STEPHENSON COLLEGE

POLICY FOR COMPLIANCE WITH THE DATA PROTECTION ACT 1998

(Extracted from Information systems security policy POL028)

1. Introduction

It is a requirement of the Data Protection Acts 1984 and 1998 that personal data must be held and processed securely and this is a component of the College's Data Protection policy, the full details of which may be found on the College Web. The processing of personal data, in the College has to be registered with the College Data Protection Officer. In accordance with the Act, personal data has to be handled in compliance with a set of eight principles. The Act also gives rights to persons about whom data is held (Data Subjects) which must be observed.

2. Registration/Notification

Any personal data held on computer, or manually in relevant structured files, as defined in the Act, may be processed for a particular purpose only if that purpose has first been registered with the College Data Protection Officer, and subsequently notified to the Information Commissioner. Where a user downloads personal data from a database for his/her own use, this constitutes a new database and must be registered accordingly. The College is also required to lodge with the Commissioner the details of the systems it has put in place to ensure the security of personal data held on those databases.

3. Compliance with the Data Protection Principles

The Data Protection Act 1998 sets out 8 Principles with which those collecting, storing and disclosing personal data, whether dealing with manual data or data processed by computer, must comply: Data must:

3.1 be obtained and processed fairly and lawfully and shall not be processed unless certain conditions are met; special additional conditions apply to sensitive data;

3.2 be obtained for a specified and lawful purpose and shall not be processed in any manner incompatible with that purpose;

3.3 be adequate, relevant and not excessive for those purposes;

3.4 be accurate and kept up to date;

3.5 not be kept for longer than is necessary for that purpose;

3.6 be processed in accordance with the data subject's rights;

3.7 be kept safe from unauthorised access, accidental loss or destruction;

3.8 not be transferred to a country outside the European Economic Area, unless that country has equivalent levels of protection for personal data.

Staff and students of the College or others who process or use any personal information for the College must ensure that they follow these principles at all times.

4. Data Security

Ensuring that personal data is held securely is thus a key feature of the Data Protection Act. Personal data is not to be disclosed either orally or in writing or accidentally to any unauthorised third party. If computerised it is to be protected by password, encryption or firewall according to sensitivity or kept only on a disk which is itself kept securely. Unauthorised disclosure will usually be considered a disciplinary matter and may be considered gross misconduct in some cases.

5. Subject Access

In accordance with the 1998 Act, a data subject is entitled to be given a description of the types of data about them being processed by the College, the purposes for which they are being processed, a description of the types of potential recipients of this data and to be given any information as to the source of the data held where it was not from the data subject himself. In addition, where data is processed automatically, and is likely to be the sole basis for any decision affecting the data subject, then s/he is also entitled to know the logic involved in the decision-making. A data subject also has a right, subject to certain exceptions, and subject to the payment of a fee, to see the actual data held about him/herself. Subject access may not be granted where this may result in the disclosure of information about another individual or where it may be required for the purpose of safeguarding nation security or the prevention or detection of crime. Students may not be given access to information they have recorded on their examination papers although they are entitled to see the marks received.

When setting up and using databases of personal data, users must register the new database with the College Data Protection Officer and act in compliance with the Data Protection Principles to ensure that personal data is held and processed securely and the rights of the individual are preserved.