Data Protection Policy

Contents

1. Introduction

Data Protection Legislation is concerned with the protection of human rights in relation to personal data. The aim of the Legislation is to ensure that personal data is used fairly and lawfully and that where necessary the privacy of individuals is respected. During the course of the activities of OCMS (the 'Charity'), the charity will collect, store and process personal data about our members, people who attend our services and activities, employees, suppliers and other third parties and we recognise that the correct and lawful treatment of this data will help maintain confidence in the charity. This policy sets out the basis on which we will process any personal data we collect from data subjects, or that is provided to us by data subjects or other sources.
The Data Protection Officer (DPO) is responsible for ensuring compliance with the Legislation and with this policy. The post is held by the Chief Operations Officer. Any questions about the operation of this policy or any concerns that the policy has not been followed should be referred in the first instance to the DPO.
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 UK General Data Protection Regulation ('UK GDPR') and the Data Protection Act 2018 ('the Act') in respect of data privacy and security. We have a duty to notify you of the information contained in this policy.
This policy applies to current and former employees, workers, volunteers, students, scholars, apprentices, consultants and donors. If you fall into one of these categories then you are a 'data subject' for the purposes of this policy. You should read this policy alongside your contract of employment, if relevant, and any other notice we issue to you from time to time in relation to your data.
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 employees is contained below. Oxford Centre for Mission Studies is a 'data controller' for the purposes of your personal data. This means that we determine the purpose and means of the processing of your personal data.

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.
This policy may be amended at any time. It is intended that this policy is fully compliant with UK GDPR and the Act. If any conflict arises between UK GDPR or the Act and this policy, we intend to comply with UK GDPR and the Act.

2. Processing Personal Data

All personal data should be processed in accordance with the Legislation and this policy. Any breach of this policy may result in disciplinary action.
Processing includes obtaining, holding, maintaining, storing, erasing, blocking and destroying data.
Personal data is data relating to a living individual. It includes employee data. It will not include data relating to a company or organisation, although any data relating to individuals within companies or organisations may be covered. Personal data can be factual (for example a name, address or date of birth) or it can be an opinion about that person, their actions and behaviour.
Examples of personal data are employee details, including employment records, names and addresses and other information relating to individuals, including supplier details, any third-party data and any recorded information including any recorded telephone conversations, emails or CCTV images. This personal data might be provided to us by you, or someone else (such as a former employer, your doctor, or a credit reference agency), or it could be created by us. It could be provided or created during the recruitment process or during the course of the contract of employment (or services) or after its termination. It could be created by your manager or other colleagues.
Employees and others (including volunteers and trustees) who process data on behalf of the charity (referred to in this policy as 'Employees') should assume that whatever they do with personal data will be considered to constitute processing.
Employees should only process data:

- If they have consent to do so; or
- If it is necessary to fulfil a contractual obligation or as part of the employer/employee relationship; for example, processing the payroll; or
- The processing is necessary for legitimate interests pursued by OCMS unless these are overridden by the interests, rights and freedoms of the data subject.

If none of these conditions are satisfied, individuals should contact the DPO before processing personal data.
This policy applies to all personal data whether it is stored electronically, on paper or on other materials.

3. Compliance with the Legislation

Employees who process data on our behalf have a responsibility for processing personal data in accordance with the Legislation. This includes the data protection principles in the Legislation. These state that personal data must:

- be obtained and used fairly, lawfully and transparently
- be obtained for specified, explicit and legitimate purposes and used only for those purposes
- be adequate, relevant and limited to the minimum necessary for those purposes
- be accurate and kept up to date (every reasonable endeavour should be used to ensure that personal data that is not accurate is corrected or erased without delay)
- be processed in a manner that ensures its security (see section regarding Information Security)

- not be kept for any longer than required for those purposes (see section regarding Retention)

We will only share personal data with other organisations or people when we have a legal basis to do so and if we have informed the data subject about the possibility of the data being shared (in a privacy notice) unless there is a legal exemption from doing so. We will keep records of any information shared with a third party including a record of any exemption which has been applied. Employees should follow the Data Breach Procedure if they think they have accidentally breached any provision of this Data Protection Policy.

4. Special Category Data

We will strive to ensure that special category data is accurately identified on collection so that proper safeguards can be put in place. Special category data means data consisting of information relating to an individual's

- Racial or ethnic origin
- Political opinions
- Religious or philosophical beliefs
- Trade union membership
- Physical or mental health, biometric and genetic information
- Sex life or sexual orientation

Although not technically special category data, we treat data relating to criminal offences similarly. Special category data may be processed in the course of our legitimate activities, but may not be passed to any third party without the express consent of the data subject.

5. Monitoring the use of personal data

We are committed to ensuring that this data protection policy is put into practice and that appropriate working practices are being followed. To this end the following steps will be taken:

- Any Employees who deal with personal data are expected to be aware of data protection issues and to work towards continuous improvement of the proper processing of personal data;
- Employees who handle personal data on a regular basis or who process special category or other confidential personal data will be more closely monitored;
- All Employees must consider whether the personal data they hold is being processed in accordance with this policy. Particular regard should be had to ensure inaccurate, excessive or out of date data is disposed of in accordance with this policy;
- Employees must follow the Breaches Procedure should they become aware of any breach of this policy;
- Employees will keep clear records of our processing activities and of the decisions we make concerning personal data (including reasons for the decisions) to show how we comply with the Legislation;
- Spot checks may be carried out;
- An annual report on the level of compliance with or variance from good data protection practices will be produced by the COO.
- Data breaches will be recorded and investigated to see what improvements can be made to prevent recurrences;
- We will only appoint data processors on the basis of a written contract that will require the processor to comply with all relevant legal requirements. We will continue to monitor the data processing, and compliance with the contract, throughout the duration of the contract.

6. Sharing your personal data

We will share your personal data with statutory bodies and government agencies (such as HMRC) as required by law. Examples include information relating to salary, tax, national insurance contributions, pension contributions and right to work in the UK. 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, personal data required to process payroll may be provided to our accountants and pension provider.
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.
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 from a mortgage provider), we will notify you and will only disclose information to these third parties with your consent.
We do not send your personal data outside the United Kingdom or the European Economic Area except that we may transfer personal data for the purposes of cloud storage only to a country and organisation that is designated as having an adequate level of protection. 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.

7. The rights of individuals

The Legislation gives individuals certain rights to know what data is held about them and what it is used for. If personal data is collected directly from an individual, we will inform them in writing of their rights by providing them with a 'Privacy Notice' at the time the personal data is collected or as soon as possible afterwards.
In principle everyone has the right to see copies of all personal data held about them. There is also a right to have any inaccuracies in data corrected or erased. Data subjects may also have a right of portability in respect of their personal data, and a right to be forgotten. Data subjects also have the right to prevent the processing of their data for direct marketing purposes.
Any request for access to data under the Legislation should be made to DPO in writing. In accordance with the Legislation we will ensure that written requests for access to personal data are complied with within one calendar month of receipt of a valid request (where permitted under the Legislation, we may take a further two calendar months to respond but we will inform the individual of why this is necessary).
When a written data subject access request is received the data subject will be given a description of a) the personal data, b) the purposes for which it is being processed, c) those people and organisations to whom the data may be disclosed, d) be provided with a copy of the information in an intelligible form.

8. Information Security

Information security involves preserving confidentiality, preventing unauthorised access and disclosure, maintaining the integrity of information, safeguarding accuracy and ensuring access to information when required by authorised users. 'OCMS data' means any personal data processed by or on behalf of OCMS. Information security is the responsibility of every member of staff, trustee, office holder, and volunteer using OCMS data on but not limited to the OCMS information systems.
Our IT systems may only be used for authorised purposes. We will monitor the use of our systems from time to time. Any person using the IT systems for unauthorised purposes may be subject to disciplinary and/or legal proceedings.

We will take appropriate technical and organisational steps to guard against unauthorised or unlawful processing. In particular:

- All data will be stored in a secure location and precautions will be taken to avoid data being accidentally disclosed.
- Manual records relating to OCMS staff or the wider OCMS community will be kept secure in locked cabinets. Access to such records will be restricted.
- Access to systems on which information is stored must be password protected with strong passwords and these should be changed at once if there is a risk they have been compromised. Passwords must not be disclosed to others.
- We will ensure that staff and members who handle personal data are adequately trained and monitored to ensure data is being kept secure.
- We will ensure that only those who need access will have access to data.
- We will take particular care of sensitive data and security measures will reflect the importance of keeping sensitive data secure (definition of sensitive data is set out above in the Data Protection Policy), e.g. password protection for documents and encryption.
- Where personal data needs to be deleted or destroyed adequate measures will be taken to ensure data is properly and securely disposed of. This will include destruction of files and back up files and physical destruction of manual files. Particular care should be taken over the destruction of manual sensitive data (written records) including shredding or disposing via specialist contractors (who will be treated as data processors -see below).
- We will ensure that any data processor engaged to process data on our behalf (e.g. for payroll) will act under a written contract and will give appropriate undertakings as to the security of data.
- Appropriate software security measures will be implemented and kept up to date.
- We will ensure that if information has to be transported or transferred, this is done safely using encrypted devices or services.
- Where personal devices are used to store or process personal data, they must be subject to appropriate security.

9. Retention of Records

All data and records will be stored in accordance with the security requirements of the Data Protection Legislation and in the most convenient and appropriate location having regard to the period of retention required and the frequency with which access will be made to the record. Data and records which are active should be stored in the most appropriate place for their purpose commensurate with security requirements.

Data and records which are no longer active, due to their age or subject, should be stored in the most appropriate place for their purpose or destroyed. The degree of security required for file storage will reflect the sensitivity and confidential nature of any material recorded. Any data file or record which contains personal data of any form can be considered as confidential in nature. Data and records should not be kept for longer than is necessary. This principle finds statutory form in the Data Protection Legislation, which requires that personal data processed for any purpose "shall not be kept for longer than is necessary for that purpose". All staff, trustees, volunteers are required to have regard to the Guidelines for Retention of Personal Data below. Any data that is to be disposed must be safely disposed of for example by shredding. Any group which does not have access to a shredder should pass material to the Finance manager who will undertake secure shredding. Special care must be given to disposing of data stored in electronic media. Guidance will be given by the DPO to any group which has stored personal data relating to its members on for example personal computers which are to be disposed of.

If you have any queries regarding retaining or disposing of data please contact the DPO. Please refer to the Appendix for the Data Retention Schedule.

10. Data Breaches

OCMS holds and processes personal data which needs to be protected. Every care is taken to protect the data we hold. Compromise of information, confidentiality, integrity or availability may result in harm to individuals, reputational damage, detrimental effect on service provision, legislative non-compliance and financial penalties.

a. Types of breach

An incident is an event or action which may compromise the confidentiality, integrity or availability of systems or data, either accidentally or deliberately, and has caused or has the potential to cause damage to data subjects.

An incident includes but is not restricted to:

- Loss or theft of personal data or the equipment on which the data is stored e.g. laptop, memory stick, smartphone, or paper record
- theft or failure of equipment on which personal data is stored
- Unauthorised use of or access to personal data
- Attempts to gain unauthorised access to personal data
- Unauthorised disclosure of personal data
- Website defacement
- Hacking attack

b. Reporting an incident

Any person using personal data on behalf of OCMS is responsible for reporting data breach incidents immediately to the DPO or in his or her absence the Executive Director. The report should contain the following details:

- Date and time of discovery of breach
- Details of person who discovered the breach
- The nature of the personal data involved
- How many individuals' data is affected

c. Containment and recovery

The DPO will first ascertain if the breach is still occurring. If so, appropriate steps will be taken immediately to minimise the effects of the breach. An assessment will be carried out to establish the severity of the breach and the nature of further investigation required. Consideration will be given as to whether the police should be informed. Advice from appropriate experts will be sought if necessary. A suitable course of action will be taken to ensure a resolution to the breach.

d. Investigation and risk assessment

An investigation will be carried out without delay and where possible within 24 hours of the breach being discovered. The DPO will assess the risks associated with the breach, the potential consequences for the data subjects, how serious and substantial those are and how likely they are to occur.

The investigation will take into account the following:

- The type of data involved and its sensitivity
- The protections in place (e.g. encryption)
- What has happened to the data
- Whether the data could be put to illegal or inappropriate use
- Who the data subjects are, how many are involved, and the potential effects on them
- Any wider consequences

e. Notification

The DPO will decide with appropriate advice who needs to be notified of the breach. Every incident will be assessed on a case by case basis. The Information Commissioner will be notified, if

at all possible within 24 hours of the data breach, if a large number of people are affected or the consequences for the data subjects are very serious. Guidance on when and how to notify the ICO is available on their website
https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/personal-data-breaches/
Where appropriate, we will notify the data subjects whose personal data has been affected by the incident; such a notification may include a description of how and when the breach occurred, and the nature of the data involved, and specific and clear advice on what they can do to protect themselves and what has already been done to mitigate the risks.
The DPO will keep a record of all actions taken in respect of the breach.

f. Evaluation and response

Once the incident is contained, the DPO will carry out a review of the causes of the breach, the effectiveness of the response, and whether any changes to systems, policies or procedures should be undertaken. Consideration will be given to whether any corrective action is necessary to minimise the risk of similar incidents occurring.

11. Subject Access Requests

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 Chief Operating Officer who will coordinate a response.
If you would like to make a SAR in relation to your own personal data you should make this in writing to the Chief Operating 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.
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.

12. Your data subject rights

You have the right to information about what personal data we process, how and on what basis as set out in this policy.
You have the right to access your own personal data by way of a subject access request (see above). You can correct any inaccuracies in your personal data. To do so you should contact the Chief Operating Officer. 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 Chief Operating Officer. 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 Chief Operating Officer.
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. You have the right to object if we process your personal data for the purposes of direct marketing.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. With some exceptions, you have the right not to be subjected to automated decision-making. You have the right to be notified of a data security breach concerning your personal data.In most situations we will not rely on your consent as a lawful ground to process your data. If we do however

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 Chief Operating Officer. 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.

13. Data Protection Complaints Process

OCMS takes your privacy concerns seriously. If you have any concerns about the way your information is being handled, please contact the DPO.
We will carefully investigate and review all complaints and take appropriate action in accordance with Data Protection Legislation. We will keep you informed of the progress of our investigation and the outcome. If you are not satisfied with the outcome, you may wish to contact the Information Commissioner's Office at https://ico.org.uk/concerns/
Any complaint received by us must be referred to the DPO who will arrange for an investigation as follows:

- A record will be made of the details of the complaint.
- Consideration will be given as to whether the circumstances amount to a breach of Data Protection Legislation and action taken in accordance with the Data Breach Procedure.
- The complainant will be kept informed of the progress of the complaint and of the outcome of the investigation.
- At the conclusion of the investigation the DPO will reflect on the circumstances and recommend any improvements to systems or procedure

14. Changes to this policy

We reserve the right to change this policy at any time, including as needed to comply with changes in law. Where appropriate we will notify data subjects of those changes by mail or email.

Revision History

Version	Date	Written by/Updated by	Approved by	Comments
1.0	11/21	DB	OCMS	
1.1	01/24	MC	SMT	Minor updates and formatting
1.2	03/25	MC	SMT	Minor updates and formatting

Appendix 1: Data Retention Schedule

Data Retention Schedule
(NB this is not an exhaustive list)

Employees/Volunteers

Type of Data	*Retention Period*
Personnel files including: training records, notes of disciplinary and grievance hearings, complaints	6 years from the end of employment. After this, only name, role history, contact details will be retained permanently.
Application forms, CV, References, Interview notes	Maximum of one year from the date of the interviews for those not subsequently employed. If employed, retain in personnel file.
Income Tax and NI returns, including correspondence with tax office	At least 6 years after the end of the financial year to which the records relate
Statutory Maternity Pay records and calculations	As Above (Statutory Maternity Pay (General) Regulations 1986)
Statutory Sick Pay records and calculations	As Above Statutory Sick Pay (General) Regulations 1982
Wages and salary records	6 years from the tax year in which generated
Accident books, and records and reports of accidents	3 years after the date of the last entry
Health records	6 months from date of leaving employment (Management of Health and Safety at Work Regulations)
Health records where reason for termination of employment is connected with health, including stress related illness	3 years from date of leaving employment (Limitation period for personal injury) claims)
Personal information relating to any safeguarding concern	25 years from the end of employment
Records generated for legal or statutory compliance purposes that 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	6 years
Emails for those who have consented to be on mailing lists	Permanently until a request is received to unsubscribe, in which case details are removed immediately
Emails, username and password information, details of when you connected or logged in to our network, and records of internet usage.	Records destroyed one year after cessation of IT system use

Students

Type of Data	*Retention Period*
Student Record file: Attendance, Identity documents, progression, Exam results, scholarships, personal details, conduct, including any records of complaints	6 years from the date the student leaves in case of litigation for negligence
Financial information	Records of outstanding payments will be held until they are paid off or a payment plan is agreed. Otherwise, financial information will be held for 6 years.
Information about ethnicity, gender, health, religion or philosophical beliefs and/or sexuality processed for the purposes of identifying or keeping under review the existence or absence of equality of opportunity or treatment, with a view to enabling such equality to be promoted or maintained	Permanently
Information submitted as part of the application process including name, address, gender, marital status, religion, degrees obtained, results of your interview	6 Months after being awarded degree or finished programme
Details of any criminal records that you declare to us on your application, or during your studies, or of any criminal incidents or allegations concerning you reported to us by anyone else, so OCMS may maintain a safe environment.	Where criminal convictions, incidents or allegations are declared or reported to us, we will retain this data permanently.
Details of any Disclosure and Barring Service Checks about you obtained prior to or during your studies	Where we require a Disclosure and Barring Service check to be carried out, we will retain the DBS certificate information for 6 months from the date the certificate is received and a skeleton record that the check was satisfactory or unsatisfactory will be kept on the file for 6 years after the student leaves
Accident books, and records and reports of accidents	3 years after the date of the last entry
Personal information relating to any safeguarding concern	25 years

External Contacts

Type of Data	*Retention Period*

One time purchase payments: Name and contact details and any details required to make payments for one time purchases (e.g. Regnum)	6 years
Regnum: ● Author CVs, other general information ● Customer data (stored in Xero) ● Book endorsers, contributors and book reviewers ● Online sales information (Shopify)	6 years for CVs; other information indefinitely
Donors: ● Donor name, contact details, 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.	6 Years following last donation, unless requested earlier
For conference participants: ● Name, contact details, payment details ● information about 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	6 years for participants, unless requested earlier
Emails for those who have consented to be on mailing lists	Permanently until a request is received to unsubscribe, in which case details are removed immediately

Company Records

Type of Data	*Retention Period*
Memorandum and articles of association (signed original)	Permanently
Accounting records Financial Information on income / expenditure / balance sheet	6 years from the date on which the record was made Indefinitely
Council of Trustees Minutes	Permanent

Appendix 2 - Privacy Notice

Oxford Centre for Mission Studies (OCMS) Privacy Notice

How OCMS ("we") use your information
Your privacy is important to us. We are committed to safeguarding the privacy of your information.
It is important that you read this privacy notice together with any other privacy notice we may provide on specific occasions when we are collecting or processing personal data about you so that you are fully aware of how and why we are using your data.

Data Controller
OCMS is the data controller and responsible for your personal data.

Why are we collecting your data?
We collect personal data to provide our programmes and activities, to monitor and assess the quality of our services, to fulfil our purposes as a charity and to comply with the law. In legal terms this is called 'legitimate interests'. When it is required, we may also ask you for your consent to process your data. We do not share your information with others except as described in this notice.
The categories of information that we may collect, hold and share include:

- Personal information (such as name, telephone number, address and email address)
- Characteristics (such as gender, marital status, language, date of birth)
- Special categories of personal data (such as your religious beliefs, or racial or ethnic origin)

Storing your data
We will only retain your personal data for as long as necessary to fulfil the purposes we collected it for, including for the purposes of satisfying any legal, accounting or reporting requirements.
We hold your data for varying lengths of time depending on the type of information in question but in doing so we always comply with Data Protection legislation. Details of retention periods are available in our retention policy which you can request by contacting us at dpo@ocms.ac.uk

Security of your data
We have put in place appropriate security measures to prevent your personal data from being accidentally lost, used or accessed in an unauthorised way, altered or disclosed. In addition, we limit access to your personal data to those employees, trustees or consultants who need to know. They will only process your personal data on our instructions.
We have put in place procedures to deal with any suspected personal data breach and will notify you and the ICO where we are legally required to do so.

Who do we share your information with?
We will not share your information with third parties without your consent unless the law requires us to do so.

Requesting access to your personal data
Under Data Protection legislation, you have the right to request access to information about you that we hold. To make a request for your personal information contact us at dpo@ocms.ac.uk
You also have the right to:

- object to processing of personal data that is likely to cause, or is causing, damage or distress
- prevent processing for the purpose of direct marketing
- object to decisions being taken by automated means
- in certain circumstances, have inaccurate personal data rectified, blocked, erased or destroyed; and
- claim compensation for damages caused by a breach of the Data Protection regulations.

For further information on how your information is used, how we maintain the security of your information and your rights to access information we hold on you please contact the Chief Operating Officer at ocms@ocms.ac.uk.

If you have a concern about the way we are collecting or using your personal data, you should raise your concern with us in the first instance or directly to the Information Commissioner's Office at https://ico.org.uk/concerns/

Contact:

If you would like to discuss anything in this privacy notice, please contact us at : dpo@ocms.ac.uk