Physical and Environmental Security

Lead Person : **Systems Manager**

Support Persons : **SLT**

Governing Body Committee : **Asset Management**

Our Aims: to prevent unauthorised access, damage or significant disruptions to ICT facilities

Context : operational spaces, bureaus, hardware set-ups.

Secure spaces

Physical security of the environment
Spaces in which vital (ICT) facilities are housed are defined and specified as such and subject to extra security.

All locations are provided with a lightning conductor installation.

Control of physical access

- Maintenance staff who carry out work on ICT installations are constantly accompanied by an expert internal staff member.
- Rooms, cupboards and shutters must all be lockable.
- Each location must have at least one secure room for storage or installation of sensitive or critical components.
- Entrances and exits of locations are subject to a form of supervision.

Security for computer rooms

- Access to secure spaces is reserved for those with appropriate authorization; in the event of emergencies the security service and technical service also have access.
- Secure spaces are provided with fire detection and extinguishing equipment.
- ICT staff must be aware of where fire-fighting equipment is kept.
- Keys to drawers and cupboards must be carefully administered.

Delivery of goods

- Goods intended for ICT services are delivered under supervision and stored securely.
- Goods intended for ICT services are signed for receipt on delivery.

Clear Desk Policy

- Sensitive information may not be open to casual consultation in operational spaces.
- Sensitive information may not be left unmanaged in operational spaces.

Removal of school property

- School equipment may be taken elsewhere only with formal permission from the responsible party.

Security of equipment

Positioning and security

- Equipment may not compromise the accessibility of emergency exits.
- There is a defined procedure for acquisition of equipment and software.

Use outside the institution

- External use of institution equipment requires authorization in accordance with regulations.
- External use of institution equipment is subject, as a minimum requirement, to the internal security requirements.
- On its return, externally used institution equipment must be in the state in which it was issued.

Discarded resources

- Information carriers which accompany equipment due to be discarded are destroyed or cleaned at bit level.

Updated : November 2016

Approved Full Governors December 2016