HARRIS MANCHESTER COLLEGE

POLICY ON DATA PROTECTION

Contents

1. Purpose and scope
2. Background
3. Principles
4. Aims and commitments
5. Roles and responsibilities
6. Breaches of data privacy legislation
7. Compliance
8. Further information
9. Review and development
10. Related policies

1.Purpose and scope

This policy provides a framework for ensuring that the College meets its obligations under the *Data Protection Act* (2018), *General Data Protection Regulation* (GDPR) and associated legislation ('data privacy legislation')[1].

Since Harris Manchester College is also a part of the University of Oxford, its members are bound by the *University Policy on Data Protection*, which College policy follows closely.

It applies to all processing of personal data carried out for a College purpose, irrespective of whether the data is processed on non-College equipment or by third parties.

> *'**Personal data**' means any information relating to an identifiable living individual who can be directly identified from that data, or indirectly from that data and other data.*
>
> *'**Processing**' means anything that is done with personal data, including collection, storage, use, disclosure and deletion.*

More stringent conditions apply to the processing of *special category* personal data.

[1] This includes all legislation enacted in the UK in respect of the protection of personal data such as the *Data Protection Acts*, (1998 and 2018) and the *Privacy and Electronic Communications* (EC Directive) Regulations 2003.

'**Special category**' *means personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying an individual, data concerning health or data concerning an individual's sex life or sexual orientation.*

This policy should be read in conjunction with any other documents that impose confidentiality or data management obligations in respect of information held by the College. Additional information can be found in the *Guide to the General Data Protection Regulation* issued by the Information Commissioner's Office. A series of guidance papers, written by the College Data Protection Officer, provide further detail and advice on the practical application of the law and this policy.

This policy does not cover the use of personal data by members of the College when acting in a private or non-College capacity.

2. Background

The processing of personal data underpins almost everything the College does.

Without it, students cannot be admitted and taught; staff cannot be recruited; living individuals cannot be researched; and events cannot be organised for alumni or visitors. We are responsible for handling people's most personal information.

By not handling personal data properly, we could put individuals at risk.

There are also legal, financial and reputational risks for the College. For example:

- If we are not able to demonstrate that we have robust systems and processes in place to ensure we use personal data properly we might lose our ability to carry out research projects requiring access to personal data, particularly in the medical field.

- Reputational damage from a breach may affect public confidence in our ability to handle personal information.

- The Information Commissioner's Office (ICO), which enforces data privacy legislation, has the power to fine organisations up to £17.5 million, or 4% of global annual turnover for serious breaches.

3. Principles

The processing of personal data must comply with data privacy legislation and, in particular, the six data privacy principles. These principles are explained in detail in both the University's *Guidance on Data Protection*, the ICO *Guide to the General Data Protection Regulation,* and the relevant guidance by the College's Data Protection Officer. In summary, they require that personal data is:

- processed fairly, lawfully and in a transparent manner;
- used only for limited, specified stated purposes and not used or disclosed in any way incompatible with those purposes;
- adequate, relevant and limited to what is necessary;
- accurate and, where necessary, up-to-date;
- not kept for longer than necessary; and
- kept safe and secure.

In addition, a new accountability principle requires us to be able to produce *written* evidence to document the College's compliance with these principles, and these documents must be open to inspection by the public, and by the Information Commissioners.

4. Aims and commitments

The College handles a large amount of personal data and takes seriously its responsibilities under data privacy legislation. It recognises that the mishandling of an individual's personal data may cause them distress or put them at risk of identity fraud.

As a result, it is committed to:

- complying fully with data privacy legislation;
- where practicable, adhering to good practice, as issued by the ICO or other appropriate bodies; and
- handling an individual's personal data in a careful and considerate manner that recognises the importance of such information to their privacy and welfare.

The College seeks to achieve these aims by:

- ensuring that staff, students and other individuals who process data for College purposes are made aware of their individual responsibilities under data privacy legislation and how these apply to their areas of work. For example, employment contracts include a clause drawing the attention of the employee to data privacy legislation and the University's data protection policy;
- providing suitable training, guidance and advice. The University's online training course on data privacy and information security is available to all members of the University. The online course is supplemented by bespoke on-site training, where appropriate, along with regular talks and presentations available at University conferences and departmental meetings. The College's *Data Protection Officer* has also written a series of guides to different aspects of the new legislation, its principles and legal requirements.

• incorporating data privacy requirements into administrative procedures where these involve the processing of personal data, particularly in relation to major information systems (the concept of 'privacy by design');

• operating a *centrally coordinated procedure* (in order to ensure consistency) for the processing of subject access and other rights-based requests made by individuals; and

• *investigating* promptly any suspected breach of data privacy legislation; *reporting* it, where necessary, to the ICO; and seeking to *learn* any lessons from the incident in order to reduce the risk of re-occurrence.

5. Roles and responsibilities

Principal and Governing Body: The College's *Principal* and *Governing Body* has executive responsibility for ensuring that the College complies with data privacy legislation. It is supported by its *Data Protection Committee*, which is responsible for keeping under review the College's policies and compliance with legislation and regulatory requirements.

Data Protection Officer: The College *Data Protection Officer* (DPO) is responsible for monitoring internal compliance, advising on the College's data protection obligations, and acting as a point of contact with the Information Commissioner's Office when necessary.

Data Protection (Compliance) Team : The College's *Data Protection (Compliance) Team* is responsible for the day to day work of:-

• establishing and maintaining policies and procedures at a central level to facilitate the College's compliance with data privacy legislation, and University policies;

• establishing and maintaining guidance and training materials on data privacy legislation and specific compliance issues;

• supporting privacy by design and privacy impact assessments;

• responding to requests for advice from departments;

• coordinating a College-wide audit and register to capture the full range of processing that is carried out, and keep this register regularly up-dated;

• complying with *subject access requests* made by individuals for copies of their personal data, and other rights-based requests; and

• requests from the ***University's*** *Information Compliance Team* for information are complied with promptly;

• investigating and responding to complaints regarding data privacy (including requests to cease the processing of personal data); and

• keeping records of personal data breaches, notifying the ICO of any significant breaches and responding to any requests that it may make for further information; and

Ensuring that there is a designated person responsible for keeping policies and records up to date with regard to the security of personal data (including risk assessments), retention and deletion schedules, Privacy Notices, and Records of Processing Activities.

In fulfilling these responsibilities, the team may also involve, and draw on support from employees and members of the College, the University's Information Compliance Team, as well as seek advice and guidance from the College's Data Protection Officer.

Those responsible for the College's principal collections of personal data (eg Admissions, Accounts, Archives, IT etc): "Heads of department"

The College's activities are diverse. In addition to be being a place where students are taught and research conducted, the College is also an employer, as well as a sponsor of a wide variety of educational initiatives, such as Open Days, Conferences, and the many activities of the *Farmington Institute*[2]. Each area of College activity (eg Admissions, or Accounts) has a "data bank"[3] of personal data (such as contact addresses) appropriate to their own distinctive activities, and the categories of people with whom they deal.

Collections of Personal Data or Personal Data "*departments*" typically include, but are not necessarily limited to the following:-

1. Applicants and Prospective Students
2. Current HMC Students, and those who have accepted offers of places at the College
3. Alumni, Donors and Supporters
4. Current Staff, Office Holders and Senior Members ("Employees"?)
5. Applicants for Office, Senior Membership (and Employment?)
6. Archives
7. IT, e Mail and Mobile Devices
8. College Website
9. Security (including CCTV and electronic building entry data)
10. Attendees, organisers and others involved in College Conferences and Events
11. Contractors, Finance, Commercial and Related Administration.

Each of these "data banks" which enables the different areas or "departments" of College life to continue, needs to have a *designated person* responsible, whether or not they formally hold the position of "*Head of Department*".

These Heads of Departments, or other designated persons are responsible for ensuring that the processing of personal data in their "department" conforms to the requirements of data privacy legislation and this policy. In particular, they must ensure that:

[2] such as scholarships, conferences and school visits.

[3] In some cases, these "data banks" are very specialised, and have little or no significant overlap with others. In other cases, personal data is held in common by several distinct areas of College activity, and/or the University.

• the data bank(s) for which they are responsible must publish (and regularly maintain the accuracy of) separate *Privacy Notices*, *Records of Processing*, Personal Data Risk Assessments, Retention and Deletion schedules, Breach and Subject Access Records (and all other required documents and records), as required by UK Data Protection law.

• new and existing staff, visitors, or third parties associated with the "department" who are likely to process personal data are aware of their responsibilities under data privacy legislation. This includes drawing the attention of College staff to the requirements of this policy, ensuring that staff who have responsibility for handling personal data are provided with adequate training and, where appropriate, ensuring that job descriptions for members of staff, or agreements with relevant third parties, refer explicitly to data privacy responsibilities and make these a contractual condition.

• adequate records of processing activities are kept (for example, by keeping registers of Processing Activities, Third Party Contracts, non-EU Data Transfers, Security Audits, rights-based Access requests);

• data protection requirements are embedded into systems and processes by adopting a '*privacy by design and default*' approach and undertaking *privacy impact assessments* where appropriate;

• privacy notices are provided to individuals where data is collected *directly* from individuals or where data is used in non-standard ways;

• data sharing is conducted in accordance with College and University guidance;

• requests from the University's *Information Compliance Team* for information are complied with promptly;

• data privacy risks are included in the department's risk management framework and considered by senior management on a regular basis; and

• College and "department" policies and procedures are adopted where appropriate.

Staff, students, volunteers, and all others processing personal data for a College purpose

Anyone who processes personal data for a College purpose is ***individually responsible*** for complying with data privacy legislation, this policy, University policy, and any other policy, guidance, procedures, and/or training introduced by the College or University to comply with data privacy legislation.

For detailed guidance, they should refer to the University's Guidance on Data Protection and any relevant College and departmental policies and procedures.

In summary, they must ensure that they:

• only use personal data in ways people would expect and for the purposes for which it was collected;

- use a minimum amount of personal data and only hold it for as long as is strictly necessary;

- keep personal data up-to-date;

- keep personal data secure, in accordance with the University's Information Security Policy;

- do not disclose personal data to unauthorised persons, whether inside or outside the University;

- complete relevant training as required;

- report promptly any suspected breaches of data privacy legislation, in accordance with the procedure in section 6 below, and following any recommended next steps;

- seek advice from the College *Data Protection (Compliance) Team*, (or University *Information Compliance Team*), as appropriate, where they are unsure how to comply with data privacy legislation, College policy, or University Policy on Data Protection

- respond promptly to any requests from the ***College*** *Data Protection (Compliance) Team*, or ***University*** *Information Compliance Team* in connection with subject access and other rights-based requests and complaints (and forward any such requests that are received directly to the College *Data Protection (Compliance) Team* or University *Information Compliance Team*, as appropriate, promptly).

6. Breaches of data privacy legislation

The College and (where appropriate) University will investigate incidents involving a possible breach of data privacy legislation in order to ensure that, where necessary, appropriate action is taken to mitigate the consequences and prevent a repetition of similar incidents in future.

Depending on the nature and severity of the incident, it may also be necessary to notify the *individuals* affected and/or the *ICO*.

A "breach" will occur where, for example, personal data is disclosed or made available to unauthorised persons, or personal data is used in a way that the individual does not expect, or where data is rendered inaccurate or unavailable.

Incidents involving failures of IT systems or processes must be reported to both the College's IT Department, and the Oxford University Computer Emergency Response Team (OxCert) **within 4 working hours of discovery**. OxCert will liaise, as appropriate, with the Information Compliance Team.

All *other* data security incidents must be reported *directly* to the College *Data Protection (Compliance) Team,* and also (where relevant) to the University's *Information Compliance Team* **at the earliest possible opportunity**.

OxCert:- Oxford University Computer Emergency Response Team

oxcert@infosec.ox.ac.uk or telephone:- 01865 (2)82222

Oxford University Information Compliance Team: data.breach@admin.ox.ac.uk

Harris Manchester College Data Protection (Compliance) Team:

data.protection@hmc.ox.ac.uk or telephone:

7. Compliance

The College, like the University, regards any breach of data privacy legislation, this policy or any other policy (and/or training introduced by the University from time to time to comply with data privacy legislation) as a serious matter, which may result in disciplinary action.

Depending on the nature of the breach, an individual may also find that they are personally liable (for example, it can be a criminal offence for a member of the College or University to disclose personal information unlawfully).

8. Further information

Questions about this policy, records, and data privacy matters in general should be directed, as appropriate, either to:-

the College Data Protection (Compliance) Team at: ? data.protection@hmc.ox.ac.uk or

the University Information Compliance Team at data.protection@admin.ox.ac.uk

Questions about information security should be directed (as appropriate) either to

the College's *IT Information Security Team* at ??? or

the University's *Information Security Team* at: infosec@it.ox.ac.uk

9. Review and development

This policy, and supporting guidance, came into effect on 25th May, 2018 and has been periodically reviewed. This is the fifth revision.

10. Related policies

This policy should be read in conjunction with related policies and regulations, including the:

- University and College Information Security Policies; and
- Regulations relating to the use of Information Technology Facilities

Chris O'Neill,

15th October, 2024