

# **SANDY UPPER SCHOOL & COMMUNITY SPORTS COLLEGE**

## **Computer Security Policy**

### **Rationale**

It is a fact of life that the smooth operation of our school depends on effective and safe use of information technology and web-based materials by both students and staff.

This document sets out the policy for both the practical management of our resources and the policies in place to ensure that materials transferred and stored electronically are safe and secure.

### **PART 1: MANAGING RESOURCES**

Due to the expensive nature of ICT equipment it is vital that purchases are planned, that equipment is maintained in a good condition and that it is used effectively.

1. ICT Technicians are responsible for maintaining an "Assets Register" which monitors the condition and deployment of all ICT.
2. Staff responsibilities are outlined in the document "Safe and Appropriate Use of ICT by School Employees" (Appendix 1). This has been issued to staff and a list of those who have signed is held in the Personnel Office.
3. All staff have a duty of care to monitor ICT equipment and report faults. Additionally, ICT technicians monitor equipment daily and report damage and faults to SLT link.
4. From time to time, equipment may be replaced due to age, damage or general wear and tear. Where possible, equipment will be re-used in other parts of the school but there will be some cases in which equipment will be disposed of. In this event, the disposal will be agreed by the Headteacher in agreement with Governors.
5. Equipment which is disposed of will have all data removed before this disposal and this will be certificated.

### **PART 2: E-SAFEGUARDING**

Guidance on e-safeguarding was received from Central Bedfordshire LA on 1<sup>st</sup> December 2009. The following section is written in response to this guidance which can be seen in full in the document "E-Safeguarding: Creating Working Procedures in Schools". The document makes the following recommendations:-

#### **1. Role and Responsibilities**

- a. All schools should nominate a Senior Information Risk Officer (SIRO). For 2009/2010 this will be Elaine Boyd.
- b. A network manager shall be identified and a job description clarifying e-safeguarding role shall be produced.
- c. All those who are responsible for specific information shall be identified (they are known as IAOs) and they will be briefed about the management of this information and how it is to be stored, transported and disposed of.

#### **2. Procedures**

- a. A risk assessment for e-safety will be produced and updated annually.
- b. All information held will be logged and classified as "general", "restricted" or "confidential".
- c. Access control will be reviewed annually.

- d. Procedures for information storage will be agreed and managed by the ICT support staff and the IAOs.
- e. Firewalls and systems protection will be put in place meeting LA recommendations.

**3. System Use**

- a. All staff will be issued with the “Safe and Appropriate Use of ICT by School Employees” (Appendix 1) annually and will sign to show their acceptance.
- b. Password protocols will be reviewed annually and in the light of any security or e-safeguarding breach.
- c. Training will be provided which makes staff and students aware of their responsibilities to ensure safe, responsible and legal use of ICT.

**4. Incident Reporting**

- a. A log for recording breaches of e-safeguarding shall be set up and maintained in the personnel office.
- b. Personnel will establish e-safeguarding routines for staff joining and leaving the school.

**5. Remote Access**

- a. Remote access will be in line with an agreed policy to be created with support from the LA E-learning Team.
- b. All remote access will require password protection.
- c. Systems will be established to prevent breaches of security.

**6. Technical Security**

- a. Systems to be set up with a sufficient technical specification.
- b. All machines should have up-to-date anti virus software.
- c. All incoming mail should be scanned and filtered.
- d. Back-up procedures should be in place and be robust.
- e. Security logging systems to be in place.

First Implemented March 2010				
Review/ Evaluation Date	Re-Written Revised	Staff Responsible	Governors Sub-Committee	Review Cycle
March 2011	June 2011	EMB EMB	Business Business	Annual Annual