

# **COMPUTER SECURITY POLICY (STAFF)**

## **1 Policy Statement**

In view of the College's heavy reliance on data processing systems the confidentiality, security and accurate processing of data are of considerable importance. If there are delays or curtailment of computer processing, serious inconvenience and even financial loss may result.

To help maintain equipment, systems and data in a sensibly controlled environment there are a number of requirements to be observed. These requirements are set down for the first time in this document, which is to be seen as part of the Governing Body's response to the Data Protection Act.

## **2 Computer Equipment**

- 2.1 Heads of Department are responsible for computer equipment under their control and for its proper use.
- 2.2 The use of equipment for purposes not directly concerned with the employer's business is allowed only with the permission of the Head of Department. Computer games are permitted only for demonstration purposes and with the express permission of the designated officer.
- 2.3 Only persons authorised by the designated officer may operate computer equipment.
- 2.4 Computer equipment must have security facilities appropriate to the sensitivity of data held.

## **3 Computer Systems and Data**

- 3.1 All computer programs and data developed for the employer are for the sole use of the employer except by permission of the Head of Department.
- 3.2 Staff negotiating contracts, under which software is to be written for the employer, must seek to ensure that suitable arrangements are made for the copyright to be vested in the employer.
- 3.3 Deliberate unauthorised access to, copying, alteration, or interference with computer programs or data is not allowed. Staff must not make or use unauthorised copies of copyrighted software.
- 3.4 A serious view will be taken of unauthorised disclosure of information from computer input or output.
- 3.5 Waste computer output must be disposed of with due regard to its sensitivity. Confidential printed output must be shredded. Individual

departments will be responsible for ensuring that appropriate facilities are provided.

## **4 Security Systems**

### **4.1 Terminals**

4.1.1 Permission from the Network Manager is required in advance to link terminals to the mainframe computer.

4.1.2 Terminals must never be left unattended when 'signed-on' to the system.

### **4.2 Passwords**

4.2.1 Passwords must not be disclosed to unauthorised persons.

4.2.2 The use of another person's Usercode/Password is not allowed except where they are shared within departments.

4.2.3 Passwords should be a minimum of 5 characters, and changed regularly to a previously unused password.

4.2.4 Only the designated IT Officer will reset forgotten passwords.

## **5 Secured Areas**

5.1 Only persons authorised by the Network Manager will be allowed in secure areas.

5.2 The transfer of identity cards, access tokens or disclosure of access codes to unauthorised personnel is not allowed.

5.3 The loss of identity cards, access tokens or breaches of security must be reported to the Head of Department.

5.4 Keys for secured areas (rooms, safes etc) must not be handed to unauthorised staff.

5.5 Computer rooms and facilities must be adequately protected, and staff must be designated and made accountable for maintaining and monitoring the security procedures.

## **6 General**

6.1 Persons leaving the employment of Governing Body must return on or by their last working day, all identity cards, manuals, equipment and any other property belonging to the employer.

- 6.2 Violations of security procedures established within this security policy must be reported to the Head of Department.
- 6.3 Periodic checks will be made by the Network Manager to ensure compliance with these rules.
- 6.4 The requirements contained in this policy statement are of a general nature covering all computers. Additionally there may be requirements designed for specific equipment and sites. Security recommendations are also included in the Standards for Microcomputers, and Guidelines for Computer Security.
- 6.5 These requirements have been agreed by the Governing Body. They may be modified from time to time in response to changing demands, both operational and legislative. If this happens you will receive a copy of the revision.

**Ratified by the Community Committee of the Governing Body  
12<sup>th</sup> May 2008**

.....

**This portion must be returned to your Line Manager.**

I confirm receipt of the College Computer Security Policy.

Signed: .....

Name (Capitals): .....

LINE MANAGER:

If you would like this held on personnel files, please forward it to the PA to the Principal