims and Objectives

- To ensure that the school is protected against disaster resulting from fire, computer failure and virus attack and theft in relation to finance and efficient running.
- To ensure that the school is able to continue to meet the educational needs of its students, to meet all statutory requirements and to fulfil the service level agreements made with sponsoring authorities in the event of the above.
- To ensure that all computers used for curriculum purposes are protected from interference by students whether accidentally or deliberately.

Strategies

For the purpose of clarity this policy separates administration from curriculum systems. It also separates short-term failures from long-term failures.

A. Administration

Computer Based Systems		
Uses	Short-term failure	Long-term failure
<ul style="list-style-type: none">• Invoicing sponsoring authorities & parents• Orders and payments	<ul style="list-style-type: none">Late payment of creditorsDisruption and delays to suppliesPossible breach of contract	<ul style="list-style-type: none">No incomeLoss of business credibility
<ul style="list-style-type: none">• Lettings	<ul style="list-style-type: none">Disruption of service	<ul style="list-style-type: none">Loss of reputation and good will in the community
<ul style="list-style-type: none">• Student records	<ul style="list-style-type: none">Minimal because of duplication	<ul style="list-style-type: none">Not applicable

The following strategies and measures are in place to minimise the above risks:

Inventories of

- All hardware
- All operating systems with full details of versions and licence numbers
- All software with full details of versions and licence numbers
- All passwords and user identification log ons
- All installation software CDs
- All licences
- All maintenance contracts
- Back-up floppy and re-writable CDs and tapes
- Students do not have unsupervised access to any areas that contain the administrative computers.

Paper Based Systems		
Uses	Short-term failure	Long-term failure
• Personnel Information	Disruption and inconvenience	Service compromised
• Invoices	Disruption and inconvenience	Service compromised
• Payroll	Outsourced - no threat	Not applicable
• Student records	Minimal because of duplication	Not applicable

The following strategies and measures are in place to minimise the above risks:

- Records stored in fire-resistant cupboards
- Fire detectors and fire alarm system connected to central control and fire station for rapid response
- Secure locks fitted to all areas storing sensitive or important information
- Students do not have unsupervised access to any areas that contain the administrative computers.

B. Curriculum

Computer Based Systems		
Uses	Short-term failure	Long-term failure
• Teaching ICT - room with computer network with internet access	Loss of student work Inconvenience	Examination results compromised
• Classroom support - a variety of stand alone computers distributed round the school	Loss of student work Inconvenience	Examination results compromised

The following strategies and measures are in place to minimise the above risks:

- Back-up tape streamer and virus protection software in ICT room
- Virus protection software installed on standalone machines

- Partition and protection software on standalone computers, which render it impossible for students to alter settings or install, unauthorised software on them.
- Passwords for administrator level access, regularly changed
- Back-up of students' work on floppy disks or re-writable CDs
- Hard copies printed. Worst case scenario - retyping of work.

External Agencies

The School Network has full virus protection measures provided by Research Machines plc. Virus protection for standalones with internet access is provided by the service providers.

Development Plan Note:

At the time of writing a proposal is being prepared for the trustees for the recruitment of an ICT Development Manager. This role will include responsibility for all disaster recovery issues relating to ICT at the New School.

Information Systems & Disaster Recovery	
This Policy should be read in conjunction with the following policies:	
Appendices:	
Monitoring of Policy Implementation is the responsibility of: The Senior Leadership Team	
Lead responsibility:	Vice Principal - Residential
Relevant Legislation:	To be detailed in the next release
Annual Policy Review Required:	Yes / No
Approved by: S.S. Committee	Date approved: 29/09/04
Ratified by: Trustees	Date ratified: 11/2004
Reviewed – no changes	Date:
Reviewed – with revisions	Date:
Revision No.	1.1