HERTFORD COLLEGE

DATA PROTECTION POLICY

V3.0 (May 2018)

Contents

1. Introduction

We regard the lawful and correct treatment of personal information as very important to our successful operation and to maintaining confidence between us and those with whom we deal. We will ensure that we treat personal information lawfully and correctly.

To this end we fully endorse and adhere to the principles of the General Data Protection Regulation (GDPR).

This policy sets out how we do this, and the specific rules or approaches we adopt.

1. Version

This document is **Version 3 (May 2018).**

The document owner is the Bursar, who is responsible for its maintenance.

2. Data Protection Officer

The College Data Protection Officer appointed to oversee its compliance activities in respect of Data Protection is the Deputy Bursar.

Contact details are : ***dpo@hertford.ox.ac.uk***

2. Definitions

"Personal data" is information that relates to an identifiable person who can be directly or indirectly identified from that information, for example, a person's name, identification number, location, online identifier. It can also include pseudonymised data.

"Special categories of personal data" is data which relates to an individual's health, sex life, sexual orientation, race, ethnic origin, political opinion, religion, and trade union membership. It also includes genetic and biometric data (where used for ID purposes).

"Criminal offence data" is data which relates to an individual's criminal convictions and offences.

"Data processing" is any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

3. Data Protection Principles

Under GDPR, all personal data obtained and held by us must be processed according to a set of core principles. In accordance with these principles, we will ensure that:

- processing will be fair, lawful and transparent
- data be collected for specific, explicit, and legitimate purposes
- data collected will be adequate, relevant and limited to what is necessary for the purposes of processing
- data will be kept accurate and up to date. Data which is found to be inaccurate will be rectified or erased without delay
- data is not kept for longer than is necessary for its given purpose
- data will be processed in a manner that ensures appropriate security of personal data including protection against unauthorised or unlawful processing, accidental loss, destruction or damage by using appropriate technical or organisation measures
- we will comply with the relevant GDPR procedures for international transferring of personal data

4. Understanding the data we hold and process

The College keeps Records of Processing Activities (ROPAs) for all activities that involve personal data, arranged according to the following categories.

- Applicants and Prospective Students
- Current Students
- Job Applicants

- Current and former Staff
- Attendees, organisers and those involved in conferences and events
- Suppliers, contractors, and those with whom we undertake financial transactions
- Those who come in to contact with our security systems and procedures
- Those who use our IT services, or telephony systems
- Users of our website
- Those whose data is stored in our archive

These ROPAs contain information about, inter alia, the nature of data held / processed, why it is processed, the legal bases by which we hold it, and the length of time we hold it for.

They will be reviewed on a regular basis to ensure they remain current, and will be published via the College's Privacy Notice.

5. Respecting Individuals' Rights

1. The right to be informed

We inform people about the data we hold on them in the following ways:

- Through our Privacy Notice, available on the College website.
- By providing links to this notice at key interaction points, e.g. when communicating with a prospective applicant for the first time, or via the particulars for an advertised role.
- Through induction training for our staff.
- By ensuring we have consent from individuals where that is the legal basis upon which we hold and process the data.

2. The right of access (Subject Access Requests)

We will provide information about the data we hold on individuals to them upon request.

All requests will be referred to the DPO for the co-ordination of a response.

Timescales

We will comply with a request without delay and at the latest within one month. Where requests are complex or numerous, we may contact the requester to inform them that an extension of time is required. The maximum extension period is two months.

Fee

We will normally comply at no cost. However, if the request is manifestly unfounded or excessive, or if it is repetitive, we may charge a fee. This fee must be paid in order for us to comply with the request. The fee will be determined at the relevant time by the DPO and will be set at a level which is reasonable in the circumstances.

In addition, we may also charge a reasonable fee for further copies of the same information.

Information we will provide

We will include the following information in our responses:

- whether or not data is processed and the reasons for the processing;
- the categories of personal data concerned;
- where your data has been collected from if it was not collected from the individual;
- details of anyone the personal data has been disclosed to or will be disclosed to, including anyone outside of the EEA and the safeguards utilised to ensure data security;
- how long the data is kept for (or how that period is decided);
- an individual's rights in relation to data rectification, erasure, restriction of and objection to processing;
- the right to complain to the Information Commissioner if an individual believes that their rights have been infringed;
- the reasoning behind any automated decisions taken about the individual.

Refusal of a request

We may refuse to deal with a subject access request if it is manifestly unfounded or excessive, or if it is repetitive. Where it is our decision to refuse a request, we will contact the requester without undue delay, and at the latest within one month of receipt, to inform them of this and to provide an explanation. They will be informed of their right to complain to the Information Commissioner and to a judicial remedy.

We may also refuse to deal with a request, or part of it, because of the types of information requested. For example, information which is subject to legal privilege or relates to management planning is not required to be disclosed. Where this is the case, we will inform the requester that the request cannot be complied with and provide an explanation of the reasons.

3. The right to rectification, erasure, restrict processing, or data portability.

All such requests will be logged, and referred to the DPO for a response.

The DPO will determine the nature of any response, including if we wish to refuse for any reason allowed under the GDPRs.

We will respond to any of these types of requests within one calendar month, or sooner where possible.

4. The right to object

All notifications of an individual's objection to processing their data will be referred to the DPO for handling.

We will set out an Individual's right to object at the point of first communication where the legal basis for processing the category of data concerned is legitimate interest or public task.

We will immediately comply with any request to cease direct marketing.

5. Rights in relation to automated decision making and profiling.

We do not undertake automated decision making / profiling, and do not therefore have any current processes for managing related rights.

If this position changes we will develop suitable policies and procedures.

6. Consent

We maintain a record / evidence of individuals' consent for any data we hold on a consent basis.

We will immediately comply with any withdrawal of consent in a manner consistent with the provisions of the GDPR.

7. Children

We are mindful of the need to adapt our communication and data processes suitably when dealing with minors, and will take this in to consideration when designing data collection and processing procedures.

8. Data Security

We will ensure that employees are made aware of their responsibilities when their role involves the processing of personal data.

Specifically, employees are required to adhere to the following rules:

- Hard copy personal information should be kept in a locked filing cabinet, drawer, or safe.
- Files or written information of a confidential nature must be stored in a secure manner so that are only accessed by people who have a need and a right to access them and employees must ensure that screen locks are implemented on all PCs, laptops etc. when unattended. No files or written information of a

confidential nature are to be left where they can be read by unauthorised people.

- Where data is computerised, it should be coded, encrypted or password protected both on a local hard drive and on a network drive that is regularly backed up. If a copy is kept on removable storage media, that media must itself be kept in a locked filing cabinet, drawer, or safe.
- Employees must always use the individual passwords provided to access the computer system and not abuse them by passing them on to people who should not have them.
- Personal data relating to employees should not be kept or transported on laptops, USB sticks, or similar devices, unless prior authorisation has been received from the Bursar. Where personal data is recorded on any such device it should be protected by:
    - ensuring that data is recorded on such devices only where absolutely necessary.
    - using an encrypted system — a folder should be created to store the files that need extra protection and all files created or moved to this folder should be automatically encrypted.
    - ensuring that laptops or USB drives are not left where they can be stolen.
- Employees have a duty to report immediately to the Data Protection Officer any suspected or actual data breach that they become aware of, whether they have direct involvement in such a breach or otherwise. Confidentiality in respect of the informant's identity will be observed if requested, in so far as it does not jeopardise the proper action required to address the breach.
- Failure to follow the College's rules on data security may be dealt with via the College's disciplinary procedure. Appropriate sanctions include dismissal with or without notice dependent on the severity of the failure.

We aim to comply to the fullest extent with the University's Information Security policies and standards, and undertake regular internal audits to assess compliance in this regard.

9. Third Party Processing

Where we engage third parties to process data on our behalf, we will ensure, via a data processing agreement with the third party, that the third party takes such measures in order to maintain the College's commitment to protecting data.

Such agreements will include the following key details:

- the subject matter and duration of the processing;
- the nature and purpose of the processing;
- the type of personal data and categories of data subject; and
- the obligations and rights of the controller.

and include the following compulsory terms stating that:

- the processor must only act on the written instructions of the controller (unless required by law to act without such instructions);
- the processor must ensure that people processing the data are subject to a duty of confidence;
- the processor must take appropriate measures to ensure the security of processing;
- the processor must only engage a sub-processor with the prior consent of the data controller and a written contract;
- the processor must assist the data controller in providing subject access and allowing data subjects to exercise their rights under the GDPR;
- the processor must assist the data controller in meeting its GDPR obligations in relation to the security of processing, the notification of personal data breaches and data protection impact assessments;
- the processor must delete or return all personal data to the controller as requested at the end of the contract; and
- the processor must submit to audits and inspections, provide the controller with whatever information it needs to ensure that they are both meeting their Article 28 obligations, and tell the controller immediately if it is asked to do something infringing the GDPR or other data protection law of the EU or a member state.

10. International Data Transfers

We will reference the European Commission's register of "adequacy" in relation to the protections afforded by other countries to guide our approach to international data sharing in specific cases.

When a data subject is resident outside the EU in a country where there is no "adequacy decision" by the European Commission, and an alternative safeguard is not available, we may still transfer data to that subject where it is necessary for the implementation of pre-contractual measures, or for the performance of a contract with us.

Otherwise, we may transfer personal data outside the European Union, but only for the purposes referred to in our Records of Processing Activities and provided:

- There is a decision of the European Commission that the level of protection of personal data in the recipient country is adequate; or
- Appropriate safeguards are in place to ensure that data is treated in accordance with UK data protection law, for example through the use of standard contractual clauses; or
- There is an applicable derogation in law which permits the transfer in the absence of an adequacy decision or an appropriate safeguard.

11. Data Breaches

We are aware of our obligation to report Data Breaches, and will apply the approaches set out in this section to managing our responsibilities in this area.

1. Definition

A personal data breach is a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or processed.

The following are examples of data breaches:

- access by an unauthorised third party;
- deliberate or accidental action (or inaction) by a data controller or data processor;
- sending personal data to an incorrect recipient;
- computing devices containing personal data being lost or stolen;
- alteration of personal data without permission;
- loss of availability of personal data.

2. Detection

We employ a variety of mechanisms to detect data breaches, including:

- Regular audit of data processing activities carried out by our employees to ensure that they aware aware of our policies and the rules we have set out for the proper protection of personal data.
- Automated and continuing monitoring of our IT systems to detect any potential or actual intrusions.
- Regular inspection of physical data storage areas and systems to ensure compliance with our policies for data security.
- Making it a duty of employees to report any suspected breach, and providing a confidential route for reporting of such.

3. Investigation

In the event that we become aware of a breach, or a potential breach, an investigation will be carried out.

This investigation will be carried out by the Data Protection Officer, in consultation with the Bursar, who will make a decision over whether the breach is required to be notified to the Information Commissioner. A decision will also be made over whether the breach is such that the individual(s) involved must also be notified.

4. Notifying the Information Commissioner

We will notify the Information Commissioner of a breach which is likely to pose a risk to people's rights and freedoms. A risk to people's freedoms can include physical, material or non-material damage such as discrimination, identity theft or fraud, financial loss and damage to reputation.

Notification will be done without undue delay and at the latest within 72 hours of discovery. If we are unable to report in full within this timescale, we will make an initial report, and then provide a full report in more than one instalment if so required.

The following information will be provided when a breach is notified:

- a description of the nature of the personal data breach including, where possible:
    - the categories and approximate number of individuals concerned; and
    - the categories and approximate number of records concerned
- the name and contact details of the Data Protection Officer from whom more information can be obtained;
- a description of the likely consequences of the personal data breach; and
- a description of the measures taken, or proposed to be taken, to deal with the personal data breach, including, where appropriate, the measures taken to mitigate any possible adverse effects.

5. Notifying Individuals

We will notify the individual whose data is the subject of a breach if there is a *high* risk to people's rights and freedoms. A high risk may be, for example, where there is an immediate threat of identity theft, or if special categories of data are disclosed online. This notification will be made without undue delay and may, dependent on the circumstances, be made before the supervisory authority is notified.The following information will be provided when a breach is notified to the affected individuals:

- a description of the nature of the breach
- the name and contact details of the Data Protection Officer from whom more information can be obtained
- a description of the likely consequences of the personal data breach and
- a description of the measures taken, or proposed to be taken, to deal with the personal data breach, including, where appropriate, the measures taken to mitigate any possible adverse impacts.

6. Record Keeping

The College records all personal data breaches regardless of whether they are notifiable or not as part of its general accountability requirement under GDPR. It records the facts relating to the breach, any impacts, and the remedial action taken.

12. Privacy by Design

We will conduct Data Protection Impact Assessments (DPIAs), in accordance with the combined requirements of the GDPR and the Information Commissioner's Office (ICO), if we:

- use new technologies;
- use profiling or special category data to decide on access to services;
- profile individuals on a large scale;
- process biometric data;
- process genetic data;
- match data or combine datasets from different sources;
- collect personal data from a source other than the individual without providing them with a privacy notice ('invisible processing');
- track individuals' location or behaviour;
- profile children or target services at them;
- process data that might endanger the individual's physical health or safety in the event of a security breach.

If a DPIA indicates that the data processing is high risk, and we cannot sufficiently address those risks, we will consult the ICO to seek its opinion as to whether the processing operation complies with the GDPR. The DPO will undertake a regular review of College operations and intended new operating practices to establish in good time whether a DPIA is required.

13. DP Records & Logs

We will maintain logs of various aspects of our activities in respect of our Data Protection obligations. These include:

- Processing Activities, including Data Sharing agreements
- Requests received in pursuit of Individual rights under GDPR, including a record of any responses made.
- Internal audits we perform to test compliance from time to time.
- Any review, update and deletion activities we undertake in accordance with our retention policies
- Any DPIAs we conduct
- Reported or actual data breaches, and the actions taken as a consequence including any ICO reporting decision taken.