HNC Policies, Protocols and Procedures

Data Protection Policy

1. 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 UK General Data Protection Regulation (UK GDPR)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.

HNC is the Data Controller for all personal data held in College systems and is responsible for checking the security credentials for third party data processers.

2. Objectives

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

2.1. 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

2.2. Personal data is processed only for the purposes for which it was collected (specified explicit purposes)

2.3. Personal data is adequate, relevant and limited to only what is necessary

2.4. Personal data is accurate and where necessary kept up to date

2.5. Personal data is not kept for longer than necessary

2.6. 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 is handled in a way that ensures appropriate security, including protection against unlawful or unauthorised processing, access, loss, destruction or damage

2.7. Personal data is processed in accordance with the rights of individuals, where applicable. These rights are:

- The right to be informed and how your data is being used

- 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 or stop processing
- The right to data portability
- The right to object
- Rights in relation to automated decision making and profiling

2.8. The design and implementation of College systems and processes must make provision for the security and privacy of personal data. Data Protection Impact Assessments will also be carried out when new systems and processes are introduced and will be reviewed and approved by the College's Data Protection and Security Group.

2.9. Personal data will not be transferred outside of the European Union (EU) without the appropriate safeguards in place.

2.10. 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. Scope

This policy applies to:

3.1. 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.

3.2. 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).

3.3. Locations from which personal data is accessed including off-campus.

4. Responsibilities

4.1. All users of Colllege information must:
- Complete data protection training every year (or based on legislative changes), and must seek advice and guidance from the Data Protection Officer if clarification is required
- Immediately report to the Data Protection Officer any actual or suspected misuse, unauthorised disclosure or exposure of personal data, "near misses" or working practice which jeopardise the security of personal data held by the College

4.2. All staff within the College are responsible for ensuring that personal data within their areas is processed in line with this Policy (and other associated policies namely the IT Acceptable and Safe Use Policy and Subject Access Request Policy) and established procedures (including but not limited to HNC's Secure Data Transmission Procedures).

4.3. All staff are responsible for ensuring that:

- Any personal data which they hold is kept securely. Personal information should be kept in a locked filing cabinet; or in a locked drawer; or if it is computerised, be password protected.
- Personal information is not disclosed either orally or in writing or accidentally or otherwise to any unauthorised third party.
- Any data protection breach they have caused, must be reported immediately to the Data Protection Officer which will be investigated in line with the college's Handling Data Breach procedure.
- The good practice guide for data protection and security and secure data transmission procedures are adhered to.

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

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

4.6. In addition, the Data Protection Officer will:

- Be visible and contactable by staff, governors, and students.
- Have direct access to the Corporation.
- Be advised of any data breaches or relevant disclosure.
- Report breaches and information disclosure to the Information Commissioners Office.
- Provide staff training.

4.7. Staff (and Governors) must note that any breach of this Policy may be treated as misconduct under the College's (and Corporation'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. 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. Review, publication and communication

The Senior Leadership Team approve this policy on recommendation from the Data Protection and Security Group and it is reviewed biennially. Once approved by SLT, staff and governors will be notified of the new policy via Teams and the policy will be published on the internal information platform (Moodle) and the external website.

Version	Date	Author(s)	Comments	Approval Route/ Date	Date of Next Review
1	January 2011	Julie France	New policy	SLT 2015	
2	March 2016	Julie Pryce	Fundamental revision to include legal requirements of the FoI Act 2000	SLT March 2016	March 2018
3	May 2018	Julie Pryce (DPO)	Revision to include new General Data Protection Regulations	SLT May 2018 (AWS)	May 2021
4	May 2021	Julie Thomas (DPO)	Revision to include updates to legislation and internal processes/procedures. Also moved to biennial review	SLT – 15th June 2021	May 2023
5	June 2023	Claire Coupland (DPO)	Revision to include updates to internal processes/procedures.	Data Protection & Security Team 07.06.23 SLT 26.06.23	June 2025