Oriel College
UNIVERSITY OF OXFORD

GDPR AND DATA PROTECTION POLICY

Version: v.2
Approved by Finance and Estates Committee: 5 February 2025
Approved by Governing Body: 12 February 2025
Next review date: Michaelmas 2026

CONTENTS

A. Introduction

This policy provides a framework for ensuring that the College meets its obligations under the UK General Data Protection Regulation (UK GDPR) and the Data Protection Act (DPA) 2018.

Oriel College's compliance with data protection legislation is guided by the six data protection principles, which are outlined in **Section F: GDPR Principles**.

College employees have access to several policies, operational procedures and guidance to give them appropriate direction on the application of the data protection legislation. These policies are set out in **Section L**.

B. Scope

This policy applies to the processing of all personal data carried out by the College, including processing carried out by joint controllers, contractors, and processors.

The data processed by the College may relate to any aspect of its operational activities including, but not limited to:

- Records relating to students, alumni, staff, visitors, conference guests, and external contractors where applicable.
- Operational plans, accounting records, and minutes.
- All processing software used in support of the College's operational activities to store, process, and transmit information.
- Any information that can identify a data subject as a living natural person.

C. Information Security Classification

This policy represents an important statement of the College's satisfaction of its legal obligations, and as such will be published on the College's website.

Copies of the policy will also be available on the College's internal SharePoint resource, or from the Governance Officer (governance@oriel.ox.ac.uk).

D. Delegated Authority

The Governing Body has delegated authority for ensuring the College is GDPR and DPA compliant to the Finance and Estates Committee, which is attended by the College DPO, the Treasurer.

This policy will be reviewed and updated in line with current legislation and guidance at least every two years.

Specific responsibilities under this policy can be found at **Section H.**

E. Definition of Terms

"Personal data" and other information covered by Data Protection legislation

The UK GDPR definition of "**personal data**" includes any information relating to an identified or identifiable natural living person.

Pseudonymised personal data is covered by the legislation, however anonymised data is not regulated by the UK GDPR or DPA 2018, providing the anonymisation is irreversible.

Some personal data is more sensitive and is afforded more protection. This is defined under "Special Category Data".

"Processing"
Anything that is done with personal data, including collection, storage, use, disclosure, and deletion.

"Special Category Data"
Personal data related to:

- Race or ethnic origin.
- Political opinions.
- Religious or philosophical beliefs.
- Trade Union membership.
- Genetic Data.
- Biometric ID data for the purpose of uniquely identifying an individual.
- Health data.
- Sexual life and / or sexual orientation.
- Criminal data (convictions and offences).

The College policy on the processing of special category data is found at **Appendix A** of this policy.

"Criminal Records Data"
Information about an individual's criminal convictions and offences, and information relating to criminal allegations and proceedings.

"Controller"
The organisation (or individual) which, either alone or jointly with another organisation (or individual) decides why and how to process personal data. The Controller is responsible for compliance with the GDPR and DPA.

"Personal Data Breach"
A breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, "personal data" transmitted, stored, or otherwise processed.

"Pseudonymisation"
The processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organisational measures to ensure that the personal data is not attributed to an identified or identifiable natural person.

F. Policy Statement

GDPR Principles

The College's compliance with Data Protection legislation is guided by the seven data protection principles, which require that data:

1. Is processed fairly, lawfully, and in a transparent manner.
2. Is used only for limited, specific stated purposes, and not used or disclosed in any way incompatible with those purposes.
3. Is adequate, relevant, and limited to what is necessary.
4. Is accurate and, where necessary, up to date.
5. Is not kept for longer than necessary.
6. Is kept safe and secure.

and that the "Controller"

7. Be able to demonstrate compliance with the six principles above, otherwise known as 'accountability'.

The accountability principle requires the College to be able to evidence compliance with the above six principles and make sure that the College does not put individuals at risk when processing their personal data. Failure to do so can result in breach of legislation, reputational damage, or financial implications due to resultant fines.

To meet our obligations, the College puts in place appropriate and effective measures to make sure compliance with data protection legislation. Further information on the College's procedures can be found in **Section G**.

The following sections outline the information that the College collects about individuals and how this is processed in line with the six data protection principles.

The personal information collected

While facilitating engagement with the College, the College may obtain or generate a range of personal data about individuals.

Personal data may be received from the subject, or it may be received from colleagues, a third party such as a referee, a public source, or another organisation. Also, the College may create data itself.

It is important that the data held is accurate and correct. That College asks that data subjects keep the College informed of any changes that may be necessary during their engagement with Oriel College.

How personal information is obtained

Most of the personal information the College processes is provided directly by the individual or generated by the College in the course of its relationship with that individual.

The College also receives personal information indirectly from various sources relative to their relationship with the College.

Our legal basis for processing data

Under data protection legislation, unless an exemption applies, the College must have a 'lawful basis' for all personal data processing. There are six main legal bases, as set out below:

1. Contract

When the College holds a contract with an individual (or one is in prospect), the primary legal basis for processing personal data is that the processing is necessary for the performance of a contract with that individual; this is inclusive of student contracts and employment contracts.

2. Legal Obligation

Processing of personal data may be necessary for compliance with the College's legal and professional obligations to third parties.

3. Legitimate Interests

The College may process personal data in pursuit of legitimate interests.

For employees, the College's legitimate interests are to be an inclusive and effective employer.

For students, the College's legitimate interests are to meet the requirements of student administration, to support students' academic development and wellbeing.

For alumni, the College's legitimate interests are to ensure alumni-engagement and fundraising activities are undertaken efficiently, effectively, and with the interests of alumni in mind. Alumni relationships with the College are life-long.

4. Public Task

The College may process data in furtherance or support of specific tasks that are in the public interest. Examples include but are not limited to processing in support of the College's educational and research functions, sharing of relevant information with government and regulatory authorities where required for their own processes, and fulfilling the College's charitable objectives.

5. Vital Interests

The College may also use personal information, typically in an emergency, where this is necessary to protect vital interests, or someone else's vital interests.

6. Consent

Depending on the relationship of the individual with the College, there may be circumstances the College ask for consent to process data. For example, where the College asks individuals to volunteer information for a survey, or where they ask for permission to share sensitive information.

Consent can be withdrawn at any time, and the College will stop any processing personal data requiring consent. To do so, email dpo@oriel.ox.ac.uk with details of the request.

Our purposes for processing data

The College's overarching purpose for processing data is to fulfil its charitable mission promoting undergraduate and graduate education, research and

advanced study within the University of Oxford. Oriel provides their academic community with the facilities and pastoral support they need to excel supported by a professional operational staff. The amount of data and how far that data meets the overarching purpose will differ based on the relationship with the College. However, it is possible for the same data to be collected or generated by the College for multiple reasons and purposes, meaning that a number of available legal bases may be relevant at any given point.

If an individual has any questions regarding processes and compliance, please contact the College's DPO: dpo@oriel.ox.ac.uk .

Although the College collates, generates and processes personal information for specific purposes, on some occasions the College may wish to use that data for a new purpose. The College is permitted to do so where the new purpose is compatible with the original purpose, the College obtains consent, or the College is under a clear obligation or function set out in law.

Data Subject Rights

Under certain circumstances, by law a data subject has the right to:

- **Request access to data** (known as a "Subject Access Request"). This enables an individual data subject to receive a copy of their data to check that the College are lawfully processing it.
- **Request correction of data**. This enables a data subject to ask us to correct any incomplete or inaccurate information the College holds about them.
- **Request erasure of data**. This enables an individual to ask us to delete or remove their data under certain circumstances, for example, if they consider that there is no good reason for the College to continuing to process it. The data subject also has the right to ask the College to delete or remove data where the individual has exercised their right to object to processing (see below).
- **Object to processing of data** when the College is processing it in order to meet public interest tasks or legitimate interests (or those of a third party) and there is something about an individual's particular situation which makes them want to object to processing on this ground. The data subject also has the right to object where the College is processing personal data for direct marketing purposes.
- **Request the restriction of processing of data**. This enables the data subject to ask the College to suspend the processing of their data, for example if they want us to establish its accuracy or the reason for processing it.
- **Request the transfer of data to another party.**

Depending on the circumstances and the nature of any request it may not be possible for us to do what has been asked, for example, where there is a statutory or contractual requirement for us to process the data and it would not be possible for the College to fulfil its legal obligations if it were to stop. However, where a data subject has consented to the processing, they can withdraw consent at any time. In this event, the College will stop the processing as soon as it can. If an individual chooses to withdraw consent it will not invalidate past processing. Further information on data subject rights is available from the Information Commissioner's Office (ICO).

If an individual wants to exercise any of the rights described above or are dissatisfied with the way the College has used their information, they should

contact the College's DPO at dpo@oriel.ox.ac.uk who will seek to deal with the request without undue delay, and in any event in accordance with the requirements of the UK GDPR. Please note that the College may keep a record of communications to help us resolve any issues which are raised.

If an individual is dissatisfied with the College's processing, they also have the right to lodge a complaint with the ICO at https://ico.org.uk/concerns.

Privacy Policies

The College has published Privacy Policies concerning the management of personal data concerning non-core College members, which can be found here: https://www.oriel.ox.ac.uk/official-information-and-foi/oriel-college-data-protection-and-privacy-notice/

These policies apply to:

- Website users
- Alumni, Donors and Supporters

The College periodically review these notices and make changes clear when they occur.

G. Procedures

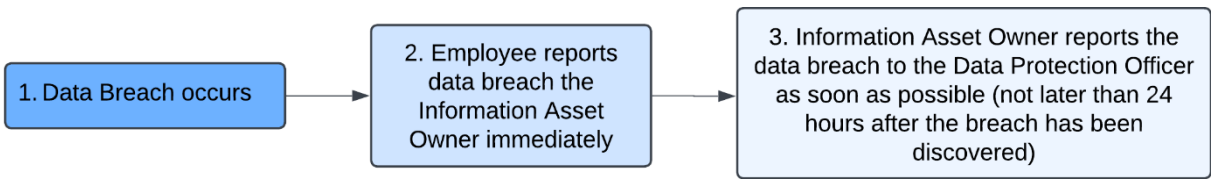
Oriel College is committed to transparent, lawful, and fair proportionate processing of personal data. This includes all personal data the College process about any member of the College community, including visitors and contractors.

The College has in place the following measures to carry through this commitment:

Data Breach Notification Procedure

The College considers personal data breach incidents and have a clear reporting mechanism to the College Data Protection Officer (DPO) that is communicated to all staff. The College assesses whether it needs to report breaches to the ICO (Information Commissioner's Office). The College takes appropriate action to make data subjects aware, if required, and take whatever action necessary to prevent similar future breaches.

All employees are required to report data breaches to their relevant Information Asset Owner immediately, who must then report to the DPO as soon as possible (and not later than 24 hours after the breach has been discovered). Employees can view a list of Information Asset Owners on the Policy SharePoint Site.



The College DPO keeps records of all data breaches and requests for information, which is shared with the Audit and Risk Committee when it convenes.

Security and Record Keeping Procedures

Information Security

The degree of security control required depends on the sensitivity or criticality of the data. The first step in determining the appropriate level of security therefore is a process of risk assessment, to identify and classify the nature of the information held, the adverse consequences of security breaches and the likelihood of those consequences occurring. All large-scale projects that involve data processing are analysed through a Data Protection Impact Assessment (DPIA); further information can be found in **Privacy by Design** below.

The risk assessment should identify the College's information assets, define the ownership of those assets, and classify them according to their sensitivity and/or criticality to the College or University as a whole. In assessing risk, the College should consider the value of the asset, the threats to that asset and its vulnerability.

Information security risk assessments should be reviewed periodically and carried out as required during the operational delivery and maintenance of the College's infrastructure, systems and processes.

Risk assessments on information assets are carried out regularly by the College's IT department and all data 'Processors' are required to comply with the College's **Information Security Policy** and **Acceptable Use Policy** when processing data. Also, the College produces and maintains a Data Asset Register recording all forms of personal data which it processes. Within this, all relevant staff members who have responsibility for specific information assets are assigned as Information Asset Owners (IAOs). The responsibilities of IAOs can be found in **Section H: Roles and Responsibilities.**

Record Keeping and Data Retention

Record Keeping refers to a set of activities required for systematically controlling the creation, distribution, use, maintenance, and disposition of recorded information maintained as evidence of the College's activities and transactions. The College's record keeping procedures ensure that personal data is used for its original purpose, or a changed purpose under relevant circumstances, and only kept as long as necessary in line with data retention procedures, to help support data minimisation.

The College retains personal data in line with the University's retention periods for staff and students. However, the periods for storage specified in it may alter depending on the requirements of law and regulation, best practice and insurance.

The College may be obliged to suspend any planned destruction or deletion under the Oxford University retention policies where legal or regulatory proceedings require it or where proceedings are underway such as require the data to be retained until those proceedings have finished. Please note that we may keep anonymised statistical data indefinitely, but individuals cannot be identified from such data.

For information on the retention of special category data, see **Appendix A**.

Privacy by Design

The College adopts a 'Privacy by Design' approach to data protection through robust procedures for data management and retention, as outlined in this policy and others mentioned in **Section L**. Additionally, the College undertake a Data Protection Impact Assessment (DPIA) before beginning the design or management of large-scale projects which involve data processing.

The assessment will include:

- Consideration of how personal data will be processed and for what purposes
- Assessment of whether the proposed processing of personal data is both necessary and proportionate to the purpose(s)
- Assessment of the risks to individuals in processing the personal data
- What control are necessary to address the identified risks and demonstrate compliance with legislation.

Use of techniques such as data minimisation and pseudonymisation will be considered where applicable and appropriate.

Transferring Data Across International Borders

The College may transfer data to other countries, which may not have the same legal protections for data as the UK.

Where data is being transferred outside of the European Economic Area, the College will take steps to ensure that data is adequately protected in accordance with legal requirements. Where the College is in a contractual relationship with the recipient, such protection will normally consist, at minimum, of appropriate contractual protections agreed between the College and the recipient.

Otherwise, the College may transfer data if, for example, it is necessary for performance of the College's contractual duties towards an individual data subject, or the College has other legal obligations to transfer the data, or it is necessary for important reasons of public interest.

If an individual requires further detail about the protections in connection with any relevant transfer, matter or jurisdiction they should email the College's Data Protection Officer: dpo@oriel.ox.ac.uk

H. Training and Responsibilities

Training

The College requires all staff to undertake mandatory training at induction on information governance and security which is retaken when required. This is provided through iHasco training courses, which can be tailored to those at management level. Staff are, also, required to complete mandatory training from the University on 'Information Security and Data Protection'.

The College's Governance Officer has undergone PDP accredited training in handling Freedom of Information requests to ensure that the College satisfies its obligations to respond to such requests, and Subject Access Requests.

Roles and Responsibilities

Data Protection Officer (DPO)

The College's data and its use is primarily overseen by the Data Protection Officer (DPO) who is the College Treasurer. The Treasurer reports to the Audit and Risk Committee with details of data breaches and information requests at least twice per calendar year.

The Treasurer follows the stipulations set out in this policy, which is reviewed at least every two years or in line with regulatory change by the Finance and Estates Committee.

Heads of Department

Heads of Department are responsible for ensuring that those in their team have appropriate training in data protection legislation, and that their team members abide by those regulatory stipulations. They assist their team when queries on the Data Breach Notification Procedure arise.

Information Asset Owners (IAOs)

Information Asset Owners (IAOs) are staff members who have responsibility for specific information assets.

Information Asset owners must:

- Maintain a log of access requests made to view the asset(s).
- Monitor as required permissions granted to transfer personal information to removable media.
- Report any breaches relating information assets they own immediately to the DPO.
- Update information assets as required, keeping a log of changes.

Information Asset owners should:

- Keep their understanding of the asset and how it is used up to date.
- Approve and minimise transfers to ensure that only as much information as is required for operational necessity is processed.
- Provide the minimum level of access required to satisfy operational needs.
- Ensure that information is archived or disposed of in line with the College's data retention policy.

I. Internal Help and Raising Concerns

Data breaches must be reported immediately (no longer than 24 hours after the relevant Information Asset owner has been notified) to the DPO, who will then carry out an investigation, and will choose the steps necessary to respond to the breach. See **Section G: Data Breach Notification Procedure** for further information.

This may involve disciplinary measures against the responsible party, notifying the data subject to whom the breach relates, and/or notifying the ICO as appropriate.

J. Consequences of Non-Observance

Punitive measures for failing to comply with this policy will be proportionate on the offence and the deliberateness with which it was carried out.

Measures range from, but are not limited to, requiring the employee to complete mandatory training, or commencing disciplinary action under the College's disciplinary procedure.

K. Further Help

Questions about this policy should be referred to the Data Protection Officer in the first instance.

By post: Data Protection Officer

Oriel College

Oriel Square

Oxford

OX1 4EW

By email: dpo@oriel.ox.ac.uk

By phone: +44 (0) 1865 276565

Current DPO: Margaret Jones, Treasurer of Oriel College.

L. Reference

This policy should be read in conjunction with the following College policies:

- Information Security Policy
- Acceptable Use Policy
- Password Security Policy
- Special Category Data Policy (**which can be found at Appendix A below**).

The College's privacy statement can be found on the college website (https://www.oriel.ox.ac.uk/official-information-and-foi/oriel-college-data-protection-and-privacy-notice/).

The College follows the collegiate University's publication scheme which is compliant with the Freedom of Information (FOI) Act and can be found here: (https://compliance.admin.ox.ac.uk/publication-scheme)

M. Policy Version Control Table

Version	Owner	Agreed by Finance and	Agreed by Governing Body	Reason for amendment	Amended by	Next review	Further notes

		Estates Committee					
v.1	Treasurer		18 June 2014	This is the original version.			v.1 was initially approved by the General Purposes Committee and encompassed within the 'Information Security' policy. Versions following this were separated from the 'Information Security Policy' due to legislation changes.
v.2	Treasurer	TBD	TBD	Scheduled review.	Governance Officer	**MT26**	

N. Appendices

Appendix A – The Processing of Special Category Data

Under the UK GDPR and DPA, additional protections for job applicants, employees, and other data subjects apply if an employer is processing "special categories" of personal data and criminal records data.

One of these protections is a requirement to have an appropriate policy document in place. This policy sets out the College's approach to processing special category personal data and criminal records data. It supplements the College's GDPR and Data Protection Policy.

Definitions which apply to this policy are the same used in the GDPR and Data Protection Policy, specified at **Section E**.

The purposes for processing special category data and criminal records data

The College processes special category personal data and criminal records data for the following purposes:

Equal opportunities monitoring

Data related to racial and ethnic origin, religious and philosophical beliefs, health (including information on whether an individual has a disability) and sexual orientation are processed for equal opportunities monitoring purposes.

Health

Data related to health (including information on whether an individual has a disability) is processed to:

- Ensure that the College is complying with its health and safety obligations.
- Assess whether an employee is fit to work.

- Carry out appropriate capability procedures if an employee is not fit for work.
- Ensure that an employee receives sick pay or other benefits to which they may be entitled.
- Allow the College to comply with its duties under the Equality Act 2010 for individuals with a disability.

Racial or Ethnic Origin

Data related to a data subject's nationality is processed to ensure that the College is complying with its obligations to check that they are entitled to work in the UK.

Criminal Records Data

Criminal Records Data is processed as part of recruitment processes and, where necessary, in the course of employment to verify that candidates are suitable for employment or continued employment and to comply with legal and regulatory obligations to which the College is subject.

The College may also undertake checks on a data subject's history with working with children where necessary as part of the safer recruitment programme under the College **Safeguarding Policy**.

Compliance with data protection principles

The College processes HR-related special category personal data and criminal records data in accordance with the following data protection principles, as outlined in **Section F: GDPR Principles** of the main policy.

(1) The College processes personal data lawfully, fairly and in a transparent manner and (2) for specified, explicit and legitimate purposes.

The College processes special category personal data and criminal records data for the purposes outlined above and in compliance with the following legal conditions for processing.

Legal basis for processing	**Special category personal data/criminal records data processing condition under sch.1 of the Data Protection Act 2018**
Equal opportunities data	
Processing is in the College's legitimate interests. These interests are not outweighed by the interests of data subjects.	Processing is necessary for monitoring equality of opportunity or treatment, as permitted by the Data Protection Act 2018 (under para.8 of sch.1).
Health data	

Processing is necessary for compliance with legal obligations (e.g. assessing an employee's fitness for work, complying with health and safety obligations, carrying out capability procedures and complying with Equality Act 2010 duties for individuals with a disability).	Processing is necessary for the purposes of performing or exercising obligations or rights imposed by law in connection with employment (under para.1 of sch.1).
Processing is necessary for the performance of a contract and/or complying with legal obligations (e.g. administering sick pay and other benefits).	Processing is necessary for the purposes of performing or exercising obligations or rights imposed by law in connection with employment (under para.1 of sch.1).
Racial or ethnic origin data	
Processing is necessary for compliance with legal obligations (e.g. checking job applicants' and employees' right to work in the UK).	Processing is necessary for the purposes of performing or exercising obligations or rights imposed by law in connection with employment (under para.1 of sch.1).
Criminal records data	
Processing is necessary for compliance with legal obligations (i.e. the College's legal requirement to carry out criminal records checks on those working with children or vulnerable adults).	Processing is necessary for the purposes of performing or exercising obligations or rights imposed by law in connection with employment (under para.1 of sch.1).

The College conducts Data Protection Impact Assessments in relation to processing operations to understand how processing may affect data subjects. The impact assessment balances the importance to the College of the reasons for processing special category personal data and criminal records data with the possible adverse impact on data subjects (for example, in relation to intrusion into an individual's private life and the impact on the duty of trust and confidence between employer and employee).

The impact assessment concluded in each case that processing is necessary and proportionate in light of the other safeguards in place and does not pose a high risk to individuals. This conclusion was endorsed by the College's Data Protection Officer.

The College explains to data subjects how special category personal data and criminal records data is used when it collects the data. This is made available to employees through the College's GDPR Data Protection Policy and the College's Staff Handbook, which is updated annually.

The College only uses such data for the purposes stated above and it reviews its processing and policies regularly to ensure that it is not using special category personal data or criminal records data for any other purpose.

Special category personal data and criminal records data are not disclosed to third parties, except in the context of seeking medical advice from the College's occupational health adviser or other medical advisers who are subject to a professional duty of confidentiality or reporting suspected offences to the appropriate authorities. The College complies with the Access to Medical Reports Act 1988 where relevant.

(3) The College processes personal data only where the data is adequate, relevant and limited to what is necessary for the purposes of processing.

The College collects and retains the minimum amount of information necessary to allow it to achieve the purposes outlined above. The impact assessment carried out in relation to each processing operation involving special category personal data and criminal records data considered data minimisation as a way of reducing the possible adverse impact of processing for individuals.

As far as possible, information required for equal opportunities monitoring purposes is kept in an anonymised form. Monitoring forms are kept under review to ensure that the information collected is accurate and not excessive.

As far as possible, the College relies on health questionnaires, rather than medical testing, to obtain necessary information. Any medical testing that is carried out is relevant to the purpose for which it is undertaken and is focused on those performing high-risk roles.

Criminal records checks are carried out only for individuals undertaking roles where the College is under a legal obligation or regulatory requirement to perform such checks or where this is necessary for the prevention or detection of unlawful acts.

(4) The College keeps accurate personal data and takes all reasonable steps to ensure that inaccurate personal data is rectified or deleted without delay.

The College takes reasonable steps to ensure that the personal data that it holds is accurate. Special category personal data and criminal records data is obtained:

- directly from job applicants, employees and other data subjects; or
- from external sources that the College is entitled to assume will provide accurate information, such as the Disclosure and Barring Service in the case of criminal records data, or medical professionals in the case of health data.

The College keeps a record of the source of all data it collects and data is reviewed periodically and checked for accuracy. Appropriate records are kept of amendments to data.

The College will erase or rectify inaccurate data that it holds without delay in line with rights of the individual as a data subject, as outlined in **Section F: Data Subject Rights** of the main policy, if an individual notifies it that their personal data has changed or is otherwise inaccurate, or if it is otherwise found to be inaccurate. Individuals are reminded to review their data on a regular basis to ensure that it remains up to date.

(5) The College keeps personal data only for the period necessary for processing.

The College has considered how long it needs to retain special category personal data and criminal records data.

It retains and processes special category personal data for the duration of an individual's employment.

The periods for which special category personal data is retained after the end of employment are as follows:

- Equal opportunities data is kept for a period of six months, after which data is anonymised so that individuals can no longer be identified.
- Racial or ethnic origin data is kept for a period of three years.
- Health data is normally kept for a period of seven years, unless statutory requirements mean that the College must keep records for longer than that.

The College does not retain details of an individual's criminal record after the commencement of employment, although it will retain a note on individual HR files indicating that a satisfactory criminal records check was completed prior to the commencement of employment. The note will be deleted at the end of the employment.

At the end of the relevant retention period, the College erases or securely destroys special category personal data and criminal records data

(6) The College adopts appropriate measures to make sure that personal data is secure and protected against unauthorised or unlawful processing, and accidental loss, destruction or damage.

The College takes the security of special category personal data and criminal records data seriously. The College has internal policies and controls in place to protect personal data against loss, accidental destruction, misuse or disclosure, and to ensure that data is not accessed, except by employees in the proper performance of their duties. The College has analysed the risk presented by processing special category personal data and criminal records data and taken this into account in assessing appropriate security requirements. Further information can be found in **Section G** of the main policy.

(7) Accountability

The College has put appropriate technical and organisation measures in place to meet accountability requirements. These include:

- appointing a Data Protection Officer (DPO)
- maintaining appropriate documentation of processing activities, specifically a register of HR-Related personal data, including special category personal data and criminal records data;
- adopting and implementing a GDPR Data Protection Policy, covering HR-related data, which is reviewed at least every two years; and
- carrying out Data Protection Impact Assessments into processing of special category personal data and criminal records data, as outlined in relation to compliance with the first data protection principle above.

Review and retention of policy and provision to Information Commissioner

This policy on processing special category personal data and criminal records data is reviewed annually and, if necessary, amended to ensure that it remains up to date and accurately reflects the College's approach to processing such data.

This policy will be retained by the College while special category personal data and criminal records data is being processed and for a period of at least six months after the College stops carrying out such processing.

A copy of this policy will be provided on request and free of charge to the Information Commissioner.

January 2025

Appendix B – The processing of children's data for Outreach activities

The College collects data from children[1] for Outreach activities. Oriel College is the "Controller" of this information and are responsible for looking after it in accordance with the UK GDPR and DPA. The data we collect depends on the Outreach activity that individual participates in.

Our purposes for processing such data

The College will use this data to register participants in the Outreach event and/or programme attended. Using data in this way is necessary for a task that the College carries out in the public interest (i.e. running events to promote access to Higher Education) and to meet the legitimate interest of promoting applications to the University.

The College will only use such data for the purposes for which it is collected, unless the College reasonably consider that it must be used for another related reason and that reason is compatible with the original purpose. If the College needs to use the data for an unrelated purpose, consent will be sought to use it for that purpose.

Who has access to the data?

Access to data within the University will be provided to those who need to view it as part of their work in carrying out the purposes described above. Access will also be provided to any third parties that we use to help organise the outreach event attended. Where the College shares data with a third party, the minimum amount necessary will be shared.

The College will add some data to the Higher Education Access Tracker database (HEAT www.heat.ac.uk), which is used to record information about Outreach activities and those who take part in them. HEAT is a shared database used by a variety of organisations to identify which activities are most helpful in preparing students for higher education and progressing to employment. Users include the University, its colleges, student organisations, educational charities and relevant public bodies (e.g. UCAS). The data collected in HEAT will depend on the Outreach activity participated in; sometimes no "personal data" is recorded. The data recorded in HEAT is done so in compliance with the University's policy.

Retaining the data

The College will only retain data for as long as it is needed to meet a lawful purpose, including relating to legal accounting or reporting requirements.

Data subject rights

Data subjects have rights related to their data. Please see **Section F: Data Subject Rights** of the main policy for further details.

[1] When we refer to a child, we mean anyone under the age of 18. This is in accordance with the UN Convention on the Rights of the Child which defines a child as everyone under 18 unless, "under the law applicable to the child, majority is attained earlier" (Office of the High Commissioner for Human Rights, 1989). The UK has ratified this convention.

Contact

If an individual wishes to raise any queries or concerns about College use of their data, please email us at outreach@oriel.ox.ac.uk or write to Outreach Officer, Oriel College, Oriel Square, Oxford, OX1 4EW.

Appendix C – Confidentiality/ Data protection agreement form for third parties

Oriel College
UNIVERSITY OF OXFORD

Confidentiality/Data Protection Agreement

I [ ] engaged as [ ] to Oriel College hereby agree that I will at all times, whether or not in the employ of Oriel College and except where such information is in the public domain:

- maintain the strictest secrecy with regard to the business affairs of the College and its customers and suppliers, except to the extent that I may be authorised or ordered to disclose them by the Governing Body of the College, a court of law, any authorised supervisory or enforcement agency (such as the police, a regulatory body given powers under the Financial Services Act or HM Revenue & Customs);
- refrain from revealing or using confidential information regarding business arrangements, systems and programme design, and data for personal gain;
- have been provided with the College's GDPR Data Protection Policy and understand my responsibilities to conform to these with regard to data provided as part of the engagement with the College

  I understand that any breach of this agreement could result in the College and its customers or suppliers sensitive and confidential data being disclosed to competitors or other interested parties.

Nothing in this agreement prevents me from making a protected disclosure within the meaning of s.43A of the Employment Rights Act 1996 reporting misconduct or a breach of any regulatory requirements to an appropriate regulator; reporting an offence to a law enforcement agency; and co-operating with a criminal investigation or prosecution.

Signed:

Print Name:

Dated: