General Data Protection Policy

February 2019, v1.1

1. Purpose and scope

This policy provides a framework for ensuring that the College meets its obligations under data protection legislation[1].

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 identified from that data or 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.

'*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 accompanying guidance, which provides further detail and advice on practical application, as well as any other documents that impose confidentiality or data management obligations in respect of information held by the College.

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,

[1] This includes the General Data Protection Regulation (GDPR) 2018, Data Protection Act 2018 as well as the Privacy and Electronic Communications Regulations 2003.

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.
- Reputational damage from a breach may affect public confidence in our ability to handle personal data.
- The Information Commissioner's Office (ICO), which enforces data protection legislation, has the power to fine organisations up to 4% of global annual turnover for serious breaches.

3. Lawful basis for processing personal data

The data protection legislation lists six lawful reasons for processing personal data.[2] The processing of personal data can only take place if at least one of the conditions applies.

(a) Consent: the individual has given clear consent for the College to process their personal data for a specific purpose.[3]

(b) Contract: the processing is necessary for a contract the College has with the individual, or because they have asked the College to take specific steps before entering into a contract.[4]

(c) Legal obligation: the processing is necessary for the College to comply with the law (not including contractual obligations).[5]

(d) Vital interests: the processing is necessary to protect someone's life.[6]

---

[2] For more information see ICO, *Lawful basis for processing* https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/lawful-basis-for-processing/

[3] For consent to be valid it must be specific, informed, freely given and unambiguous. Where consent is the most appropriate basis for processing personal data, the College will ensure that individuals are aware of their right to withdraw their consent and will maintain records of consent.

[4] Personal data is needed in order to meet a contractual obligation to the individual

[5] Most of the processing done on this basis is likely to apply to centrally collected personal data, for example, the provision of student and staff data to HESA or the provision of salary data to HMRC.

[6] This basis is very limited in scope, and will generally only apply to matters of life or death, for example where the College may need to disclose information in order to ensure that someone receives emergency medical treatment.

(e) Public task: the processing is necessary for the College to perform a task in the public interest or for its official functions, and the task or function has a clear basis in law.[7]

(f) Legitimate interests: the processing is necessary for the College's legitimate interests or the legitimate interests of a third party, unless there is a good reason to protect the individual's personal data which overrides those legitimate interests. (This does not apply when the College (as a public authority) is processing data to perform its official tasks.)[8]

4. Data protection principles

The processing of personal data must comply with data protection legislation and, in particular, the six data protection principles.

In summary, these six data protection principles 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 evidence compliance with these principles.

5. Aims and commitments

The College handles a large amount of personal data and takes seriously its responsibilities under data protection 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

[7] The University's (and therefore the College's) public interest tasks are its 'charitable objects', as laid down in Statute I: (i) 'the advancement of learning by teaching and research'; and (ii) 'its dissemination by every means'. The use of this legal basis to justify the processing of personal data for research purposes is covered in the separate University guidance for researchers on the GDPR https://researchsupport.admin.ox.ac.uk/gdpr..

[8] As a public authority, the University (and the College) cannot rely on legitimate interests for any processing it does to perform its public tasks, as outlined in (e) above. This basis would apply only to non-core activities, as opposed to teaching and research.

to:

- complying fully with data protection 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 protection 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 protection legislation and the College's data protection policy;
- providing suitable training, guidance and advice. The University's online training course on data protection and information security is available to all members of the University and College. The online course is supplemented by bespoke on-site training, where appropriate, along with regular talks and presentations at University conferences and college meetings.
- incorporating data protection 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 protection legislation; reporting it, where necessary, to the ICO; and seeking to learn any lessons from the incident in order to reduce the risk of reoccurrence.

6. Roles and responsibilities

Governing Body

Governing Body has executive responsibility for ensuring that the College complies with data protection legislation.

It is supported by the *Fellows' Meeting* and *General Purposes Committee*, which are responsible for keeping under review the College's policies and compliance with legislation and regulatory requirements.

Data Protection Officer (DPO)

The DPO is responsible for monitoring internal compliance, advising on the College's data protection obligations and acting as a point of contact for individuals and the ICO. The DPO is also responsible for:

- establishing and maintaining policies and procedures at a central level to facilitate the College's compliance with data protection legislation;
- establishing and maintaining guidance and training materials on data protection legislation and specific compliance issues;
- supporting privacy by design and privacy impact assessments;
- responding to requests for advice from staff;
- coordinating a College-wide register exercise to capture the full range of processing that is carried out;
- complying with subject access and other rights based requests made by individuals for copies of their personal data;
- 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 (and the University's Information Compliance team of any significant breaches and responding to any requests that it may make for further information.

In fulfilling these responsibilities, the DPO may also involve, and draw on support from, representatives from sections, departments and divisions.

College officers

College officers (e.g. Head of Finance, Head of Operations, Principal, Senior Tutor, College Librarian (also the College DPO), Director of Development) are responsible for ensuring that the processing of personal data in their areas of responsibility conforms to the requirements of data protection legislation and this policy. In particular, they must ensure that:

- new and existing staff, visitors or third parties associated with their area of responsible who are likely to process personal data are aware of their responsibilities under data protection legislation. This includes drawing the attention of 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 reference data protection responsibilities.
- adequate records of processing activities are kept (for example, by undertaking

register exercises);

- data protection requirements are embedded into systems and processes by adopting a 'privacy by design' approach and undertaking privacy impact assessments where appropriate;
- privacy notices are provided where data is collected directly from individuals or where data is used in non-standard ways;
- data sharing is conducted in accordance with University guidance;
- requests from the DPO 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
- departmental policies and procedures are adopted where appropriate.

Other people who may process personal data for a College purpose (e.g. staff, students and volunteers)

Anyone who processes personal data for a College purpose is individually responsible for complying with data protection legislation, this policy and any other policy, guidance, procedures, and/or training introduced by the College to comply with data protection legislation. For detailed guidance, they should refer any relevant College 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 College'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 protection legislation, in accordance with the procedure in section 6 below, and following any recommended next steps;
- seek advice from the DPO where they are unsure how to comply with data protection legislation; and
- respond promptly to any requests from the DPO in connection with subject access and other rights based requests and complaints (and forward any such requests that are received directly to the DPO immediately).

7. Breaches of data protection legislation

The College will investigate incidents involving a possible breach of data protection 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.

Data breach incidents must be reported immediately to the College's Data Protection Officer (DPO). The DPO will liaise with other key stakeholders, including the Oxford University Computer Emergency Response Team (OxCert), the University's Information Compliance team, the College's IT staff, and the College's senior management.

8. Compliance

The College regards any breach of data protection legislation, this policy or any other policy and/or training introduced by the College from time to time to comply with data protection 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 to disclose personal data unlawfully).

9. Further information

Questions about this policy and data protection matters in general should be directed to the Data Protection Officer at: data.protection@regents.ox.ac.uk.

Or by post to:

Data Protection Officer
Regent's Park College
Pusey Street
Oxford
OX1 2LB

10. Making a complaint relating to the College's use of personal data

If the College has not fully complied with this policy or in accordance with the data protection legislation, please refer to the Data Protection Officer in the first instance. The matter can also

be referred to the Information Commissioner's Office (ICO) http://ico.org.uk. The ICO is the UK's independent body set up to uphold information rights in the public interest.

11. Review and development

This policy, and supporting guidance, will apply with effect from 25 May 2018. It will be reviewed annually.

Next review date: May 2019

Version control

Version	Changes made	By	Date
1.0	Initial policy	Governing Body	May 2018
1.1	Revised to include new Data Protection act 2018 and Lawful Basis for processing. Also responsibility for maintenance and monitoring of the policy moved from GP committee to DPO.	Data Protection Officer. Approved by Governing Body 23/2/19	February 2019