# DATA PROTECTION POLICY

| | |
|---|---|
| Policy Reference Number | **D01** |
| Version | 1 |
| Originator | Chris Hufton |
| Approved | Finance & General Purposes Committee – 11.3.14 |
| Issue Date | 12 March 2014 |
| Review Date | Three yearly / as legislation changes |

## A Introduction

A.1 The College holds personal information about its staff, students, Corporate Board members, suppliers and other people it comes into contact with as a normal part of its day to day business. It is necessary to process personal information so that staff can be recruited and paid, students enrolled, examinations and assessments held, and legal obligations complied with.

A.2 The manner in which personal information is collected, used, stored, disclosed, updated and destroyed is regulated by the Data Protection Act 1998. Other statutory provisions that also affect the College's processing of personal information include the Human Rights Act 1998, the Freedom of Information Act 2000, and the Regulation of Investigatory Powers Act 2000.

A.3 The College will ensure that the interests of its staff and students are safeguarded by complying with all the provisions of these Acts and by reviewing this policy every three years or as required by changes in legislation or guidance issues by the Information Commissioner.

A.4 The Data Protection Act requires the College to notify the Information Commissioner annually about the types of 'personal data' 'processed' by the College and the purposes of such 'processing'. See below for further details of these defined terms.

A.5 The College may in certain circumstances be legally obliged to disclose information to external authorities including the Educational Funding Agency, the Department for Education, the Police, tax inspectors etc. In certain circumstances the College may also be required not to inform the relevant student or member of staff that it is disclosing his/her 'personal data' to such an authority.

## B Outline of Data Protection Law

B.1 The Data Protection Act places duties and obligations on 'Data Controllers' in relation to their 'processing' of 'personal data'.

B.2 Data Controller: the College, as a corporate body, is the Data Controller of all the personal data processed by its staff or otherwise on its behalf and is therefore ultimately responsible for ensuring that such personal data is processed in accordance with the Data Protection Act.

B.3 A Vice-Principal is designated as the College's Information Officer and is responsible for ensuring that the requirements of the Data Protection Act are complied with on a day to day basis and in particular is responsible for:

a) this policy
b) responding to requests for subject access (see below)

c) the annual data protection notification to the Information Commissioner
d) ensuring that the College's procedures are compliant with the Data Protection Act
e) ensuring the College's compliance with the Freedom of Information Act.

B.4 Personal Data as defined and regulated by the Data Protection Act includes information about a living person from which that person can be identified and which contains biographical information (such as date of birth, address, phone number, National Insurance number, exam results) or has that individual as its focus. This can include opinions and decisions made in relation to an individual.

B.5 In addition, to be personal data, the information must either be held in a computer or other digital format including CCTV, or in a manual filing system that is structured and filed in such a way that all the individual's personal details can easily be accessed without having to leaf through or inside files.

B.6 Data Subject is the person to whom the personal data belongs.

B.7 Processing is widely defined to include the obtaining, recording, holding, disclosing, updating, archiving and disposal of personal data.

B.8 The Data Protection Act 1998 sets out eight basic data protection principles that must be complied with when processing personal data. In summary, these principles require that personal data must be:

a) fairly and lawfully processed
b) processed for specified and lawful purposes
c) adequate, relevant and not excessive
d) accurate and (where relevant) kept up to date
e) not kept longer than necessary
f) processed in accordance with the rights of the data subject
g) kept secure
h) not transferred outside the European Economic Area without adequate protection.

B.9 Sensitive Personal Data: certain personal data is defined as sensitive personal data which may only be processed in more restricted circumstances, for example, if there is a legal obligation to do so, or if the data subject has given their express agreement to its processing. Sensitive personal data includes racial or ethnic origin, political opinions, religious beliefs, trade union membership, physical/mental health, sexual life, and criminal record.

## C Notifying data subjects about the personal data processed by the College

C.1 All staff, students and other data subjects are entitled to know:

a) what types of information the College processes about them and why
b) how to gain access to it
c) how to keep it accurate and up to date
d) what the College is doing to comply with its obligations under the 1998 Act.

C.2 Staff personal data is held by Human Resources.

C.3 All students have access to their personal data on Tyber.

## D Responsibilities of staff for data security

D.1 All staff are responsible for ensuring that:

a) any personal data which he/she holds is adequately protected, having regard to the nature of the data and the likely harm that could result from any unauthorised access or corruption of it;
b) personal data is not disclosed to any unauthorised third party without consent or as otherwise permitted under the Data Protection Act. For example, medical data may be released where a failure to do so would result in harm to or death of someone.

D.2 Staff should be aware that those seeking information about individuals may use deception to obtain information and should verify the identity of those seeking information. Further guidance is available in the College's Information Security Policy and associated guidelines.

D.3 Requests by other public bodies, including the Police, must meet the requirements for lawful processing under the Data Protection Act. Third parties must be able to demonstrate that the College is legally entitled and/or legally obliged to make the requested disclosure. For example, the College may be so entitled where the Police require the personal data in pursuit of a criminal investigation and they have reasonable grounds for suspecting that a student or member of staff was involved in a crime. In any event, non-routine requests for access to personal data should always be referred to the Information Officer.

## E Student obligations

E.1 Personal data is collected from students throughout the application and enrolment process. Additional personal data including in relation to courses, progress, examinations and disciplinary matters is recorded throughout their time at the College. The College will only hold such student personal data which is reasonably required to support their progress or well-being at the College or which is required by legislation or for the monitoring of College policies.

E.2 Students are responsible for ensuring that all personal data he/she provides to the College is accurate and up to date, informing the College of any changes to his/her personal data, and checking that the personal data that the College makes available on Tyber is correct.

E.3 Any students requiring clarification of their rights and obligations under the Data Protection Act should contact the Information Officer.

## F Rights to access information

F.1 Staff, students and other data subjects about whom the College processes personal data have the right to access the personal data that is being held about them, subject to a number of exemptions (examples of which are given below). Anyone who wishes to exercise this right must put the request in writing to the Information Officer and pay the appropriate fee as requested by the College (see appendix 1).

F.2 The data subject must supply sufficient information to enable the College to locate the information that is being requested.

F.3 The College may refuse to disclose personal data that makes reference to third parties, that where disclosing the information may prejudice the College's management planning, and/or is a reference written by the College (although the person may be entitled to access this information when he/she has transferred to another organisation.

F.4 The College may make a charge of up to £50 on each occasion that access is requested, and will ensure that access is provided within 40 days (see appendix 1).

## G Processing of personal data

G.1 All personal data processed by or on behalf of the College must only be processed in accordance with the Data Protection Act. Personal data may only be processed if one or more prescribed conditions are satisfied. These include the following:

a) the data subject has given their consent
b) it is necessary in order to carry out a contract to which the data subject is a party
c) the processing is necessary for the College to comply with a legal obligation
d) the processing is necessary for the College to exercise any of its public functions.

G.2 In many cases the College may only process personal data with the consent of the relevant data subject, and where the data is sensitive personal data such consent may need to be explicit. Agreement to the College processing some specified classes of personal data for specific purposes may be a condition of acceptance of a student onto a course, or a condition of employment for staff. For example, it is a condition of employment that a member of staff discloses information about previous criminal convictions.

G.3 The College has a duty to ensure that staff are suitable for the job, and students for the courses offered to them. All prospective staff and students will therefore be asked to give consent to the processing of any personal data submitted by them to the College including via their application form. Where necessary, staff already in post may be asked to give written consent to the processing of their personal data.

## H Processing sensitive information

H.1 Sometimes it is necessary for the College to process sensitive personal data, for example to ensure that the College is a safe place for everyone or to operate College policies such as those relating to sick pay or equal opportunities. Because the processing of this sensitive personal data may cause particular concern or distress to individuals, all staff and students will be asked to give their express consent for this. However, offers of employment or a place at the College may be withdrawn if an individual refuses to give consent without good reason.

H.2 Sensitive personal data will only be handled by specifically designated staff and will only be processed without the consent of the data subject where the College is legally entitled to do so and it is the best interests of the data subject or other individual.

H.3 There are a number of occasions where the College could process sensitive personal data without explicit consent, such as where the processing is necessary:

a) to protect the vital interests of an individual where consent cannot be obtained, ie life and death situation
b) for the purpose of or in connection with any legal proceedings or obtaining legal advice
c) for medical purposes (on certain conditions)
d) for the detection or prevention of any unlawful act.

## J Retention of data

J.1 The College follows the recommendations in the most recent version of the JISC Retention Schedules for Further Education for deciding the length of time for which staff and student personal data should be retained. Also refer to D031 Information Handling Guidelines.

## K Compliance

K.1 Compliance with the Data Protection Act is the responsibility of all members of the College. Any deliberate breach of this policy may lead to disciplinary action being taken. In extreme cases, an individual member of staff may be held liable for criminal offences under the Act.

K.2 Any questions or concerns about the interpretation or operation of this policy should be taken up with the Information Officer:

Martin Sullivan
Vice-Principal
The Sixth Form College, Solihull
Widney Manor Road
Solihull
B91 3WR

Telephone number 0121 704 2581 extension 2716
Email: msullivan@solihullsfc.ac.uk

**Subject access requests**

All staff and students have a right to access their personal data held by the College. Almost all data held about students is visible to them on Tyber; separate student files are no longer held by the College. Staff records are held by the Human Resources Office and staff who therefore wish to see a copy of their personal information need to make a subject access request. This request should be made by email or in writing to the Information Officer or the Human Resources Officer.

Please remember that documentation that makes reference to a third party or references written by College staff do not have to be disclosed and some documentation may only be released after deleting some sections to protect the rights of other individuals.

The College would normally make a charge of £10 for this, but if answering the request involves extensive work (for example, if copies of all emails are requested) then a charge of £50 would be made.

The College aims to comply with requests for access to personal information as quickly as possible and will ensure that it is provided within 40 calendar days unless there is good reason for the delay. In such cases, the reason for the delay will be explained in writing to the member of staff making the request.

Staff who may be unsure of what they require are advised first of all to talk to the Information Officer or the Human Resources Officer.