

# Data Protection Code of Practice


## **1 Introduction**

---

- 1.1 This Code of Practice has been approved by the Board of Governors of Sussex Coast College Hastings as part of its commitment to its legal duties and the highest standards of information governance, as expressed in its Information Governance Policy Statement.
- 1.2 The Code applies to the College and its subsidiary companies, including Plaza Trading, hereon known as the 'College'.
- 1.3 The College must comply with the Data Protection Principles which are set out in the Data Protection Act 1998 (the Act). These principles state that personal information shall:
- be obtained and processed fairly and lawfully and shall not be processed unless certain conditions are met;
  - be obtained for a specified and lawful purpose and shall not be processed in any manner incompatible with that purpose;
  - be adequate, relevant and not excessive for those purposes;
  - be accurate and kept up to date;
  - not be kept longer than is necessary for the purpose;
  - be processed in accordance with the data subject's rights under the Act;
  - be kept safe from unauthorised access, accidental loss or destruction;
  - not be transferred to a country outside the European Economic Area, unless that country has adequate levels of protection for personal data.
- 1.4 The College needs to keep certain information about its employees, students and pupils and other persons to allow it to monitor performance, achievements, and health and safety. 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 met. To comply with the law, information must be collected and used fairly, stored safely and not disclosed to any other person unlawfully.
- 1.5 All staff who process any personal information must ensure that they comply with these principles and the provisions within this Code at all times.

## **2 Status of the Code of Practice**

---

- 2.1 This Code of Practice does not form part of the formal contract of employment, but it is a condition of employment that employees will abide by the rules and policies made by the College from time to time. Any failures to follow the Code might, therefore, result in disciplinary proceedings.
- 2.2 Any member of staff, who considers that the Code has not been followed in respect of personal data about themselves, should raise the matter with the designated data

controller initially. If the matter is not resolved it should be raised as a formal grievance.

### **3 Notification of Data Held and Processed**

---

- 3.1 All staff, students, and other College 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.
- 3.2 Parents of children of compulsory school age are entitled to know what information the College holds and processes about their child.

### **4 Responsibilities of Staff**

---

- 4.1 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 the personal data which they have previously provided;
  - checking the information that the College sends out to them advising of the data that is kept and processed about them;
  - informing the College of any errors or changes that the data subject is aware of.
- 4.2 If and when, as part of their responsibilities, staff collect information about other people (e.g. about students' course work, opinions about ability, references to other academic institutions, or details of personal circumstances), they must comply with this Code.

### **5 Data Security**

---

- 5.1 All staff are responsible for ensuring that:
- any personal data (for any parties) which they hold is kept securely;
  - personal information is not disclosed either orally or in writing, accidentally or otherwise, to any unauthorised third party.
- 5.2 Staff should note that unauthorised disclosure will usually be a disciplinary matter and may be considered gross misconduct in some cases.
- 5.3 Personal information should be:
- kept in a locked filing cabinet/locked drawer or other acceptable secured area.
  - if it is computerised, be password protected
  - kept only on media (hard disk, floppy disk, USB stick) which is itself kept securely
  - only held where absolutely necessary and not readily available from existing systems.

### **6 Student Obligations**

---

- 6.1 Students, or parents of children of statutory school age, should ensure that all personal data provided to the College is accurate and up to date. They must ensure, for example, that changes of address are notified to the relevant Administration Office and the College Student Services

## **7 Rights to Access Information**

---

- 7.1 Staff, students and other users of the College have the right to access any personal data that is being held about them either on computer or in certain organised files. Any person who wishes to exercise this right should apply in writing to the relevant Data Controller (see section 12)
- 7.2 Parents of children of statutory school age have the legal right to access personal data that is held about their children. This legal right does not automatically extend to parents of students of College unless the consent of the student has been obtained.
- 7.3 The College will make a charge of £10 on each occasion that access is required, although the College has the discretion to waive this.
- 7.4 The College aims to comply with requests for access to personal information as quickly as possible and will ensure that it complies with the Act unless exceptions apply. In such cases, the reason for any delay will be explained in writing to the data subject making the request.
- 7.5 In processing a request, the identity of the data subject has to be verified before information will be released. No personal data will be disclosed to a third party without the written consent of the data subject, unless the College is legally required to do so.
- 7.6 The College reserves the right to refuse repeated/vexatious requests.

## **8 Publication of Information**

---

- 8.1 Information that is already in the public domain is exempt from the 1998 Act and will usually fall within the remit of the Freedom of Information Act 2000, with details possibly included in the College's Publication Scheme. It is the College's policy to make as much information public as possible.
- 8.2 The College internal phone list will not be a public document.

## **9 Subject Consent**

---

- 9.1 In many cases, the College may 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.
- 9.2 Some jobs or courses will bring the applicants into contact with children, including young people, between the ages of 4 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 has a duty of care to all staff and students and must, therefore, make sure that employees and those who use the College's facilities do not pose a threat or danger to other users.

- 9.3 The College may also ask for information about particular health and/or learning needs, such as allergies to particular forms of medication, dyslexia, or conditions such as asthma or diabetes. The College will only use the information in the protection of the health and safety of the individual, to offer suitable support and in the event of a medical emergency.
- 9.4 All prospective staff and students will be asked to sign their consent to process particular types of information when a conditional offer of employment or a course place is made. A refusal to sign consent may result in the offer being withdrawn.

## **10 Sensitive Data**

---

- 10.1 Any information about a living individual that includes facts, intentions or opinions about any of the following matters is sensitive data for the purposes of The Act:
- Racial or ethnic origin
  - Political opinions
  - Religious beliefs or other beliefs of a similar nature
  - Whether or not someone is a member of a trade union
  - Sexual life
  - Physical or mental health or condition
  - The commission or alleged commission of any offence
  - Any proceedings for any offence committed or alleged to have been committed
- 10.2 The Act introduces a number of restrictions and conditions on data controllers who want to record and process this type of information, including an obligation to obtain the “explicit consent” of the relevant individual before doing so.

## **11 Processing Sensitive Information**

---

- 11.1 Sometimes it is necessary to process information about a person’s health, criminal convictions, race, gender and family details. This may be to ensure that the College is a safe place for everyone or to operate the College’s policies such as the sick pay policy or equal opportunities policy. Because this information is considered sensitive, staff and students will be asked to give explicit consent for the College to process it. Offers of employment or course places may be withdrawn if an individual refuses to consent to this without good reason. All data subjects providing these types of information should be assured that they will be processed in an appropriate manner. Any contravention of this may result in disciplinary proceedings against the individual concerned.

## **12 The Data Controller and the Designated Data Controllers**

---

- 12.1 Under the Act, each separate legal entity within the College will be a data controller in its own right. Thus, Sussex Coast College Hastings and Plaza Trading Ltd are data controllers and are separately responsible for implementation. However, the designated data controllers will deal with day to day matters.

- 12.2 The College's designated data controller is the Head of MIS. The Head of Department will be its designated data controller, in cases where there is no Head the areas SLT member will be the designated data controller.

### **13 Retention of Data**

---

- 13.1 The College will keep some forms of information for longer than others.

#### **Appendix A provides full guidelines on periods of retention of records**

Because of storage problems, information about students cannot be kept indefinitely. In general, the information retained about students will include:

- name and address
- academic achievements, including marks for coursework
- copies of any references written
- enrolment details

- 13.2 All other information, including any information about health, race or disciplinary matters will be destroyed after 7 years.

- 13.3 The College will need to keep information about staff for longer periods of time. In general, all information will be kept for 7 years after a member of staff leaves the College. Some information will need to 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.

### **14 Key Point**

---

- 14.1 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, access to the College's 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 designated data controller.

## APPENDIX

The following is a list of College records to be maintained and retained for the periods stated.

Record	To be Maintained by	Period of Retention	Location of Records
Customer Comments, College Surveys	Quality	5 Years	Archive Room
Financial Records (all records including invoices, receipts as well as copies of ledgers and accounts - electronic and hardcopy)	Finance	7 Years	Archive Room
Minutes of the Board of the Corporation and its committees	Clerk to the Corporation	Historical records never be disposed of	Office/Archive
Agenda, papers and other records of the Board of the Corporation	Clerk to the Corporation	10 Years	Office
Internal and External Audit	Finance	7 Years	Office
Tenders and Time-expired Contracts	Finance	7 Years	Office /Archive Room
Employers Liability Certificate	Finance	20 Years	Office
Data Protection Registration	MIS	10 Years	Office
Student MIS Records (all records - electronic and hardcopy)	MIS	7 Years	Office/Archive
Exam and Assessment Records + correspondence with examination bodies	Exams	5 Years	Office / Archive
Software Licences and Hardware Registers	IT Services	5 Years	Office / Archive
Confidential Student Counselling Records	College Counsellors	2 Years	Office
Internal Quality Audit Files	Quality	5 Years	Office / Archive
Document Control Records			Office / Archive
Staff Professional Development Records and Files	HR	5 Years	Office / Archive
Accident Register	Health & Safety Manager	7 Years	Office
Health and Safety Records (including risk assessment, audits, PAT testing records, tests and inspection records)	Health & Safety Manager	10 Years	Office / Archive
Staff Personal Files	HR	Duration of individual's employment, then archived for 10 years	Office / Archive

Recruitment Files	HR	4 months from the date of decision	Office / Archive
Student Files	Faculty Administrators	5 Years	Office / Archive
Course Files	Course Teams	5 Years	Office / Archive
Student Examination Scripts	Exams	5 Years	Office / Archive
Library Statistics	LRC/Library Manager	5 Years	Office
Staff Timetables	Curriculum Heads	2 Years	Office /Archive
Student Services: - <ul style="list-style-type: none"> <li>• Student Counselling</li> <li>• Advice and Guidance</li> <li>• Bursary/dLSF</li> <li>• Education Maintenance Allowance (EMA)</li> <li>• Access Fund</li> <li>• Childcare</li> </ul>	Head of Student Services	Duration of Student's enrolment with the College, then archived for 3 years	Office /Archive
Payroll Data	HR	Duration of individual's employment, then archived for 10 years	Office /Archive
Line Manager's Staff Files and records relating to staff (e.g. PDR, staff development, file notes)	All Line Managers	Duration of individual's employment, then forwarded to HR for disposal	Office