# Worcester College Data Protection Policy

**1. Introduction**

The introduction of the General Data Protection Regulation (GDPR) in May 2018 and the Data Protection Act (DPA) 2018, the UK legislation which supplements and tailors the GDPR, recognise the importance of data in today's world. They seek to ensure that everyone's data is used properly and legally, and that people are treated fairly and openly. Worcester College handles a large amount of personal data, and we take data privacy very seriously. By not handling personal data properly, we could put students, staff and other individuals affiliated with the College at risk.

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

- 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 20 million Euros or up to 4% of global annual turnover for serious breaches

The processing of personal data underpins almost everything we do: without it, students cannot be admitted or taught; staff cannot be recruited; living individuals cannot be researched; and events cannot be organised for alumni or visitors. We have a duty to ensure that people continue to trust us with their data.

We reserve the right to make changes to this policy at any time. Where appropriate, we will notify data subjects of these changes by mail or email.

**2. Purpose**

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

**3. Scope**

This policy 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. This includes any individual acting as an officer or agent of the College in any capacity.

**4. Definitions**

*Personal data* means any information relating to an identified or identifiable natural person; an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

*Processing* means 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.

More stringent conditions apply to the processing of *special categories of personal data*, which cover personal data revealing racial or ethnic origins, political opinions, religious or philosophical beliefs, trade union membership; and the processing of genetic data, biometric data for the purpose of uniquely identifying someone, data concerning health, or data concerning an individual's sex life or sexual orientation.

*Data subjects* include all living individuals who can be identified from personal data that we hold. A data subject need not be a UK national or resident. All data subjects have legal rights in relation to their personal data.

Further information on definitions can be found at https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-law-enforcement-processing/scope-and-key-definitions/ .

**5. Aims and commitment**

Worcester College, Oxford, handles the personal data of a variety of individuals 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:

- Protecting the privacy and security of personal data
- Complying fully with data privacy legislation
- 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:

- Appointing a Data Protection Officer (DPO) to have oversight of Data Protection within College and monitor compliance with Data Protection Procedures.
- Ensuring that staff and other individuals who process data for College purposes are made aware of their individual responsibilities under data privacy legislation.
- Providing suitable training, guidance and advice.
- Incorporating the concept of 'privacy by design' into administrative processes where they involve the processing of personal data: for example, by processing the least quantity of personal data consistent with the needs of the process
- Operating a centrally coordinated procedure for the processing of subject access and other rights-based requests made by individuals.
- 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 reoccurrence.

**6. Data Protection Principles**

All processing of personal data must be conducted in accordance with the data protection principles as set out in Article 5 of the GDPR. Worcester College's policies and procedures are designed to ensure compliance with the principles.

In summary, the principles require that personal data is:

1. processed fairly, lawfully and in a transparent manner ['lawfulness, fairness and transparency']
2. used only for limited, specified stated purposes and not used or disclosed in any way incompatible with those purposes ['purpose limitation']
3. adequate, relevant and limited to what is necessary ['data minimization']
4. accurate and, where necessary, up-to-date ['accuracy']
5. not kept for longer than necessary ['storage limitation']
6. kept safe and secure ['integrity and confidentiality']

In addition, a new accountability principle requires us to be able to evidence compliance with these principles.

In order to comply with the data protection principles:

- Worcester College has published Privacy Notices and Records of Processing Activities (ROPAs), available online at https://www.worc.ox.ac.uk/about/policies-and-procedures/privacy-gdpr. Links to these official Privacy Notices should be included whenever the College collects personal data.
- Data obtained for specified purposes must not be used for a purpose that differs from those formally listed in the College's privacy notices and ROPAs.
- The Data Protection Officer will ensure that, on an annual basis, all data collection methods are reviewed to ensure that collected data continues to be adequate, relevant, and not excessive.
- Personal data will be retained in line with the Records of Processing Activities (ROPA). Once its retention date is passed, it must be securely destroyed or archived as set out in the ROPAs. Note that Worcester College may store data for longer periods if the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes, subject to the implementation of appropriate technical and organisational measures to safeguard the rights and freedoms of the data subject.
- To ensure that data is kept safe and secure, Worcester College has Information Security Policies available at http://www.worc.ox.ac.uk/about/policies-and-procedures/privacy-gdpr.
- The College will ensure that relevant staff are trained in the importance of collecting accurate data and maintaining it.
- Whenever we use a processor to handle personal data on our behalf, we will put in place a written contract that sets out each party's responsibilities and liabilities.

## 7. Data Subject Rights

Data Subjects have a number of rights including the right to erasure.

Data is stored only for as long as is necessary. For details of the College's data retention periods please refer to the Records of Processing Activities available at:
https://www.worc.ox.ac.uk/about/policies-and-procedures/privacy-gdpr

If any data subject wishes to exercise their right to erasure, they should contact the Data Protection Officer (dataprotection@worc.ox.ac.uk). Any request for erasure can be made verbally or in writing.

**8. Limitations on transferring personal data abroad**

The GDPR restricts data transfers to countries outside the European Economic Area to ensure that the level of data protection afforded to individuals by the GDPR is not undermined. Personal Data originating in one country is transferred across borders when it is transmitted, sent, viewed or accessed in or to a different country.

Personal data may only be transferred outside the EEA if one of the following conditions applies:

(a) the European Commission has issued a decision confirming that the country to which the personal data is transferred ensures an adequate level of protection for data subjects' rights and freedoms;

(b) appropriate safeguards are in place such as standard contractual clauses approved by the European Commission, an approved code of conduct or a certification mechanism;

(c) the data subject has provided their explicit consent to the proposed transfer after being informed of any potential risks; or

(d) the transfer is necessary for one of the other reasons set out in the GDPR including the performance of a contract between the College and the data subject, reasons of public interest, to establish, exercise or defend legal claims or to protect the vital interests of the data subject where the data subject is physically or legally incapable of giving consent and, in some very limited cases, for the College's legitimate interest.

**9. More detailed procedures**

Worcester College has also developed more detailed procedures on the following processes. Please consult these for more information:

**9.1 Data Protection Impact Assessment (DPIA) Procedure**

A DPIA is an essential accountability tool and a key part of taking a data protection by design approach to what we do. DPIAs will help the College identify and minimise the data protection risks of any new projects we undertake. It will help us apply the concept of 'privacy by design' to our data processing procedures. The College's DPIA Procedure is detailed at https://www.worc.ox.ac.uk/intranet/information-security .

**9.2 Data Subject Access Requests (SAR)**

Individuals have a 'right of access' to their data, i.e. a right to find out if an organisation is storing or using their personal data. People can exercise this right by asking for a copy of the data, commonly known as making a 'subject access request'. The College's Subject Access Request procedure is detailed at https://www.worc.ox.ac.uk/intranet/information-security .

**9.3 Data Breach Procedure**

Despite all our best efforts, it is possible that a personal data breach may occur. 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. The College 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.

Full information on the College's Personal Data Breach Procedure, including how to report a breach, can be found at https://www.worc.ox.ac.uk/intranet/information-security.

**9.4 Records Management**

Conformity with GDPR depends heavily on good information and records management practices, both to satisfy GDPR requirements and demonstrate compliance.

The College Archivist and Records Manager is happy to be consulted about matters relating to records management.

The Records Management Policy is available at: http://www.worc.ox.ac.uk/about/policies-and-procedures/privacy-gdpr.

**10. Roles and Responsibilities**

**Worcester College**: data controller and a data processor under the GDPR.

**The Governing Body**: responsible for ensuring that the College complies with data protection law. It designates a Data Protection Officer to monitor internal compliance.

**Data Protection Officer (DPO)**: the DPO is responsible for monitoring internal compliance, advising on the College's data protection obligations (where necessary, seeking legal advice from the College's solicitors), and acting as a point of contact for individuals and the ICO. The DPO will review data protection policies annually (or after a major incident). The DPO will investigate any data breaches in accordance with the data breach procedure.

**Data Protection Committee**: Data Protection Committee meets termly to facilitate the DPO's oversight of compliance with GDPR across College. All administrative departments are represented within the Committee and it is a forum at which reports on data breaches, subject access requests, records management and other data-related matters can be made. The Committee reports to Governing Body through the College's committee structure.

**College Officers and Heads of Department:** 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:

- 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 staff to the requirements of this policy and associated policies/procedures, 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 privacy responsibilities.
- The Register of Processing Activities (ROPA) relating to their department is checked annually and, where necessary, updated, in consultation with the College Archivist
- The College's retention schedules are implemented.
- 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
- Requests from the DPO – for example, in relation to Subject Access Requests – are responded to promptly
- Data privacy risks are considered by senior management on a regular basis; and
- Departmental policies and procedures are adopted where appropriate

**Others processing personal data for a College purpose, e.g. College staff, students and volunteers:** anyone who processes personal data for a College purpose is individually responsible for complying with data privacy legislation, reading, understanding and adhering to this policy and any other policy, guidance, procedures, and/or training introduced by the College to comply with data privacy legislation. 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 Policies available at https://www.worc.ox.ac.uk/intranet/information-security;
- Do not disclose personal data to unauthorised persons, whether inside or outside the College;
- Report promptly any suspected breaches of data privacy legislation, in accordance with the Data Breach Procedure (available at https://www.worc.ox.ac.uk/intranet/information-security);
- Seek advice from their Head of Department and/or the College's DPO where they are unsure how to comply with data privacy legislation;
- 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 Data Protection Officer by email to dataprotection@worc.ox.ac.uk); and
- Do not transfer personal data outside the European Economic Area unless one of the conditions for transfer applies.

**11. Compliance**

The College regards any breach of data privacy legislation, this policy or any other policy and/or training introduced by the College 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 to disclose personal information unlawfully).

**12. Related Policies**

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

- Privacy Policies and Registers of Processing Activities available at https://www.worc.ox.ac.uk/about/policies-and-procedures/privacy-gdpr
- Data Breach Procedure (see https://www.worc.ox.ac.uk/intranet/information-security)
- SAR Procedure (see https://www.worc.ox.ac.uk/intranet/information-security)
- DPIA Procedure (see https://www.worc.ox.ac.uk/intranet/information-security)

- Records Management Policy (see http://www.worc.ox.ac.uk/about/policies-and-procedures/privacy-gdpr)
- Information Security Policy (see http://www.worc.ox.ac.uk/about/policies-and-procedures/privacy-gdpr)
- Mobile Device Policy (see https://www.worc.ox.ac.uk/intranet/information-security)

## 13. Reference Documents

- EU GDPR 2016/679 (Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC), available online at https://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1567068513902&uri=CELEX:32016R0679
- UK Data Protection Act 2018, available online at http://www.legislation.gov.uk/ukpga/2018/12/contents/enacted
- Worcester College Privacy Notices and ROPAs, available at https://www.worc.ox.ac.uk/about/policies-and-procedures/privacy-gdpr

## 14. Validity and document management

The owner of this document is the Data Protection Officer, who must check and, if necessary, update the document at least once a year.

Questions about this policy and data privacy in general can be directed to the Data Protection Officer: dataprotection@worc.ox.ac.uk

A current version of this document is available on the College's website: http://www.worc.ox.ac.uk/about/policies-and-procedures/privacy-gdpr

## 15. Change History Record

| Version | Date | Author | Rationale |
|---|---|---|---|
| **0.1** | **August 2019** | **Mark Bainbridge** | **First draft (with comments)** |
| **0.2** | **September 2019** | **Mark Bainbridge** | **Second draft (with comments removed)** |
| **0.3** | **October 2019** | **Mark Bainbridge** | **Incorporating Data Protection Committee comments** |
| **0.4** | **October 2019** | **Mark Bainbridge** | **With lawyers' amendments** |
| **1.0** | **October 2019** | **Mark Bainbridge** | **Agreed by Governing Body, 30/10/2019** |