

DATA PROTECTION POLICY FOR GENERAL USERS of the Oxford Centre for Mission Studies (OCMS):

1 Overview

- 1.1 We take the security and privacy of your data seriously. We need to gather and use information or 'data' about you as part of our business and to manage our relationship with you. We intend to comply with our legal obligations under the EU General Data Protection Regulation ('GDPR') in respect of data privacy and security. We have a duty to notify you of the information contained in this policy.
- 1.2 This policy applies to current & prospective general users of OCMS which includes but is not restricted to those who receive communications from OCMS, supporters, alumni, contractors, those who purchase books through our imprint, Regnum Books, and any who make contact with us. If you fall into one of these categories, then you are a 'data subject' for the purposes of this policy.
- 1.3 We will only hold data for as long as necessary and for the purposes for which we collected it. Further information on how long we hold data on our general users is contained below.
- 1.4 OCMS is a 'data controller' for the purposes of your personal data, which means that we determine the purpose and means of the processing of your personal data.
- 1.5 This policy explains how we will hold and process your information. It explains your rights as a data subject. It also explains your obligations when obtaining, handling, processing or storing personal data in the course of working for, or on behalf of us.
- 1.6 This policy may be amended at any time. It is intended that this policy is fully compliant with GDPR. If any conflict arises between GDPR and this policy, we intend to comply with GDPR.

2 Personal data

- 2.1 'Personal data' means information which relates to a living person who can be identified from that data (a 'data subject') on its own, or when taken together with other information which is likely to come into our possession. It includes any expression of opinion about the person and an indication of the intentions of us or others, in respect of that person. It does not include anonymised data.
- 2.2 This policy applies to all personal data whether it is stored electronically, on paper or on other materials.
- 2.3 This personal data might be provided to us by you, or someone else (such as a conference organiser), or it could be created by us.

2.4 We may collect and use the following types of personal data about you:

- your contact details and date of birth;
- the contact details for your emergency contacts;
- your gender;
- your marital status and family details;
- your bank details and information, credit card numbers, financial information required for payment;
- your images (whether captured by photograph or video); and
- any other category of personal data which we may notify you of from time to time.

3 Sensitive personal data

3.1 'Sensitive personal data' are types of personal data consisting of information as to:

- your racial or ethnic origin;
- your political opinions;
- your religious or philosophical beliefs;
- your trade union membership;
- your genetic or biometric data;
- your health;
- your sex life and sexual orientation; and
- any criminal convictions and offences.

We may hold and use sensitive personal data in accordance with the law.

4 Data Protection Principles

4.1 Personal data must be processed in accordance with six 'Data Protection Principles.' It must:

- be processed fairly, lawfully and transparently;
- be collected and processed only for specified, explicit and legitimate purposes;
- be adequate, relevant and limited to what is necessary for the purposes for which it is processed;
- be accurate and kept up to date. Any inaccurate data must be deleted or rectified without delay;
- not be kept for longer than is necessary for the purposes for which it is processed (see 4.2 below); and
- be processed securely.

We are accountable for these principles and must be able to show that we are compliant.

4.2 General users' personal data will be retained for no longer than necessary. There are statutory requirements to keep certain general user records for a minimum length of time, as follows:

Nature of data	Minimum length of time to be retained
<p>One time purchase payments:</p> <ul style="list-style-type: none"> • Your name and contact details and any details required to make payments for one time purchases (e.g., Regnum) 	Deleted as soon as no longer necessary
<p>Donors:</p> <ul style="list-style-type: none"> • Donor name, contact details, securely stored electronically with access by finance and development officers only • Gift amounts • Fund to which donation was earmarked • Information for requested tax receipts • Due diligence to ensure money was not obtained through criminal activity, etc. 	Permanently
<p>For conference participants:</p> <ul style="list-style-type: none"> • Name, contact details, payment details • information about your health, dietary requirements and/or disabilities, and records of decisions we make taking that information into account. • Emergency contact details • List of participants • Accommodation bookings • Records of OCMS life: photographs from chapel, RIS, lectures, seminars, event recordings, etc. • Consent will be obtained for any pictures used for publication. 	<p>One year for participants who opt out of further communication from OCMS, six years for organisers</p> <p>Permanently in the archive</p>
<p>All users:</p> <ul style="list-style-type: none"> • Records generated for legal or statutory compliance purposes that 	7 years

<p>contain names and/or associated personal data. For example, copies of data supplied pursuant to requests made under data protection and/or freedom of information legislation, records made to comply with safeguarding, health and safety or counter-terrorism legislation, in connection with legal advice or claims, or to comply with auditor's requirements</p>	
<ul style="list-style-type: none"> • Emails for those who have consented to be on mailing lists 	<p>Until a request is received to unsubscribe, in which case details are removed immediately</p>
<ul style="list-style-type: none"> • Computer and email information, including guest login, username and password information, IP addresses of devices you connect to College IT systems, details of when you connected or logged in to our network, and records of internet usage. 	<p>Records destroyed one year after cessation of IT system use.</p>

5 Processing

5.1 'Processing' means any operation which is performed on personal data such as:

- collection, recording, organisation, structuring or storage;
- adaption or alteration;
- retrieval, consultation or use;
- disclosure by transmission, dissemination or otherwise making available;
- alignment or combination; and
- restriction, destruction or erasure.

This includes processing personal data which forms part of a filing system and any automated processing.

6 How we process your personal data

6.1 We will process your personal data (including sensitive personal data) in accordance with our obligations under the law.

6.2 We will use your personal data for:

- performing any contract between us;
- complying with any legal obligation; or
- if it is necessary for our legitimate interests (or for the legitimate interests of someone else). However, we can only do this if your interests and rights do not override ours (or theirs). You have the right to challenge our legitimate interests and request that we stop this processing.

6.3 We can process your personal data for these purposes without your knowledge or consent. We will not use your personal data for an unrelated purpose without telling you about it and the legal basis that we intend to rely on for processing it.

6.4.1 If you choose not to provide us with certain personal data, you should be aware that we may not be able to carry out certain parts of the contract between us. For example, if you do not provide us with your bank account details or credit card payment, we may not be able to accept your payment and you may not be able to attend a conference, be booked for accommodation, or complete a purchase.

6.4.2 We will take reasonable steps to ensure that any personal data processed is accurate and up to date. To assist us in this, we ask that you inform us of any changes to the personal data you have supplied during the course of your tenure as a general user.

7 Examples of when we might process your personal data

7.1 We have to process your personal data in various situations during your recruitment, tenure as a general user, and even following the end of your studies, for example:

- to carry out the contract between us including where relevant, its termination;
- to process payments for purchase or donation;
- to email you newsletters and updates if you have subscribed to them;
- to determine what adjustments we may need to make to accommodate your health, disability, and dietary requirements;
- to monitor and protect the security (including network security) of the organisation, of you, our other staff, customers and others;
- to monitor and protect the health and safety of you, our other staff, customers and third parties;
- monitoring compliance by you, us and others with our policies and our contractual obligations;
- the prevention and detection of fraud or other criminal offences;
- to defend us in respect of any investigation or litigation and to comply with any court or tribunal orders for disclosure;

- for any other reason which we may notify you of from time to time.

7.2 We will only process sensitive personal data in certain situations in accordance with the law. For example, we can do so if we have your explicit consent. If we ask for your consent to process sensitive personal data, then we will explain the reasons for our request. You do not need to consent and can withdraw consent later if you choose by contacting the Data Protection Officer.

7.3 We do not need your consent to process sensitive personal data when we are processing it for the following purposes:

- where it is necessary for carrying out rights and obligations under law;
- where it is necessary to protect your vital interests or those of another person where you/they are physically or legally incapable of giving consent;
- where you have made the data public;
- where processing is necessary for the establishment, exercise or defence of legal claims; and
- where processing is necessary for the purposes of occupational medicine or for the assessment of your working capacity.

8 Sharing your personal data

8.1 Sometimes we might share your personal data with our contractors and agents to carry out our obligations under our contract with you or for our legitimate interests. For example, to complete a purchase, book a conference or accommodation.

8.2 We require those companies who we share your personal data with to keep your personal data confidential and secure and to protect it in accordance with the law and our policies. They are only permitted to process your data for the lawful purpose for which it has been shared and in accordance with our instructions.

8.3 If we receive a request from a third party for your personal data for a reason not related to our contractual, statutory, or management obligations (such as another educational institution or a job provider), we will notify you and will only disclose information to these third parties with your consent.

8.4 We do not send your personal data outside the European Economic Area, save for the names and photographs of some general users and staff on brochures advertising OCMS in other parts of the world. If this changes you will be notified of this and the protections which are in place to protect the security of your data will be explained.

9 Data breaches

9.1 A data breach may take many different forms, for example:

- loss or theft of data or equipment on which personal information is stored;
- unauthorised access to or use of personal information either by a member of staff or third party;
- loss of data resulting from an equipment or systems (including hardware and software) failure;
- human error, such as accidental deletion or alteration of data;
- unforeseen circumstances, such as a fire or flood;
- deliberate attacks on IT systems, such as hacking, viruses or phishing scams;

9.2 We have robust measures in place to minimise and prevent data breaches from taking place. Should a breach of personal data occur, OCMS will take notes and keep evidence of the breach. If the breach is likely to result in a risk to the rights and freedoms of individuals, then we will notify the Information Commissioner's Office within 72 hours.

10 Subject access requests

10.1 Data subjects can make a 'subject access request' ('SAR') to find out the information we hold about them. This request must be made in writing. If you receive such a request you should forward it immediately to the Data Protection Officer who will coordinate a response.

10.2 If you would like to make a SAR in relation to your own personal data, you should make this in writing to the Data Protection Officer. We must respond within one month unless the request is complex or numerous in which case the period in which we must respond can be extended by a further two months.

10.3 There is no fee for making a SAR. However, if your request is manifestly unfounded or excessive, we may charge a reasonable administrative fee or refuse to respond to your request.

11 Your data subject rights

11.1 You have the right to information about what personal data we process, how and on what basis as set out in this policy.

11.2 You have the right to access your own personal data by way of a subject access request (see above).

11.3 You can correct any inaccuracies in your personal data. To do so you should contact the Data Protection Officer.

- 11.4 You have the right to request that we erase your personal data where we were not entitled under the law to process it or it is no longer necessary to process it for the purpose it was collected. To do so you should contact the Data Protection Officer.
- 11.5 While you are requesting that your personal data is corrected or erased or are contesting the lawfulness of our processing, you can apply for its use to be restricted while the application is made. To do so you should contact the Data Protection Officer.
- 11.6 You have the right to object to data processing where we are relying on a legitimate interest to do so and you think that your rights and interests outweigh our own and you wish us to stop.
- 11.7 You have the right to object if we process your personal data for the purposes of direct marketing.
- 11.8 You have the right to receive a copy of your personal data and to transfer your personal data to another data controller. We will not charge for this and will in most cases aim to do this within one month.
- 11.9 With some exceptions, you have the right not to be subjected to automated decision-making.
- 11.10 You have the right to be notified of a data security breach concerning your personal data.
- 11.11 In most situations, we will be relying on contract or consent as lawful grounds to process your data. If we do request your consent to the processing of your personal data for a specific purpose, you have the right not to consent or to withdraw your consent later. To withdraw your consent, you should contact the Data Protection Officer.
- 11.12 You have the right to complain to the Information Commissioner. You can do this by contacting the Information Commissioner's Office directly. Full contact details including a helpline number can be found on the Information Commissioner's Office website (www.ico.org.uk). This website has further information on your rights and our obligations.