Data Protection Policy

Document Control	
Manager Responsible	Dave Robinson IT & Digital Resources Manager
Version Number	1.0
Approved By	Corporation
Approval Date	December 2021
Review Date	December 2024

*This policy replaces previous policies following new document standardization introduced in 2019

Accessibility Statement
If you have any learning difficulty, disability or health problem, that means you are unable to use the admissions policy and procedure in the way laid out in this document, or you may require additional support to help you with the process, please contact the college to discuss how the process can be adjusted to support your needs. Should you require this guide in an alternative format please contact the college.

Data Protection Policy

1 Introduction

1.1 Hereford College of Arts ('the College') collects, stores and processes the personal data of living individuals such as its staff, students, contractors and customers in order to carry out its functions. This processing is regulated by the General Data Protection Regulation 2016 and Data Protection Act 2018 ('data protection law').

1.2 Personal data can be defined as any information relating to an identified or identifiable person who can be identified – directly or indirectly – by reference to an identifier such as name, an identification number, location data or online identifier.

1.3 The purpose of this Policy is to provide detailed information and advice to ensure compliance with data protection law.

1.4 The policy covers all College activities and processes in which personal data is used, whether in electronic or manual form, and provides a framework for its staff, students and other stakeholders to work within to ensure compliance.

1.5 This policy forms part of College's commitment to the compliant processing of personal data.

2 Scope

2.1 This Policy applies to all staff and students when processing personal data on behalf of College. 'Staff' includes any individual conducting work at or for College and/or its subsidiaries. This includes, but is not limited to, temporary, honorary, visiting, casual, voluntary, and agency workers, students employed by College and its suppliers.

2.2 This policy applies to all personal data processed by College in whatever form. This is not restricted by location or method of access.

3 Accountable Roles

3.1 As a Data Controller, the College has the overall responsibility to comply with data protection law and to be able to demonstrate this.

3.2 The Data Protection Officer (DPO) has primary responsibility for overseeing data protection compliance matters relating to the College. This means:

- 3.2.1 Informing and advising the College of its obligations under data protection law.
- 3.2.2 Monitoring compliance with the regulations and related policies, including raising of awareness and training of staff.
- 3.2.3 Providing procedures, guidance and advice in support of this policy e.g. for Data Protection Impact Assessments (DPIAs).
- 3.2.4 Acting as College's first point of contact with the Information Commissioner's Office (ICO).
- 3.2.5 Handling subject access requests and official requests for personal data from third parties.
- 3.2.6 Investigating losses and unauthorised disclosures of personal data.

3.3 The responsibilities of Information Asset Owners (IAO) and Information

Custodians (IC) are laid out in the Information Management Policy.

3.4 Heads of Department are responsible for ensuring their staff understand the data protection principles and for ensuring compliance. They are required to ensure IAO's are designated for their Departments and provided with appropriate training and support.

3.5 All staff (as defined under the scope of this Policy) and students are responsible for:

3.5.1 Following this Policy and the implementation guidance.

3.5.2 Ensuring the processing of personal data in all formats is compatible with the data protection law principles.

3.5.3 Raising any concerns in respect of the processing of personal data with the DPO.

3.5.4 Promptly passing on to the DPO any individual requests made under the 'rights of the data subject' as set out in data protection legislation, including Subject Access Requests (SAR) and authorised access requests from third parties for personal data (e.g. Police).

3.5.5 Responding promptly to requests from the DPO. (or any delegated authority)

3.5.6 Reporting data security incidents, losses, near misses or unauthorised disclosures of personal data immediately to the Information Security Group isg@ucl.ac.uk and cooperating fully and promptly with the Incident Management Group (IMG) after the incident.

3.5.7 Successfully completing the College's online IT training, including any refresher training.

3.5.8 Completing DPIA's where necessary.

3.6 Where staff are sharing and processing personal data with other organisations they must ensure appropriate data sharing and processing agreements are in place.

3.7 Students process personal data in several ways in the course of their study, such as carrying out research and communicating with staff and fellow students. The College is the controller of personal data when it is processed as part of a student's programme of studies while at the College.

3.8 All students shall successfully complete the required online IT training and IT Induction before processing personal data for the purposes of their study.

4 Policy statements

4.1 The College is committed to complying with the data protection principles. These state that personal data shall be:

4.1.1 Processed lawfully, fairly and in a transparent manner in relation to the data subject. ('lawfulness, fairness and transparency')

4.1.2 Collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes. ('purpose limitation')

4.1.3 Adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed. ('data minimisation')

4.1.4 Accurate and, where necessary, kept up to date. ('accuracy')

4.1.5 Kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed. ('storage limitation')

4.1.6 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. ('integrity and confidentiality')

4.1.7 Processed in such a way that College shall be responsible for and able to demonstrate compliance with the above six principles ('accountability').

4.2 The College shall ensure that data protection is incorporated into systems and processes from the outset, referred to as 'data protection by design and default'.

4.3 The College shall only transfer personal data outside of the European Economic Area where there is adequate protections in place.

4.4 Any incident or near miss that threatens the security of personal data shall be reported to the ISG immediately or as soon as it is known.

4.5 The College shall adhere to the Privacy and Electronic Communications Regulations (PECR) when engaging in direct marketing activity.

4.6 The College shall embed Data Protection Impact Assessment (DPIA) completion as a key part of process and activity planning.

4.7 The College shall uphold the rights of individuals as defined by data protection law.

4.8 The sharing and processing of personal data with other organisations shall be governed by explicit sharing and processing agreements where necessary.

4.9 The College shall maintain a Record of Processing Activities as required by the Information Commissioner's Office.

4.10 The College shall respond to all official third-party requests for personal data following data protection legislation.

4.11 The College shall ensure that all personal information it owns has a designated Information Asset Owner and Information Custodian at all times. The College shall ensure timely transfer of these roles whenever necessary. (e.g. when staff leave).

4.12 When a member of staff is ceasing employment or a student contract expires they shall not retain any College owned personal data unless by an explicit written transfer agreement consistent with the data protection principles.

5 Breaches of Policy

5.1 It is a condition of employment that employees abide by the Regulations and Policies made by College.

5.2 It is a condition of the student contract that students abide by the Regulations and Policies made by College.

5.3 Any breach of this these Policies is considered a serious matter and may result in College taking disciplinary action.

6 Complaints

6.1 Any individual has the right to lodge a complain about how an organisation is handling personal data. The Information Commissioners Office is the UK's independent body set up to uphold information rights and has published guidance on how to make a complaint.

7 Summary

4.1 Hereford College of Arts is committed to providing a safe and managed environment for students, staff and visitors to any part of the campus, by embedding this Policy and ensuring the College complies with all aspects of relevant Regulation and Law any residual risks in relation to data protection law and the College's handling of personal data should be extremely small.

4.2 Everyone working across the campus has a responsibility to follow all guidance as detailed in this Policy, should any person require clarification, guidance or advice then they should contact the Data Protection Officer.