

Gravenhurst Academy

Policy for Computing security

Physical Equipment Security

- Where possible computer equipment will be situated so as to reduce the risk of unauthorised access and damage.
- The details of all computer equipment will be recorded in the official inventory record together with relevant serial numbers.
- Computer hardware will be appropriately security marked using an etcher.
- A record will be kept of any computer equipment taken off site and kept in the inventory record book. The removal of any equipment from the school's premises must be authorised by the Principal
- Modems will be switched off when not in use.
- The **officer responsible for physical equipment security is Mrs D Randall**

Backup Procedures

- All data will be saved on the computer hard disks.
- All data held on the school's computer system will be backed up at least once a week on the Server Hard Drive and the office computer onto encrypted memory sticks.
- Keys will be backed up to encrypted memory sticks weekly and a copy of finance backed up after each monthly reconciliation.

- A year-end backup of financial data will be taken and retained using separate disks.
- All computer backup disks will be stored off-site overnight.
- The **officers responsible for backup procedures is Mrs C Davison/ Mrs A Day.**

Virus Detection

- All computers will have virus detection software installed within their start-up procedures. The software should be updated regularly.
- Any disks of uncertain origin must be scanned for viruses before use.
- The use of unlicensed software is prohibited.
- Any perceived virus attack should be immediately reported to Mrs D Randall.
- The **officers in charge of virus protection is Mrs C Davison/ Mrs A Day.**

Software Controls

- All software maintained on the school's computers must be properly owned by the school. Software may only be used in accordance with the licence agreements.
- All licences and system disks will be held in the fireproof metal filing cabinet.
- An inventory of all software maintained on the schools computers will be kept together with relevant serial numbers with the ICT policy.
- Access to software will be restricted to authorised staff.
- **The Principal is the System Manager** and is the only person who may issue passwords and amend access levels.
- Users of the school's computer system will be issued with individual passwords.
- It should be ensured that passwords are kept confidential. They should be changed at least every half term.
- Staff should log out of the computer system before leaving the office unattended.
- When staff leave, their passwords will be deleted immediately by the Systems Manager.
- Any suspected breach of security will be immediately reported to the Principal.
- The **officer responsible for software controls is Mrs D Randall.**

Legal Obligations

All staff should be made aware of the requirements and their responsibilities in relation to the following legal statutes:

- 1984 Data Protection Act
- 1986 Copyright, Designs and Patents Act (extended to cover computer software)
- 1990 Computer Misuse Act

Please contact the **Principal**

Acquisition, Maintenance and Disposal of Hardware

- The Principal has overall responsibility for the acquisition, maintenance and disposal of equipment.
- The Central Purchasing Department and Courtland Services will be contacted when buying equipment to ensure “best prices” are obtained from suppliers.
- Official orders will always be used to make any purchases.
- The write off and disposal of equipment should be authorised by the Governing Body and the Principal
- Acquisition and disposal of equipment must be in accordance with the Financial Regulations for Schools.

User Training

- Users should receive appropriate training in the correct use of the school’s IT facilities including use of software packages and security arrangements.

Disaster Recovery

- There will be adequate arrangements in place for disaster recovery including emergency procedures, manual fallback plans and resumption procedures.
- The **officers responsible for disaster recovery is Mrs C Davison/ Mrs A Day.**

This policy has been reviewed byon behalf of the Governing Body and will be reviewed on a triennial basis.

Chairman

Principal

Date