Huddersfield New College Further Education Corporation

Data Protection Policy

1.0 Policy Statement

This Policy forms part of a suite of policies and procedures that support data, information and security and meet the regulations within the Data Protection Act 2018 (DPA 2018), and the General Data Protection Regulation (GDPR) as it applies in the UK.

The College needs to hold and to process large amounts of personal data about its students, employees, applicants, governors, alumni, contractors and other individuals in order to carry out its business and organisational functions.

Data protection law defines personal data as any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

2.0 Objectives

Compliance with legislation will be achieved through the implementation of controls and responsibilities including measures to ensure that:

a) Personal data is processed lawfully, fairly and transparently. This includes the provision of appropriate information to individuals upon collection of their data by the College in the form of privacy or data collection notices. The College must also have a legal basis to process personal data

b) Personal data is processed only for the purposes for which it was collected

c) Personal data is adequate, relevant and not excessive for the purposes for which it was collected

d) Personal data is accurate and where necessary kept up to date

e) Personal data is not kept for longer than necessary

f) Personal data is processed in accordance with integrity and confidentiality principles; this includes physical and organisational measures to ensure that personal data, both manual and digital, are subject to an appropriate level of security when stored, used and communicated by the College, in order to protect against unlawful or malicious processing and accidental loss, destruction or damage. It also includes measures to ensure that personal data transferred to or otherwise shared with third parties have appropriate contractual provisions applied

g) Personal data is processed in accordance with the rights of individuals, where applicable. These rights are:
   - the right to be informed;
   - the right of access to the information held about them by the College (through a subject access request);
   - the right to rectification;
   - the right to erase;
   - the right to restrict processing;
   - the right to data portability;
   - the right to object; and
   - rights in relation to automated decision making and profiling

h) The design and implementation of College systems and processes must make provision for the security and privacy of personal data

i) Personal data will not be transferred outside of the European Economic Area (EEA) without the appropriate safeguards in place

j) Additional conditions and safeguards must be applied to ensure that more sensitive personal data (defined as Special Category data in the legislation), is handled appropriately by the College. Special category personal data is personal data relating to an individual's:
   - race or ethnic origin
   - political opinions
   - religious or philosophical beliefs
   - trade union membership
   - genetic data
   - biometric data (where used for identification purposes)
   - health
   - sex life or sexual orientation

   In addition, similar extra conditions and safeguards also apply to the processing of the personal data relating to criminal convictions and offences.

3.0 Scope

This Policy applies to:

a) Personal data held and processed by the College. This includes expressions of opinion about the individual and of the intentions of the College in respect of that individual. It includes data held in any system or format, whether electronic or manual
b) Members of staff, as well as individuals conducting work at or for the College, who have access to College information. This includes governors, temporary, honorary, visiting, casual, voluntary and agency workers, students employed by the College and suppliers (this list is not intended to be exhaustive)
c) Locations from which personal data is accessed including off-campus

4.0 Responsibilities

All staff and other approved users of College systems must:

a) Complete data protection training every two years, and must seek advice and guidance from the Data Protection Officer if clarification is required
b) Immediately report to the Data Protection Officer any actual or suspected misuse, unauthorised disclosure or exposure of personal data, "near misses" or working practices which jeopardise the security of personal data held by the College

All leaders within the College are responsible for ensuring that personal data within their areas is processed in line with this Policy and established procedures.

The Data Protection Officer is responsible for providing procedures, guidance and advice in support of this policy and for training staff.

The Data Protection Officer is responsible for overseeing the College's compliance with the data protection legislation.

Staff must note that any breach of this Policy may be treated as misconduct under the College's relevant disciplinary procedures and could lead to disciplinary action or sanctions. Serious breaches of this Policy may constitute gross misconduct and lead to summary dismissal or termination of contract.

5.0 Monitoring compliance

This Policy and its implementation are subject to internal monitoring and auditing throughout the College, and the outcomes from these processes will inform and improve practices as part of a commitment to continual improvement. The College will also undertake appropriate benchmarking and may be audited by external bodies.

6.0 Linked Policies, Procedures and Frameworks

- Anti-fraud, Bribery and Corruption Policy
- Anti-fraud, Bribery and Corruption Response Plan
- IT Security Framework
    - IT Disaster Recovery Plan
    - IT Business Continuity Plan
    - Third Party Network Connection agreement
    - Inventory-Asset Recording Procedure
    - Software Requests and License Management procedures
    - IT Acceptable and Safe Usage Policy
    - IT Security Incident Procedure
    - Change Control Procedure
    - Patch Management Procedure
    - Systems and Network Security Procedure
    - Account management Procedures
    - Password Management Procedure
    - Archiving Procedure
    - Data Protection Impact Assessment

7.0 Review of Policy

The Data Protection Officer will review the policy every two years or if legislation is changed or published. The Senior Leadership Team will approve the policy.

v	Date	Policy Owner	Comments	Approval Route/ Date	Provenance	Date of Next Review
1.	January 2011	Julie France	Update			
2.	March 2016	Julie Pryce	Full re-write	SLT March 2016	Fundamental revision to include legal requirements	March 2018
3.	May 2018	Julie Pryce	Full re-write	SLT May 2018 (AWS)	Fundamental revision to include new General Data Protection Regulations	May 2020