Policy

Goldsmiths
UNIVERSITY OF LONDON

# Data Protection

Owner: Senior Information Risk Officer
Review date 20 May 2019

## 1. Introduction

1.1 The College holds and processes personal information about its current, past and prospective staff, applicant students, students, alumni as well as others with whom it has dealings. It does this in order to carry out the functions of a university and to discharge certain statutory and regulatory responsibilities.

1.2 In processing personal information such as personal data, the College is committed to respecting the privacy rights of individuals and meeting its obligations as a data controller in accordance with all relevant data protection and privacy legislation to which it is subject.

## 2. Definitions

2.1 Data Protection and Privacy Legislation

This includes the Data Protection Act (hereafter “DPA”), the General Data Protection Regulation (hereafter “GDPR”) and the Privacy and Electronic Communications Regulations (hereafter “PECR”), as well as other future legislation that supplements or supersedes the aforementioned.

2.2 Personal Data

Any information, contained within a structured record, by which a living individual can be identified. Lots of information can serve to identify an individual, such as name, identification numbers, location data or images.

2.3 Sensitive Personal Data

Certain information about an individual, such as ethnicity and health, is considered to be sensitive personal data. Information within this category of personal data must be given greater protection.

2.4 Data Controller

A data controller determines the purposes and means of processing personal data. The College is a data controller.

2.5 Data Processor

A data processor is responsible for processing personal data on behalf of the controller. The College is a data processor.

2.6 Processing

Processing occurs when the College treats personal data in any way, whether or not by automated means. Examples of processing are collection, storage, disclosure, review and erasure.

2.7 Data Subject

This is the identifiable subject of any personal data that the College processes. The data subject is afforded privacy rights.

2.8 Personal Data Breach

A breach is a security incident that affects the confidentiality, integrity or availability of personal data. A breach will occur where there is accidental or unlawful destruction, loss, alteration, unauthorised disclosure of or access to, personal data.

## 3. Principles

3.1 When processing any personal data, the College will always observe the following principles:

a) Lawful basis - that one or more of the following lawful bases exist for processing:

- that consent to do so has been freely given by the data subject, is specific, informed and unambiguous;
- to fulfil contractual obligations to the data subject
- that the processing is necessary in order to comply with a legal or regulatory obligation to which the College is subject;
- that the processing is necessary to protect the vital interests of a data subject;
- to exercise the functions of an official authority or perform a specific task in the public interest that is set out in law; and/or
- that the processing is in the legitimate interests (including commercial interests or broader societal benefits) of the College or third parties.

b) Fair and transparent - that the College will be fair and transparent when processing personal data by providing data subjects with the information required to ensure they understand the nature of the processing and how to exercise their rights in relation to that processing.

c) Collected for specified, explicit and legitimate purposes – that personal data will only be collected for particular purposes that have been made clear to the data subject and shall not be processed for any further or alternative purpose.

d) Accuracy – the College ensures that the personal data it holds is accurate and does, where necessary, take steps to keep it up to date.

e) Minimisation – the College will only hold relevant personal data for so long as is necessary for legitimate purposes. However, it may be held for longer solely for archiving purposes that are in the public interest, for scientific or historical research purposes or statistical purposes.

f) Security – the College will have in place effective organisational and technical measures to protect personal data against being processed unlawful processing.

g) Privacy by design and default – the College's commitment to privacy rights will be at the core of any project undertaken which may result in new processing of personal data. Appropriate technical and organisational measures to ensure that data protection principles are incorporated into the development and operation of personal data processing activities.

h) Accountability – that the College takes responsibility for what is does with the personal data it holds. We will maintain appropriate records to allow us to demonstrate our compliance with these principle, including records of processing activities under our control. A Data Protection Officer will be designated to monitor and drive compliance with these principles and shall be provided with the resources and support necessary to carry out those tasks.

i) International transfers – Goldsmiths will not transfer personal data to a state that is not a member of the European Union unless the recipient processor has in place adequate measures to safeguard the privacy rights of data subjects.

3.2 Any member of the College who processes personal data otherwise than in accordance with the principles scheduled above or who by their actions breach this Policy could face disciplinary action.

## 4 Roles of specified College staff in relation to data protection

4.1 The Senior Information Risk Owner

The Registrar and Secretary has been designated as the College's Senior Information Risk Officer with overall responsibility for ensuring compliance with data protection legislation as well as the College's accountability.

4.2 Data Protection Officer

4.2.1 The College shall designate a Data Protection Officer. In addition to any additional tasks they may be asked to undertake by the College, the Data Protection Officer shall carry out those statutory tasks assigned to them as follows:

- to inform and advise the College and its staff about the need to comply with data protection and privacy legislation and this Policy;
- to monitor the College's compliance with data protection and privacy legislation and this Policy;
- to raise awareness of data protection and privacy issues;
- to ensure that adequate training is undertaken by the College's staff in respect of data protection and privacy;
- to conduct internal audits of compliance
- to advise on, and to monitor, data protection impact assessments; and
- to be the first point of contact for the Information Commissioner and to cooperate in the same
- coordinate the College's responses to enquiries from data subjects about data protection and their privacy rights.

4.2.2 The Data Protection Officer, reporting directly to the highest level of management, shall enjoy the independence necessary to perform their tasks and shall be sufficiently well resourced. They will suffer no penalty as a result of performing their tasks.

4.3 Managers and Data Owners

Managers and all staff who process personal data on behalf of the College have a responsibility for ensuring that data protection issues within their areas are managed in a way that meets the provisions of this policy and that all staff undertake the mandatory training necessary to fulfil that role.

## 5 Responsibilities of all staff and students

5.1 Goldsmiths expects all staff and students to process personal data for which the College is controller in accordance with this Policy and other associated policies.

5.2 In processing personal data controlled by the College, all staff and students will at all times exercise due care and attention to ensure that the principles set out above are observed.

5.3 Any reckless or wilful conduct by staff or students which undermines this Policy or puts at risk the security of any personal data may result in disciplinary action being taken against them.

5.4 All staff are required to undertake the mandatory training courses concerning information management and data security within three months of joining the College. Where these training courses are revised to reflect changes in the data protection and privacy legislation landscape, staff will be expected to refresh their training. The College will maintain a record for the purposes of monitoring completion of training.

5.5 Wherever a new or changed business practice is to be instituted that will impact the processing of personal data, staff will complete the College's

Personal Data Collection Form (Appendix A) and submit the same to the Data Protection Officer.

## 6 Personal data security breach reporting

6.1 Any loss, unintended deletion, alternation or sharing of personal data is a security breach and must be reported to the University's Data Protection Officer immediately a member of staff becomes aware of the incident.

Appendix A – Personal data collection template

Appendix B – General information privacy notice

Appendix C – Student collection notice

Appendix D – Staff collection notice

Appendix E – Alumni Collection notice

Appendix F – Model specific collection notice

Appendix H – Other related polices & procedures