

# The Oxford Union Society

## Data Protection Policy

Updated August 2025

### 1. Purpose and scope

This policy provides a framework for ensuring that the Oxford Union Society meets its obligations under the General Data Protection Regulation (GDPR) and associated legislation ('data privacy legislation').

It applies to all processing of personal data carried out for the Oxford Union Society's purpose, irrespective of whether the data is processed on equipment owned by the Oxford Union Society, individual members, staff, 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 the 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 Society.

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

### 2. Background

The processing of personal data underpins much of what the Oxford Union Society ('OUS') does. Without it, the OUS cannot operate. By not handling personal data properly, we could put individuals (members, guests, staff, visitors, and others who use our facilities) at risk.

There are also legal, financial and reputational risks for the Oxford Union Society, its officers, and staff. The Information Commissioner's Office (ICO), which enforces data privacy legislation, has the power to fine organisations up to 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 on the [Information Commissioner's Office website](#).

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 evidence compliance with these principles.

### **4. Aims and commitments**

The Oxford Union Society handles a considerable amount of personal data about its members, guest speakers, and staff 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 Union seeks to achieve these aims by:

- ensuring that all senior and junior OUS officers, committee members, ordinary members, staff, and other individuals, e.g., members of the Audit Committee, or contractors who process data for OUS purposes are made aware of their individual responsibilities under data privacy legislation and how these apply to their areas of work. For example, statement of terms and conditions of employment and job descriptions include a clause drawing the attention of the employee to data privacy legislation and the Union's data protection policy and all staff and Committee members are required to read and sign a copy of this policy;
- providing suitable training, guidance and advice to enable all members and staff to discharge their responsibilities for data protection effectively;
- incorporating data privacy requirements into the OUS's administrative procedures where these involve the processing of personal data, particularly in relation to major information systems, such as the membership application

and records systems and the staff application, payroll and record systems and processes (the concept of 'privacy by design').

- providing procedures 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 reoccurrence.

## **Roles and responsibilities**

### *Standing Committee*

The OUS Standing Committee (TSC) and, in particular the President, Secretary, and Librarian, supported by the Head of Library and Collections, have executive responsibility for ensuring that the OUS complies with data privacy legislation.

TSC is supported in fulfilling its data protection duties by the OUS Audit Committee which is responsible for ensuring the effectiveness of the OUS's system of internal controls (financial and non-financial) and its processes for compliance with legislation and regulatory requirements.

### *Data Protection Officer (DPO)*

The Head of Library and Collections is the Union's Data Protection Officer (DPO).

The DPO is responsible for:

- advising the Society (members, the Society officers, and staff) on their responsibilities and obligations to comply with GDPR and other data protection legislation;
- developing appropriate policies and procedures to enable them to comply with these obligations;
- establishing and maintaining guidance and training materials on data privacy legislation and specific compliance issues;
- monitoring compliance, and acting as a point of contact for individuals and the ICO;
- maintaining an OUS-wide register of data processing activity and ensuring that all those who control or process personal data are aware of their responsibilities;
- supporting privacy by design and privacy impact assessments;
- ensuring that subject access and other rights-based requests made by individuals for copies of their personal data are fulfilled;
- 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.

In fulfilling these responsibilities, the DPO may also involve and draw on support from its members, staff, and appropriate external advisers.

All OUS Committee members, senior and junior officers, the Head of Library and Collections, administrative staff (including the Membership Secretary, the Accountant, the Head of Library and Collections, and Events Manager) and all other staff whose work involves the processing of personal data are responsible for ensuring that the processing of personal data in their department or area of responsibility 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 OUS who are likely to process personal data are aware of their responsibilities under data privacy legislation. This includes drawing the attention of new Committee members and all staff to the requirements of this policy, ensuring that those 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;
- records of processing activities are kept (including consulting the Head of Library and Collections/Data Protection Officer if it is proposed to create a new processing activity or significantly change an existing electronic or paper one; all such information assets and data processing activity must be included on the OUS Information Asset register);
- 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 College and University guidance;
- requests from the Data Protection Officer for information are complied with promptly;
- data privacy risks are included in the Society's risk management framework and considered by senior management on a regular basis; and
- policies and procedures to ensure compliance with GDPR and data protection obligations are adopted where appropriate.

*Others processing personal data for an OUS purpose e.g., staff, Committee and ordinary members of the society*

Anyone who processes personal data for an OUS purpose is individually responsible for complying with data privacy legislation, this policy and any other policy, guidance,

procedures, and/or training introduced by the OUS to comply with data privacy legislation. They should refer to the [ICO Guidance on Data Protection](#) and any relevant OUS 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 Oxford Union's Information Security Policy;
- do not disclose personal data to unauthorised persons, whether inside or outside the Society;
- 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 Data Protection Officer where they are unsure how to comply with data privacy legislation; and
- promptly respond to any requests from the Data Protection Officer in connection with subject access and other rights-based requests and complaints.

## **Breaches of data privacy legislation**

The OUS 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.

Incidents involving failures of IT systems or processes must be reported immediately to the Head of Library and Collections on 01865-246782 and [tom.corrick@oxford-union.org](mailto:tom.corrick@oxford-union.org). The Head of Library and Collections or his deputy will liaise, as appropriate, with the OUS computer support providers and OUS senior and junior officers.

## **6. Compliance**

OUS regards any breach of data privacy, this policy or any other policy and/or training provided by it 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 Society or its staff to disclose personal information unlawfully).

### **7. Further information**

Questions about this policy and data privacy matters in general should be directed to the Society's Data Protection Office, the Head of Library and Collections, [tom.corrick@oxford-union.org](mailto:tom.corrick@oxford-union.org)

### **8. Review and development**

This policy, and supporting guidance, will apply with effect from March 2023.

### **9. Related policies, Privacy Notices, and Records of Processing Activities**

This policy should be read in conjunction with the related policies and regulations which can be found on our website or requested from [tom.corrick@oxford-union.org](mailto:tom.corrick@oxford-union.org)

ENDS