Data Protection Policy

1 Purpose

The EU General Data Protection Regulation (GDPR) and the Data Protection Act 2018 (DPA) came into force on 25 May 2018.

They are concerned with the rights of individuals with regards to the processing of their personal data and their rights to gain access to personal information held about them by an organisation or individual within it, and the right to challenge the accuracy of data held.

Individuals have a right to apply for access to information held about them by the College, or to information about a third party if they have appropriate permission to do so. The terms of GDPR and the Act relate to data held in any form, including written notes and records, not just electronic data. The College is committed to ensuring that personal data is collected, stored and disposed of in a secure and appropriate manner.

We respect the data subject's right to privacy and accuracy, and their right to access their own personal data where appropriate.

2 Scope

This policy outlines how the College will fulfil its obligations in accordance with the General Data Protection Regulation and the Data Protection Act 2018. The College needs to process certain personal data (see section 3 of this policy, Definitions) relating to staff and students in order to fulfil its purpose and to meet its legal obligations to funding bodies and the government. The College will process such information according to the Data Protection Principles that are set out in the GDPR and DPA.

3 Definitions

Personal data is identified by the College under the following terms: Photographs, written personal details, video recordings, audio recordings, and any combination of items that can be assembled to identify an individual. Classes of information currently held by the College may include:

- Personal details.
- Family, lifestyle and social circumstances.
- Education and training details.
- Employment details.
- Financial details.
- Goods or services provided.
- Racial or ethnic origin.
- Trade union membership.
- Physical or mental health or condition.
- Offences (including alleged offences).

GDPR and the DPA defines both personal data and sensitive personal data. Data processors must ensure that the necessary conditions are satisfied for the processing of personal data and in addition that the extra, more stringent, conditions are satisfied for the processing of sensitive personal data. Personal data has a wide-ranging definition and can include not only items such as home and work address, age, telephone number and schools attended but also photographs and other images. Sensitive personal data consists of racial or ethnic origin, political opinion, religious or similar beliefs,

trade union membership, physical or mental health or condition, sexual life and criminal record. For further definitions, see the Data Protection Glossary.

4 Key Principles

The College will process all personal data according to the 6 principles of the Data Protection Act. College Data Areas as defined in Section 5 will be responsible for the following aspects of data protection, which are regarded as essential for data integrity and security:

- Awareness of the principles as detailed in the guidelines and in the act.
- Suitability of storage facilities.
- Retention and deletion of records.
- External disclosure and sharing procedures.
- Knowledge of GDPR subject access data request procedures.
- Review of local information policy.
- Clearly defined roles and responsibilities.
- Data breach reporting.
- Knowledge of data sharing arrangements (e.g. with UHI).
- How to deal with Freedom of Information Requests.

5 Responsibilities

The College, as Data Controller, is responsible for all Data Protection policies and procedures. Any Data Protection incidents should be reported to the Data Protection Officer.

The named Data Controller contact for the College is: The Director of Corporate Affairs (data@smo.uhi.ac.uk).

The following members of staff have responsibility for overseeing day-to-day data processing activities in the following data areas:

- Principal/Senior Management Team (high level College strategy and finance).
- College Registrar (central College information systems/Personal Academic Tutor records/ International student records).
- Director of Corporate Affairs (staff records, training and development).
- Head of IT (IT systems and security, library records, procurement).
- Director of Finance (payroll, finance, estates).
- All data processors are responsible for awareness of, and adherence to, relevant data protection policies, procedures and regulations. The DIrector of Corporate Affairs is responsible for monitoring the review of College policies.

6 Linked Policies/Related Documents

ICO Register of Data Controllers
SMO Publication Scheme (Freedom of Information (Scotland) Act 2002)
GDPR Subject Access Request Form
SMO College ICT Acceptable Use Policy
SMOCollege Records Management and Procedures Policy
GDPR
Data Protection Subject Access Request Form (CCTV)
Data Protection Glossary
ICO CCTV Code of Practice

7 Relevant Legislation

Data Protection Act 2018
Freedom of Information (Scotland) Act 2002
Human Rights Act1998