Data Protection Policy

Anthony McGarel, Deputy Principal and Chief Executive

26th September 2022

EXECUTIVE SUMMARY

Data Protection Policy

South Essex College needs to keep certain information about its employees, students and other users to allow it to monitor performance, achievements, and health and safety, for example. It is also necessary to process information so that staff can be recruited and paid, courses organised and legal obligations to funding bodies and government complied with. To meet our statutory obligations, information must be collected and used fairly, stored safely and not disclosed to others unlawfully. To do this, the College must comply with the Data Protection Principles which are set out in the Data Protection Act and other relevant legislation.

In summary these state that personal data shall be:

- Obtained and processed fairly and lawfully and shall not be processed unless certain conditions are met.
- Obtained for a specified and lawful purpose and shall not be processed in any manner incompatible with that purpose.
- Adequate, relevant and not excessive for those purposes.
- Accurate and kept up to date.
- Not kept for longer than is necessary for that purpose.
- Processed in accordance with the data subject's rights.
- Kept safe from unauthorised access, accidental loss or destruction.

All staff or others who process or use any personal information must ensure that they follow these principles at all times. In order to ensure that this happens, the College has developed its Data Protection Policy.

SIGNIFICANT CHANGES FOLLOWING REVIEW

Policy Review on date

Page Number or Heading Name	Details of significant change	Changes made by
Whole document	Reference to old job titles removed or changed	Craig Willcocks
Whole document	Minor changes to reflect departmental and college wide structural changes	David Hunt
Appendix 1	Changes to approval authorities in line with changes to management committees	David Hunt

Data Protection Policy

Definitions

The legislation uses particular definitions, which are also used in the Data Protection Policy. These are set out below:

Data
Any information which will be or which is being used or "processed" by a computerized system, or which is recorded with the intention that it will be processed in this way will be "data" for the purpose of the Act. In addition, any information kept as part of a "relevant filing system" will be "data". Relevant filing system refers to any paper or other manual filing system which is structured so that information about an individual is readily accessible. This may include personnel records, or student registers or files as well as information collected with the intention that it will be filed in such a system. Data can be written information, photographs, or other information such as voice recordings.

Personal Data
This is information about a living individual, who is identifiable by the information, or who could be identified by the information combined with other data, which the College currently has or may have in the future. For example, application forms marked only with a number will not identify an individual, but put together with the list of numbers and names, will do so. Personal data will include names and addresses, ethnic origin, details about sickness absence, birthdays or marital status.

Sensitive Data
Includes information about a person's religion or creed, gender, trade union membership, political beliefs, sex life or sexuality, health or criminal record.

Processing
Accessing, altering, adding to, changing, disclosing or merging any data will be processing for the purpose of the Data Protection Act.

Status of the Policy

It is a condition of employment that employees will abide by the rules and policies made by the College which may be varied from time to time. It is the responsibility of individual members of staff to ensure that they keep themselves informed of the College's policies and procedures which are published on the College intranet. Any failures to follow the policy may result in disciplinary proceedings.

Any member of staff, who considers that the policy has not been followed in respect of personal data about themselves, should raise the matter with the Director of People & Organisational Development initially.

Notification of Data Held and Processed

All staff, students and other users are entitled to:

- Know what information the College holds and processes about them and why.
- Know how to gain access to it.
- Know how to keep it up to date.
- Know what the College is doing to comply with its obligations under the 1998 Act.

The College will therefore provide all staff and students and other relevant users with a standard form of notification, on written request. This will state the types of data the College holds and processes about them, and the reasons for which it is processed.

Responsibilities of Staff

All staff are responsible for:

- Checking that any information that they provide to the College in connection with their employment is accurate and up to date.
- Informing the College of any changes to information, which they have provided, i.e. changes of address.
- Checking the information that the College will send out from time to time, giving details of information kept and processed about staff.
- Informing the College of any errors or changes. The College cannot be held responsible for any errors unless the staff member has informed the HR Team.

If and when, as part of their responsibilities, staff collects information about other people, (i.e. about students' course work, opinions about ability, references to other academic institutions, or details of personal circumstances), they must comply with the guidelines for staff, which are at Appendix 1.

Data Security

All staff are responsible for ensuring that:

- Any personal data which they hold is kept securely.
- Personal information is not disclosed either orally or in writing or accidentally or otherwise to any unauthorised third party.
- Staff should note that unauthorised disclosure will usually be a disciplinary matter, and may be considered gross misconduct in some cases.

Personal information should be:

- Kept in a locked filing cabinet, or in a locked drawer.
- If it is computerised, be password protected.
- Kept only on disk which is itself kept securely.

Student Obligations

Students must ensure that all personal data provided to the College is accurate and up to date. They must ensure that changes of address, etc. are notified to the Team Administrator/ Registry as appropriate.

Rights to Access Information

Staff, students and other users of the College have the right to access any personal data that is being kept about them either on computer or in certain files. Any person who wishes to exercise this right should make their request in writing to the Head of IT. The College will make a charge of £10 on each occasion that access is requested, although the College has discretion to waive this. The College aims to comply with requests for access to personal information as quickly as possible, but will endeavour to provide the information within 30 days unless there is good reason for the delay. In such cases, the reason for delay will be communicated in writing to the applicant.

N.B. Staff should note the procedure for dealing with subject access requests which is set out at Appendix 2.

Subject Consent

In many cases, the College can only process personal data with the consent of the individual. In some cases, if the data is sensitive, **express consent** must be obtained. Agreement to the College processing some specified classes of personal data is a condition of acceptance of a student onto any course, and a condition of employment for staff. This includes information about previous criminal convictions.

Some jobs or courses will bring the applicants into contact with children, including young people between the ages of 16 and 18. The College has a duty under the Children Act and other enactments to ensure that staff are suitable for the job, and students for the courses offered. The College also has a duty of care to all staff and students and must therefore make sure that employees and those who use the College facilities do not pose a threat or danger to other users.

The College will also ask for information about particular health needs, such as allergies to particular forms of medication, or any conditions such as asthma or diabetes. The College will only use the information in the protection of the health and safety of the individual, but will need consent to process in the event of a medical emergency, for example.

Processing Sensitive Information

Sometimes it is necessary to process information about a person's health, criminal convictions, race and gender and family details. This may be to ensure the College is a safe place for everyone, or to operate other College policies, such as the sick pay policy or equal opportunities policy. Because this information is considered sensitive, and it is recognized that the processing of it may cause particular concern or distress to individuals, staff and students will be asked to give express consent for the College to do this. Offers of employment or course places may be withdrawn if an individual refuses to consent to this, without good reason.

The Data Controller and the Designated Data Controller/s

The College as a body corporate is the data controller under the Act. However, there is a designated data controller who will deal with day to day matters. This is the Head of IT whom any requests or queries should be directed in the first instance.

Student Assessment

Students will be entitled to information about their marks for both coursework and examinations. However, this may take longer than other information to provide. The College may withhold certificates, accreditation or references in the event that the full course fees have not been paid, or all books and equipment returned.

Retention of Data

The College will keep some forms of information for longer than others. Because of storage problems, information about students cannot be kept indefinitely, unless there are specific requests to do so. In general information about students will be kept for 10 years after they leave the College. This will include:

- name and address
- academic achievements, including marks for coursework
- copies of any reference written

The College will need to keep information about staff for longer periods of time. In general, all information will be kept for 5 years after a member of staff leaves. Some information, however, will be kept for much longer. This will include information necessary in respect of pensions, taxation, potential or current disputes or litigation regarding the employment, and information required for job references. A full list of information with retention times is available from the Head of IT.

Conclusion

Compliance with the 1998 Act is the responsibility of all members of the College. Any deliberate breach of the data protection policy may lead to disciplinary action being taken, or access to College facilities being withdrawn, or even a criminal prosecution. Any questions or concerns about the interpretation or operation of this policy should be taken up with the Head of IT.

APPENDIX 1

Staff Guidelines for Data Protection

1. The majority of staff will process data about students on a regular basis, when marking registers, or College work, writing reports or references, or as part of a tutorial or academic supervisory role. The information that staff deal with on a day-to-day basis is likely to include:

- General personal details such as name and address.
- Details about class attendance, course work marks and grades and associated comments.
- Notes of personal supervision, including matters about behaviour and discipline.

2. Information about a student's physical or mental health; sexual life; political or religious views; trade union membership or ethnicity or race is sensitive and can only be collected and processed with the student's consent.
E.g. recording information about dietary needs, for religious or health reasons prior to taking students on a field trip; recording information that a student is pregnant, as part of tutorial duties.

3. All staff have a duty to make sure that they comply with the data protection principles, which are set out in the College Data Protection Policy. In particular, staff must ensure that records are:

- Accurate
- Up-to-date
- Fair
- Kept and disposed of safely, and in accordance with College policy

  The College will designate staff in each area as 'authorised staff'. These staff are the only staff authorised to hold or process sensitive data

We must also take care to ensure that, when data subjects advise us of changes to or errors in the data currently being held by the College, amendments are made as quickly as is reasonably practicable.

4. Authorised staff will be responsible for ensuring that data is kept securely.

5. Staff must not disclose personal data to any student, unless for normal academic or tutorial purposes, without authorisation or agreement from the Head of IT or the Deputy Principal and Chief Executive, or in line with College policy.

6. Staff shall not disclose personal data to any other staff member except with the authorisation or agreement of Head of IT or the Deputy Principal and Chief Executive, or in line with College policy. If in any doubt, members of staff should consult their line manager.

APPENDIX 2

Procedure for dealing with Subject Access Requests

Staff, students and other users of the College have the right to access any personal data that is being kept about them either on computer or in certain files (unless this would involve disproportionate effort on the College's part). This is known as a "subject access request". The College will make a charge of £10 on each occasion that access is requested, although the College has discretion to waive this. The College aims to comply with valid requests for access to personal information as quickly as possible, but will endeavor to provide the information within 30 days unless there is good reason for the delay. In such cases, the reason for delay will be communicated in writing to the applicant. Anyone who wishes to make such a subject access request will need to follow the procedure set out below:

1. Information requests must be in writing and addressed to the Head of IT. Open-ended requests, such as "give me a copy of everything you have on me" will be invalid. Requests must be sufficiently precise to enable the College to locate the right information.

2. Generally, the request will need to be hand-delivered as it is necessary to check the identity of the person making the request before responding to ensure that only those entitled to request the information are asking for it. Normally, identification will be checked by production of a College staff or student ID card. In the case of students, the verification should be undertaken by a member of the Registry staff; and in the case of staff by a member of the Human Resources Team.

3. The member of staff accepting the information request should photocopy the College identification card, sign the photocopy, and ensure that the request is date stamped. The documentation should then be passed without delay to the Head of IT.

SLT Member Responsible	
Author of Procedure	
Date agreed by SLT	
Date Effective From	
Date last amended	
Review Date	