

Physical Equipment Security

Where possible, computer equipment will be sited 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.
- A record will be kept of any computer equipment taken off site. The removal of the equipment from the school's premises must be authorised by the Headteacher/Children's Centre Manager.
- The Officers responsible for the physical equipment security are the Headteacher/Children's Centre Manager and the ICT Technician.

Back-up Procedures

- All data held on the school and children's centre computer systems will be backed up at least once a week.
- There will be at least three generations of back-up information stored on a memory stick.
- A year-end backup of financial data will be taken and retained using a memory stick each year.
- The latest version of the computer backup will be stored off site and the office set of backup disks will be kept in a secure place.
- The Officer responsible for the back-up procedures is the Office and Finance Manager .

Virus Detection

- All computers will have virus detection software installed within their start-up procedures; the software is up-dated regularly.
- Any CDs or memory sticks 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 the Headteacher/Children's Centre Manager and the ICT Technician.
- The Officers responsible for virus detection procedures are the ICT Technician and the Administration Team from the school and the children's centre.

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 license agreements.
- All licenses and related software will be held securely.
- Access to software will be restricted to authorised staff.
- The ICT Technician, the Office and Finance Manager, Finance Assistant and the Children's Centre Coordinator are the Systems Managers; they are responsible for ensuring that individuals are issued with passwords and they may also amend access levels.
- Users of the school's computer system will be issued with individual passwords.
- It should be ensured that passwords remain confidential; they should be changed regularly for security reasons.
- Staff should not leave any of the office computer systems unattended when accessible; they should log out of the system before leaving the office.
- When members of staff leave, their passwords will be deleted immediately by the ICT Technician, the Office and Finance Manager or the Children's Centre Coordinator.
- Any suspected breach of security will be immediately reported to the Headteacher/Children's Centre Manager.
- The Officers responsible for the software controls are the ICT Technician, the Office and Finance Manager and the Children's Centre Coordinator.

Acquisition, Maintenance and Disposal of Hardware

- The Headteacher/Children's Centre Manager has overall responsibility for the acquisition, maintenance and disposal of equipment.
- The write-off and disposal of any equipment should be authorised by the Governors and Headteacher/Children's Centre Manager through the Governing Body Health and Safety Sub-Committee meetings.
- 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 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 are the Headteacher/Children's Centre Manager and the Administration Team from the school and the children's centre.

Internet Access

- There will be adequate procedures in place to ensure that access to the internet is restricted to authorised staff.
- The ICT Technician, the Office and Finance Manager and the Children's Centre Coordinator are the Officers responsible for ensuring that access is restricted.

R. Willsher (Computing and EYFS Leader)

January 2015