DATA PROTECTION POLICY 2022/23

AUTHORS: Sharon Bowker, Executive Director, Finance & Funding
Naomi Korn Associates

DATE: June 2022

VERSION 1

Data Protection Policy

1 PURPOSE OF THIS POLICY

The objective of this policy is to ensure that:

- all data processing carried out by the College complies with data protection legislation and is in line with the data protection principles
- all members of staff are familiar with their obligations under the General Data Protection Regulation (GDPR) and associated data protection laws

This policy also signposts the procedures in place to support implementing this policy

2 LEGISLATION

The College is subject to the following laws in regard to this data:

- The **UK General Data Protection Regulation (UK GDPR)** - sets out the data protection principles and legal basis for processing, the rights of data subjects, the obligations of data controllers and processors, international transfers, and enforcement
- The **Data Protection Act 2018 (DPA 2018)** - sets out the data protection framework for UK data protection law, defining exemptions and the powers of Information Commissioner's Office (ICO), the UK's regulator for data protection and freedom of information law
- The **Privacy and Electronic Communications (PECR)** - These regulations provide a range of rules around electronic communications. The College will most commonly follow these for direct marketing by email, telephone campaigns and the use of cookies on our websites and emails

The College is registered with the Information Commissioner's Office as a 'data controller', registration number Z6455437. The College is listed as a public authority in Schedule 1 of the Freedom of Information Act 2000 and therefore is defined as a public authority in the UK GDPR and DPA 2018. Breaching the UK's privacy laws can result in enforcement action, including monetary penalties.

3 DEFINITIONS

The following terminology is used in the legislation:

Personal Data

Data which relates to an identifiable living individual, which is being processed automatically or recorded as part of a relevant, filing system.

Special Category Data

Personal data relating to racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation.

Criminal Convictions Data

Personal data relating to criminal convictions and offences or related security measures.

Data Controller

A person or organisation who (either alone or jointly or in common with other persons) determines the purposes for which and the manner in which any personal data are, or are to be, processed.

Data Subject

An individual who is the subject of personal data.

Data Processor

A person or organisation who processes data on behalf of the Data Controller and according to their instructions.

Processing

Obtaining, accessing, altering, adding to, deleting, changing, disclosing or merging data and any other action that can be carried out with data.

4 SCOPE

This policy applies to:

- all employees at the College
- all contractors and suppliers in the services they carry out for the College
- all external projects managed by the College's External Funding Unit, including European Social Funded training programmes

5 RESPONSIBILITIES

The Data Protection Officer ("DPO")

- informs and advises the College and its employees about their obligations to comply with the GDPR and other data protection laws
- reports to the Senior Leadership Team (SLT), College Management Team (CMT) and Finance and Resource Committee on data protection compliance
- monitors compliance with the GDPR and other data protection laws
- manages internal data protection activities
- advises on data protection impact assessments (DPIAs)
- trains staff and conducts internal audits
- they are the first point of contact for supervisory authorities and for data subjects

College Governors and Finance & Resources Committee

- approve this policy and review at regular intervals
- monitor compliance with this policy through reviewing regular reports
- ensure that the Data Protection Officer has appropriate resources and authority to carry out their function

Departmental 'Data Champions'

- act as point of contact between departments and DPO
- raise awareness and promote best practice around data protection in their departments

All Staff

- responsible for processing personal data securely and in line with this policy and associated procedures.
- ensure they have undertaken their mandatory data protection training
- aware that misuse of data by a member of staff can result in disciplinary action and a possible criminal record

The College's third-party suppliers or contractors

- processing personal data on our behalf in a secure and lawful manner
- follow our contractual instructions in regard to the processing of personal data
- ensure they and their staff are appropriately trained in data protection law and associated procedures

6 DATA PROTECTION PRINCIPLES

The seven data protection principles are set out in the UK GDPR:

Lawfulness, fairness, and transparency - The College explains to its student, staff, and other data subjects how it processes their personal data at the point of collection, what the legal basis is for processing and for what purposes the data will be used. In circumstances where the data is not sourced from the individual, information is made available which explains how the data is used.

Purpose limitation - The College only uses the personal data it has for the purposes it was collected for unless certain safeguards around re-use apply.

Data Minimisation - The College only collects personal data which is relevant to the purposes for which it is collected.

Accuracy - The College ensures that personal data is correct, up to date and it is able to be rectify any mistakes quickly.

Storage Limitation - The College does not retain personal data for longer than it is needed unless certain safeguards around long term or permanent storage apply.

Integrity and Confidentiality - The College protects their personal data against unauthorised access, loss, or destruction by a range of security measures.

Accountability - The College will be responsible for its data processing and be able to demonstrate compliance with the other data protection principles.

7 LEGAL BASIS FOR PROCESSING DATA

The College is required to have a legal basis in place for processing personal data.

The available legal bases are as follows, with some illustrative examples for the college:

Legal basis	Example for the college
Data subject has given their consent	A prospective applicant has signed up to the College mailing list to hear about courses and events
Data subject is party to a contract with the College	A member of staff is employed by the College and their details are stored in their personnel file
The College has a legal obligation to process the data	The College is required to provide progression data to ESF
The data subject's vital interests are at stake, and they cannot give consent	A student has a medical emergency at the College and relevant details are provided to emergency services
The data processing is part of the College's function as an education provider	The College records the marks and assessment data for its students
The data processing meets a legitimate interest for the College or another party	The College uses its meeting and events records to create aggregated statistics to monitor outcomes and plan new projects

The processing of Special Category Data requires an additional legal basis under GDPR and a substantial public interest condition from the Data Protection Act 2018. The processing of Criminal Convictions data requires a substantial public interest condition from the Data Protection Act 2018. In most cases the processing of this type of data will be related to a legal obligation around health and safety, equality or employment law.

The legal bases for each type of processing the College carries out will be recorded in the College's Record of Processing Activities (ROPA – please see the 'Record keeping' section below) and communicated to data subjects in the College's Privacy Notice (see the 'Privacy and transparency' section below).

8 RIGHTS

The College will ensure that staff, students and other data subjects are aware of their rights in regard to their data and have in place processes to deal with rights requests in a timely and compliant manner.

Procedural document: Data Rights Request Procedure

9 PERSONAL DATA BREACHES

The College will ensure it has an agreed procedure for identifying and managing personal data breaches, in line with UK GDPR Article 33 (notification of a breaches to the Information Commissioner's Office) and 34 (notification of breach to data subjects).

Procedural document: Data breach procedure

10 DATA PROTECTION BY DESIGN

The College will ensure that it ensures all new projects are implemented with the data protection principles embedded from the start. All new projects involving personal data will require a Data Protection Impact Assessment (DPIA) to be carried out.

Procedural document: Data Protection Impact Assessment (DPIA)

11 RECORD KEEPING

The College will ensure it documents its processing activities in accordance with GDPR Article 30, listing the data it collects, the categories of data subjects and the legal basis for processing. The Record of Processing Activities (ROPA) will be maintained by the College's Data Protection Officer.

Procedural document: Record of Processing Activities (ROPA)

12 DATA PROCESSORS

The College will appoint data processors to process personal data on its behalf and according to its instructions. All data processors will be appointed under the terms of a written contract including commitments to process personal data in line with the responsibilities of processors set out in GDPR Article 28. Data processors will be listed in the Record of Processing Activities (ROPA).

Procedural document: Template data processor clauses / checklist

13 INFORMATION SHARING

Where the College is required to routinely share personal data with another agency in government (local or central), education or health, it will ensure that a suitable information sharing agreement is in place to determine the fair and lawful sharing of personal data.

Ad hoc sharing with the police or other third parties will be carried out within the legal framework of the exemptions in the Data Protection Act 2018. Any instances of this type of sharing will need the required documentation from the requestor and be logged with the Data Protection Officer.

Procedural document: Data Sharing Agreement template / Police data sharing checklist

14 SECURITY

The College will ensure the integrity and confidentiality of its personal data by ensuring appropriate technical measures, in both physical and digital format, are in place. This will include cyber security, policies and procedures and staff training.

Procedural document: Security Advice / Staff training programme / IT Security policies

15 PRIVACY AND TRANSPARENCY

The College will ensure a comprehensive privacy notice is available to all data subjects, describing the purposes for processing, the College's legal basis to do and all information required by GDPR articles 12 to 14.

Procedural document: College Privacy Notice

16 INTERNATIONAL DATA TRANSFERS

If the College or one of its data processors transfer data outside the UK or EEA, then one of the following arrangements will be in place:

- The transfer will be to a country with an "adequacy finding" by the UK or EU
- The transfer will be covered by an appropriate safeguard, such as the International Data Transfer Agreement (ITDA) or the Standard Contractual Clauses (SCC)
- In exceptional circumstances, the transfer may be covered by a derogation in the UK GDPR or an exemption in the Data Protection Act 2018

17 FREEDOM OF INFORMATION ACT 2000 (FOIA)

The College is a public authority and will receive Freedom of Information Act (FOIA) requests. The College will not disclose personal data in FOIA requests if to do so would breach the data protection principles. In some cases, it may not breach the principles (an example would be senior management team professional email addresses) and the College will disclose personal data to comply with the obligations of FOIA.

Procedural document: Freedom of Information Policy

18 STUDENTS AND PARENTS / GUARDIANS

The College's default arrangement for all enrolled students is that they will keep the listed parent(s) or guardian(s) informed where required of the progress of their child for the duration of their studies. When students reach eighteen years of age, they have the option of withdrawing from that arrangement by filling in the 'Withdrawal of consent form'. Parents and guardians will be notified of this decision.

Procedural document: Withdrawal of consent form and template notification letters

19 REVIEW

Changes made: new draft policy as a product of Naomi Korn Associates Data Protection Health Check, April 2022

Review date	Approved by	Approval	Final approval	Next review date	Review period
August 2019	HR Business Partner	Head of HR and Organisational Development		August 2022	3 years
February 2020	HR Business Partner	Head of HR and Organisational Development	Audit Committee	February 2023	
July 2020	HR Business Partner			February 2023	
April 2022	Head of HR and Organisational Development	Executive Director Finance & Funding	Finance and Resources Committee	April 2025	

Prepared by	Authorised by	Date	Review Date
HR Business Partner	Head of HR and Organisational Development	August 2019	August 2021
Senior Data Protection Advisor, Naomi Korn Associates for the DPO		April 2022	

Equalities Impact Assessment

Prepared by	Date	Final / Approved assessment conducted by	Date
HR Business Partner	August 2018	Head of HR and Organisational Development	August 2018

Publication

Audience	Published
Staff	Staff intranet
	College website