

## Data Protection Policy

### 1. Background

From 25<sup>th</sup> May 2018 the General Data Protection Regulation (GDPR) replaces the previous Data Protection Directive. The advancements in digital technology and the use of the internet have changed the way data is collected and processed. The GDPR provides for more safeguards of personal data and higher fines for noncompliance.

The GDPR relates not only to personal data processed by an automated system but also to manual filing systems where personal information is accessible based on specific criteria. This includes chronologically ordered manual filing systems. This may include personnel records or student registers or files which are indexed or any information collected with the intention that it will be filed in such a system. Data can be written information, photographs, or information such as fingerprints or voice recordings.

The GDPR applies to “personal information”. The GDPR makes a distinction between personal data and “sensitive” personal information (Special Categories Data).

Personal information is defined as data relating to a living individual who can be identified directly or indirectly from that information. It includes names and addresses, identification number, location data, online identifier, features such as hair and eye colour which may be in the form of photographs, ethnic origin, qualifications and experience, details about sick leave and holidays taken, birthdays and marital status. Any opinion about, or intentions regarding, a person that are recorded will also be personal information-

**Sensitive** personal information (Special Categories Data) is defined as personal data consisting of information as to:

- Race
- Ethnic origin
- Political opinion
- Religious or other beliefs
- Trade union membership
- Physical or mental health or condition
- Sexual life
- Criminal proceedings or convictions
- Health data
- Genetic and Biometric data where used for ID purposes

### 2. Introduction

The 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 comply with the law, information must be collected and used fairly, stored safely and not disclosed to

any other person unlawfully. To do this, the College must comply with the General Data Protection Regulation.

Personal data shall be:

1. Processed lawfully, fairly and in a transparent manner in relation to individuals
2. Collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be considered to be incompatible with the initial purposes
3. Adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed
4. Accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data which is inaccurate, having regard to the purposes for which it is processed, is erased or rectified without delay
5. Kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data is processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes subject to implementation of the appropriate technical and organisational measures required by the GDPR in order to safeguard the rights and freedoms of individuals
6. Processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures

The Controller shall be responsible for and be able to demonstrate compliance with the General Data Protection Regulation.

Personal information may only be transferred to non EU countries that have adequate level of protection of personal data, in compliance with the conditions for transfer set out in Chapter V of the GDPR.

The College and its 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 this Data Protection Policy.

### 3. Status of the Policy

This 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 from time to time. Any failures to follow the policy can therefore result in disciplinary proceedings.

Any member of staff who considers that the policy has not been followed in respect of personal information 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.

#### 4. 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;
- How to gain access to it;
- How to keep it up to date;
- What the College is doing to comply with its obligations under the General data Protection Regulation (GDPR)

The College will therefore provide all staff and students and other relevant users with the standard form of notification. This will state all the types of data the College holds and processes about them, and the reasons for which it is processed. The College will try to do this at least once every year.

#### 5. 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, e.g. change of address;
- Checking the information that the College will send out from time to time giving details of the information kept and processed about themselves;
- Informing the College of any errors or changes. The College cannot be held responsible for any errors unless the staff member has informed the College in writing.

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 educational establishments, details of personal circumstances), they must comply with the guidelines for staff which are in Appendix 1.

#### 6. Data Security

All staff are responsible for ensuring that:

- Any personal information which they hold is kept securely;
- Personal information is not disclosed either orally or in writing or by electronic transfer 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; or
- If it is computerised, be password protected;

Staff should ensure that they complete the training on Data Protection and keep up to date with information security guidelines provided by the College

#### 7. Student Obligations

Students must ensure that all personal information provided to the College is accurate and up to date. They must ensure that changes of address etc. are notified to their personal tutor or Customer Services.

Students who use the College computer facilities may, from time to time, process personal data. If they do so they must notify the data controller. Any student who requires further clarification about this should consult their personal or subject tutor.

#### 8. Rights to Access Information

Staff, students and other users of the College have the right to access any personal information that is being kept about them either in a computer system or a manual filing system. Any person who wishes to exercise this right can do so verbally or in writing. You can complete the College "Access to Information" form attached and give it to Customer Services/Personal Tutor/Human Resources. The data subject making such a request will be required to produce proof of their identity.

The College reserves the right not to respond to a personal information request or to charge a reasonable fee for the administrative costs of complying with the request if it considers this to be unfounded or excessive. If a request is refused the College will explain to the individual the reason and of the right to complain to the Information Commissioner's Office. The College will respond without undue delay and at the latest within a month.

The College will aim to comply with requests for access to personal information as quickly as possible and will ensure that it is provided within one month of receipt of the request unless there is good reason for delay for example multiple or complex requests. In such cases the reason for delay will be explained in writing to the data subject making the request. This will take place within one month of the receipt of the request.

*The statutory time-span set for access to personal information is one month.*

#### 9. Publication of College Information

Information that is already in the public domain is exempt from the GDPR. It is the College policy to make such information as public as possible and, in particular, the following information will be available to the public for inspection:

\*Names of the College Corporation Members and Register of Interests of those members

\*Non confidential minutes and papers of full Corporation meetings

#### 10. Processing Sensitive Information (Special Category data) and Criminal Convictions

Sometimes it is necessary to process information about a person's health, race and gender, family details, criminal convictions. This may be to ensure that the College is a safe place for everyone, or to operate other College policies, such as the Equalities Policy.

#### 11. Examination Marks

Students will be entitled to information about their marks for both coursework and examinations.

## 12. Retention of Data

The College recognises that the efficient management of its records is necessary to support the College's core functions and to comply with its legal and regulatory obligations. (See Records Management Policy: Records Retention Guidelines).

## 13. Conclusion

Compliance with the General Data Protection Regulation (GDPR) is the responsibility of all members of the College. Any deliberate breach of the data protection policy will 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 designated College Data Controller.

Designated College Data Controller: *Director of Employer Partnership*

## APPENDIX 1

### Staff Guidelines for Data Protection

1. College staff will process information about students on a regular basis, when marking registers or College work, writing reports or references, or as part of a pastoral or academic supervisory role. The College will ensure, through registration procedures, and privacy notices that all students are informed and notified of the categories of processing, as required by the GDPR. The information that staff deal with on a day-to-day basis will be “standard” and will cover categories such as:
  - General personal details such as name and address;
  - Details about class attendance, course work marks and grades;
  - Notes of personal supervision, including matters about behaviour 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 restricted to those staff that have a need to know.
3. All staff have a duty to make sure that they comply with the GDPR principles which are set out in the College’s 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
4. The College will designate staff as “authorised staff”. These are the only staff authorised to hold or process data that is:

Not standard data or  
Sensitive data

The only exception to this will be if a non-authorised staff member is satisfied that the processing of the data is necessary and:

- in the best interests of the student or staff member, or a third party, or the College AND
- he or she has either informed the authorised person of this, or has been unable to do so and processing is urgent and necessary in all the circumstances

This should only happen in very limited circumstances.

5. Authorised staff will be responsible for ensuring that all information is kept securely.
6. Staff must not disclose personal information to any student, unless for normal academic or pastoral purposes, without authorisation or agreement or in line with College policy.
7. Staff should not disclose personal information to any other staff member except with authorisation or in line with College policy.

8. Before processing any personal information, all staff should consider the checklist:

#### Staff Checklist for Recording Information

- Do you really need to record the information?
- Is the information “standard” or is it “sensitive”?
- If it is “sensitive”, record why and any special handling conditions?
- Has the student been told that this type of information will be processed?
- Are you authorised to collect/store/process the data?
- If yes, have you checked with the individual that the data is accurate?
- Are you sure that the information is secure?
- Are you satisfied that it is in the best interests of the student or the staff member to collect and retain the information?
- Have you reported the fact of information collection to the authorised person within the required time?
- Read and the Data Access Policy

APPENDIX 2

Standard Request form for access to Information

I, (insert name), wish to have access to either (delete as appropriate):

1. All the information that the College currently has about me, either as part of an automated system, or part of a relevant filing system, or
2. Information that the College has about me in the following categories (please tick):
  - Academic marks or course work details
  - Academic or employment references
  - Disciplinary records
  - Health and Medical matters
  - Political, religious or trade union information
  - Any statements of opinion about my abilities or performance
  - Personal details including name, address, date of birth etc
  - Other information, please list below:

---

---

Signed:

Date: