city college brighton and hove

Data Protection Policy

Policy Review Area	Marketing, Communications and IT
Lead Manager	COO
Originated	December 2008
Last updated	March 2013
Reviewed by Board	December 2015
Next Review	December 2018

1. Introduction

1.1. City College Brighton and Hove, Pelham Street, Brighton, BN1 4FA, (hereafter referred to as "the College") is required to maintain certain data about individuals for the purposes of operational and legal requirements. The College recognises the importance of the correct and lawful treatment of personal data as it maintains confidence in the College and provides for successful operations.

1.2. The type of data the College may require includes information on current, past and future employees, students, sponsors, suppliers and others the College is involved with (hereafter referred to as "Subjects").

1.3. Personal data whether held electronically, on paper or on other media is subject to the Data Protection Act 1998 (DPA).

1.4. Personal data means data relating to a living and identifiable individual. Personal data can be factual (such as name, address or date of birth) or it can be an opinion (such as an appraisal).

1.5. Sensitive personal data can include information about a person's racial or ethnic origin, political opinions, religious or similar beliefs, trade union membership, health condition or any offences, alleged or committed.

2. Principles

2.1. The College endorses and adheres to the eight principles of the DPA. These specify the conditions that must be satisfied in obtaining, handling, processing, transportation and storage of personal data.

2.2. The principles are that personal data is:

2.2.1. to be obtained and processed fairly, lawfully and shall not be processed unless certain conditions in Schedule 2 (see paragraph 2.3) and for sensitive data
in Schedule 3 (see paragraph 2.4) are met;

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

2.2.3. to be adequate, relevant and not excessive for those purposes;

2.2.4. to be accurate and kept up to date;

2.2.5. not to be kept for longer than is necessary for that purpose;

2.2.6. to be processed in accordance with the data subject's rights;

2.2.7. to be kept safe from unauthorised access, accidental loss or destruction;

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

2.3. Schedule 2

Conditions relevant for the purpose of the first Principle: processing of any personal data:

a) With the consent of the data subject
b) To establish or perform a contract with the data subject
c) To comply with a legal obligation
d) To protect the vital interests of the data subject
e) For the exercise of certain functions of a public interest nature
f) For the legitimate interests of the data controller unless outweighed by the interests of the data subject.

2.4. Schedule 3

The following is not a complete list of all conditions relevant for the purpose of the first Principle: processing of any sensitive personal data:

a) With the explicit consent of the data subject
b) To perform any right or obligation under employment law
c) To protect the vital interests of the data subject or another person
d) For the legitimate activities of certain not-for-profit bodies
e) When the data has been made public by the data subject
f) In connection with legal proceedings
g) For the exercise of certain functions of a public interest nature
h) For medical purposes
i) For equal opportunity ethnic monitoring

3. Status of the Policy

3.1. Any breach of this policy will be taken seriously and may result in disciplinary proceedings.

3.2. The policy 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.

3.3. Any Subject who considers that the policy has not been followed in respect of personal data about themselves should raise the matter with the Data Protection Officer (DPO).

4. Designated Data Protection Officer

4.1. The College's DPO is responsible for overseeing compliance with the DPA and implementation of this policy on behalf of the College.

4.2. Any questions or concerns about the policy should, in the first instance, be taken up with the DPO.

5. Responsibilities of Subjects

All subjects are responsible for:

- Checking that any personal data they provide to the College is accurate and kept up to date
- Informing the College of any changes to the information held about them

- for Staff this is the HR Department
- for Students this is the MIS Team
- for Suppliers this is the Finance Department
- For all other notifications contact the DPO

- Checking any information the College may send to them giving details of the information being kept or processed, any errors should be reported to the College

- If their responsibilities involve collecting or processing information about other people they must comply with the Policy and the DPA

6. Subject Access Requests

All individuals who are the subject of personal data held by the College have the right to access their personal data. Any person who wishes to see this data must make the request in writing to the DPO.

7. Data Security

7.1. The need to keep data securely means that precautions must be taken against physical loss or damage and that both access and disclosure must be restricted.

7.2. All College staff are responsible for ensuring that:

- Any personal data which they hold is kept securely; for example records held on a computer must be password protected
- Personal data is not disclosed either orally, in writing or otherwise to any unauthorised party
- Immediately report any loss to the DPO.

8. Publication of College Data

Data already in the public domain is exempt from the DPA.

9. Retention of Data

9.1. The College will keep some types of information for a longer time than others. All staff are responsible for ensuring information is not kept longer than necessary - see Appendix A.

9.2. Any data destruction is performed in a secure manner.

Appendix A – Guidelines for Retention of Personal Data

Note: This is not an exhaustive list. Medical records, for example, are kept for a variety of health and safety reasons and will carry their own retention times.

Type of Data	Suggested Retention Period	Reason
Minutes of the Board of Governors and all committees	Historical records never to be disposed of	
Agenda, papers and other records of the Board of Governors	10 years	
Personnel files included in training records and notes of disciplinary and grievance hearings	6 years from the end of employment	References and potential litigation
Application forms/interview notes	At least 6 months from the date of the interviews	Time limits on litigation
Facts relating to redundancies where less than 20 redundancies	3 years from date of redundancies	Time limits on litigation
Facts relating to redundancies where 20 or more redundancies	12 years from date of redundancies	Time limits on litigation
Income Tax and NI returns, including correspondence with tax office	At least 6 years after the end of the financial year to which the records relate	Income Tax (Employment) Regulations 1993
Statutory Maternity Pay records and calculations	At least 6 years after the end of the financial year to which the records relate	Statutory Maternity Pay (General) Regulations 1986
Statutory Sick Pay records and calculations	At least 6 years after the end of the financial year to which the records relate	Statutory Sick Pay (General) Regulations 1982
Wages and salary records	At least 6 years after the end of the financial year to which the records relate	Taxes Management Act (1970)
Accident books, and records and reports of accidents	6 years after the date of the last entry	RIDDOR 1985
Safeguarding Casework Records	25 years	Legal Requirement

Student records, including academic achievements, and conduct	▪ At least 6 years from the date the student leaves the College, in case of litigation for negligence. ▪ For EU-funded projects records should be kept for 7 years after completion of programme.	Limitation period for negligence