OXFAM GB DATA PROTECTION POLICY

POLICY DETAILS	
POLICY NUMBER:	COCR009
POLICY OWNER:	Data Protection Officer
POLICY AUTHOR:	Data protection Officer
SLT SPONSOR:	Chief Operating Officer

APPROVAL INFORMATION	
AUTHORITATIVE VERSION:	Here.
APPROVED BY:	Audit & Risk Committee
APPROVAL DATE:	8 July 2025
EFFECTIVE FROM:	8 July 2025
SUPERSEDES:	Data Protection Policy 2022
DATE OF REVIEW:	July 2027
FREQUENCY OF REVIEW:	Every 2 years

CONSULTATION AND IMPLEMENTATION	
STAKEHOLDERS CONSULTED:	☐ Board Committee ☐ Country Director(s) ☐ Governance team ☐ HR team ☒ InfoSec team ☐ Integrity team ☐ International Ops ☐ Legal team ☐ Risk & Assurance ☐ SLT ☐ Trustee Board ☐ Union ☐ Other
DATE(S) OF CONSULTATIONS:	N/A
DESCRIPTION OF CONSULTATIONS:	N/A

IMPLEMENTATION OWNER:	Data Protection Officer
IMPLEMENTATION PLAN:	• Via the Weekly Manager's Briefing; • Via the annual mandatory data protection training required of all staff; • Via the mandatory induction data protection training requirement for new staff; • Via the OGB network of Data Protection Focal Point, as one of their duties is to know and signpost colleagues to this policy; • Additional guidance material is provided to relevant clusters of staff, such as redaction guidance for investigation teams, Subject Access Request process guidance to some HR colleagues.

SCOPE AND CONFIDENTIALITY	
GEOGRAPHICAL SCOPE:	Worldwide, except in countries where the following policy contravenes local legislation. In these cases, local legislation must be followed.
SECURITY CLASSIFICATION:	☒ Public ☐ Internal ☐ Confidential
CIRCULATION:	Public

1. INTRODUCTION

1.1. BACKGROUND

This policy updates Oxfam GB's previous Data protection Policy, and ensures all staff understand Oxfam's responsibility to process personal data safely and securely.

1.2. PURPOSE

This policy sets out how Oxfam GB, its management, trustees and staff will meet their obligations under privacy and data protection laws[1] by:

- establishing a management framework for compliance with these laws;
- setting out the principles to which Oxfam GB will adhere when collecting and using personal data

1.3. SCOPE AND APPLICABILITY

This policy applies to everyone in the organisation, including volunteers.

This Data Protection Policy applies to all Personal Data processed by Oxfam GB. In particular, it sets out standards and processes for working with and being compliant with laws relating to Personal Data considered in scope for European Data Protection law.

- For *personal Data*, all sections of this policy will apply to that data, including principles of governance and privacy.
- For data that does not fall in the scope of GDPR (non-personal data) the Standards section of this policy is non-binding. Indeed, for non-personal data the principles of the Responsible Programme Data Policy apply in lieu, except where the context makes clear that parts of that policy only apply in some territories[2].

2. POLICY STATEMENT

Oxfam GB has a statutory obligation to process personal data in accordance with UK data Protection Legislation (GDPR and the Data protection Act 2018). As a rights-based organization, Oxfam GB is committed to employees and volunteers protecting privacy and personal data and using data responsibly to uphold the rights of the individuals, groups and organizations with whom we work. Oxfam GB recognizes that people have rights with regard to the information related to them and that we have a responsibility to uphold those rights and freedoms. This Data Protection policy should be read in tandem with Oxfam's Responsible Program Data Policy, which principally concerns the treatment of program data. Oxfam GB affirms its commitment to the Responsible Programme Data Policy worldwide and will update this policy to adapt it to new challenges and

[1] Including the GDPR and relevant electronic communication regulations.

[2] The Responsible Program Data Policy can be seen at: https://www.oxfam.org/sites/www.oxfam.org/files/file_attachments/story/oxfam-responsible-program-data-policy-feb-2015-en_1.pdf

technical stakes.

3. RELATED DOCUMENTS

Responsible Data in Program Policy
Acceptable Usage Policy
Information Security Policy
Staff Code of Conduct
Subject Access Request Policy
Breach Response Policy
Information Asset Process
Biometric & Foundational Identity Policy

3.1. POLICIES

Oxfam Responsible Program Data Policy.docx
OGB Acceptable Use Policy
OGB Information Security Policy
OGB Biometric and Foundational Identity Policy

4. POLICY CONTENTS

1. **Definitions**
2. **Commitments**
3. **Standards & Principles**
4. **Roles and responsibilities**
5. **Consequences of non-compliance**

4.1. DEFINITIONS

Personal data means any information relating to an identified or identifiable natural person (a "data subject"). Data will be deemed personal if it identifies/makes identifiable someone, directly or indirectly.

Sensitive data (also called *special category data*) is a subcategory of personal data requiring additional safeguards as it is data that has or could be used to discriminate natural persons.

Processing should be taken to mean any operation defined in law, i.e. collection, recording, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure and destruction.

Pseudonymization means 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 are not attributed to an identified or identifiable natural person

Anonymization means the processing of personal data with the aim of irreversibly preventing the identification of the individual.

4.2. COMMITMENTS

APPOINTMENT OF DATA PROTECTION OFFICER

Oxfam GB has appointed a Data Protection Officer (DPO). The DPO has specified legal responsibilities under the GDPR. Among other things, the DPO will advise Oxfam GB on compliance with privacy and data protection laws and principles. The DPO acts as the contact point for Oxfam GB with relevant supervisory authorities, other DPOs/Data Protection Focal Points in the Confederation, and data subjects.

Oxfam GB commits to providing the DPO with the independence and resources necessary to meet their GDPR and privacy obligations. The DPO will provide an annual report to the Audit & Risk Committee (ARC) and have access to the Board at other times to advise on compliance matters, including data breaches.

APPOINTMENT OF SPECIALIST COMPLIANCE LEADS

Each Division within Oxfam GB is required to appoint one or more Specialist Compliance Leads (referred to as Data Protection Focal Points - DPFPs) to whom Directors will delegate responsibility for data protection compliance and respect for privacy in the Director's area of responsibility.

A list of the DPFPs to whom responsibility is delegated will be maintained by the Data Protection Officer.

5. STANDARDS (MUST BE MEASURABLE AND REPORTABLE)

Oxfam commits to having standards and principles that are measurable and reportable and ensure we process personal data ethically and lawfully.

5.1 Principles

Oxfam GB commits to the following principles in relation to privacy and data processing. These principles reflect the principles laid down in the General Data Protection Regulation (GDPR[3]). A key requirement of the GDPR is the ability to demonstrate compliance with the principles - also referred to as the accountability principle. This means that appropriate documentation of actions is critical.

Oxfam GB employees and volunteers commit to only process personal data where necessary, and to seek to limit their access to this data when they feel their level of access is unnecessary. This requires that employees and volunteers are empowered to challenge their level of access to data. The more sensitive the data or if there is a high likelihood that access could result in harm, the stronger this commitment should be.

[3] Where this policy refers to the GDPR, it includes the equivalent obligations under UK legislation which incorporates the terms of the GDPR.

5.2 Oxfam GB is committed to upholding guiding data protection principles

OGB will collect and use personal data lawfully

There are six legal bases on which Oxfam GB may lawfully collect and use personal data[4]. One of which must be present and evidenced before any data processing activity occurs. Oxfam GB will keep a record, on an ongoing basis, of its personal data processing activities. Oxfam GB will specify which basis for processing it is relying on in relation to each activity.

Stricter rules apply to 'special' categories of data. Special category data is data that reveals racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, or is biometric data, data concerning health, data concerning a person's sex life or sexual orientation, or financial data. The collection, use, storage or any other form of processing of these types of data are prohibited unless a specific exception applies[5]. Oxfam GB will keep a record, on an ongoing basis, of any data processing activity that involves special categories of data and specify which exception it is relying on in relation with this processing.

Where Oxfam GB relies on consent as the basis for collecting and using personal data, including special categories of data, Oxfam GB will have GDPR-compliant consent processes and notices in place, and keep records of the consents provided. Oxfam GB will also have processes in place to action withdrawals of consent.

Oxfam GB will process personal information fairly and transparently

Oxfam GB will be transparent about the information is obtains, collects and holds about individuals, for what purposes that information will be used, with whom it is shared, and an individual's rights over their data. The more an individual is disempowered or otherwise vulnerable, the more Oxfam GB's duty to empower with a clear understanding of what is done with their data and the consequences of the data processing activities.

OGB's main privacy notices shall be reviewed at least every two years. These privacy notices cover at least the staff, the website and the whistleblowing hotline privacy notices.

Oxfam GB will only collect personal data that is necessary

Oxfam GB will only collect personal data from an individual where this is needed for Oxfam GB's legitimate purposes and it will only collect the minimum data necessary to fulfil those purposes. Oxfam GB will be able to explain and justify these purposes. Analysis of legitimate interests and record-keeping may be required for these purposes.

Oxfam GB will keep personal information accurate and up to date

Oxfam GB will encourage individuals to notify Oxfam of any inaccuracies by following a simple procedure set out in Oxfam GB privacy notices. Oxfam GB will respond to requests for rectification of data in a timely manner. Oxfam GB will implement information-governance processes and staff

[4]These are: consent; processing is necessary for a contract with the data subject; compliance with a legal obligation; the protection of the vital interests of the data subject or another person; processing is necessary for the performance of a task carried out in the public interest; or processing is necessary for the purposes of the legitimate interests of Oxfam or a third party.

[5] Under Article 9 GDPR

training to assist with implementation of this principle. Oxfam GB commits to ensuring any inaccurate information recognized as inaccurate throughout their daily activities is also updated where appropriate.

Oxfam GB will not keep information for longer than is required or necessary

If Oxfam no longer needs personal information for the original business purpose for which it was collected it will securely delete/destroy it in accordance with its data destruction procedures unless it has a legal obligation to retain the personal information for a longer period.

5.3 Oxfam GB will respect the privacy and data protection rights of individuals

Oxfam GB will respect the rights granted to individuals by data protection laws, including rights to:

- access their data
- restrict the use of their data
- rectify inaccuracies in their data
- erase their data
- restrict unsolicited contact
- be informed of the criteria for any automated decision-making about them
- be notified of data breaches
- move their data efficiently (data portability) - where this right applies

Guidelines and Policies in relation to: Subject Access Requests, Data Subject Breach Notifications, Automated decision-making and Marketing communication consents is available.

5.4 Oxfam GB will keep personal information secure

Oxfam GB has implemented relevant security procedures through its Information Security Policy and the Acceptable Use Policy to prevent unauthorised access, accidental loss, destruction or damage of the personal data it holds.

Where Oxfam GB uses third parties to obtain or process personal data on its behalf this will only be done under written contracts with the supplier of the data/services that contain the necessary data protection clauses required by the GDPR.

Oxfam GB will not use third parties to obtain or process personal data without conducting reasonable due diligence on the supplier in relation to their compliance with data protection law. Those involved in procurement of such services will receive training and support in ensuring the principles of data protection and compliance are upheld and implemented through the required documents, including risk assessments and contractual arrangements.

Members of staff and volunteers are responsible for ensuring that any personal data which they hold is kept securely and not disclosed to any unauthorised third parties. Oxfam GB will ensure that personal data is accessible only to those who have a valid reason for seeing or using it.

5.5 Privacy by Design and Default

Oxfam GB supports initiatives that support privacy by design and default.

Before adopting new data processing or activities that may present high risks to privacy and personal data, Oxfam GB will conduct and document a data protection impact assessment (DPIA).

Oxfam GB commits to consulting with the relevant supervisory authority where a DPIA indicates a high risk from a proposed processing activity or technology.

Where appropriate, Oxfam GB will use processes such as pseudonymization (to reduce privacy risks to data subjects) or anonymization (which cannot be 'reversed' to identify data subjects) to minimize the collection, use, storage or any other form of processing of personal data. Oxfam GB recognises that anonymization processes are required to often be revised to follow best practice, and that complex sensitive sets of data should be assumed as not anonymizable.

5.6 Electronic communications

Oxfam GB recognizes the specific privacy rights of individuals in relation to electronic communications. It will comply with relevant laws in relation to its marketing activities and use of cookies or similar technology on its public websites[6].

5.7 Training, awareness and development of a privacy culture

Oxfam GB provides mandatory on-line training on data protection and privacy to all its EU staff and compliance related individuals oversees too. Others are provided with a Data Rights training, focused on data protection principles and data subject rights.

Oxfam GB will support employees with specific privacy or data protection responsibilities in any additional training requirements.

This policy and related guidance will form part of the induction of all Oxfam GB employees and volunteers. Breaches of the policy will attract action under Oxfam GB's disciplinary policy.

5.8 CCTV, sound and other video surveillance technologies

The use of CCTV or other video surveillance technologies is tolerated as long it serves strict safety of individuals (except beneficiaries) or Oxfam property purposes. In line with data protection law and ethics, if such technology is put in place there will need to be:

- Very clear and obvious information available in the area surveilled. For instance, at least one sign on the wall easy to read for a person with vision impairment, in the most common language of the country or region;
    - This information must at least inform on surveillance, on the purpose of that surveillance, and on means to reach the relevant team at Oxfam to raise concerns or questions. Contact means must be generic to continue to work through staff changes.
- Prior check with the team tasked to oversee the Oxfam property(ies) at hand;

[6] Organizations in the EU must currently comply with national legislation which implements a European Directive (Directive 2002/58/EC on Privacy and Electronic Communications).

- Check with the team aforementioned on the legal requirements applicable in the country at hand.

Please use the OGB/OI guidance on the use of CCTV or other video surveillance technologies.

Note – For safeguarding reasons, the deployment of surveillance technology to protect beneficiaries should be avoided. In order to factor in power dynamics and the concerns it may raise among communities it could be allowed but only after the Safeguarding, Privacy and Cybersecurity Teams approve its use.

5.9 Transfers of personal data out of the EU

Data sharing outside of OGB, unless already covered by an agreement with international transfer clauses, can only be done after written data protection focal point advice has been received.

For *personal Data*:
Transfers of personal data out of the EU are restricted under the GDPR. Oxfam GB will ensure personal data will only be transferred out of the EU where there is a lawful basis for this[7]; and the transfer is subject to the required standard of protection for data subjects.

Oxfam GB uses the European Commission's Standard Contractual Clauses (SCCs) for transfers of staff data to Affiliates out of the EU, called internally the Data Passport. In this respect, it has entered into SCCs with each Oxfam Affiliate outside the European Union[8] except New Zealand (for which another lawful basis of data transfer is available[9]).

The data that may be lawfully transferred under the SCCs is only such data as is specified in the Annexs to the SCCs, which require completion when a new data sharing activity is required.

6. ROLES AND RESPONSIBILITIES

6.1 Disclosures between Oxfam GB and other affiliates

Transfers of personal data from Oxfam GB to OI or other affiliates are disclosures to third parties; the confederation is not considered a single organization for these purposes. Oxfam GB may only disclose personal data to OI or affiliates where it has a lawful basis for doing so. In many cases, Oxfam GB will be able to rely on 'legitimate interest' as the basis for disclosure. Oxfam GB will state in all Privacy Notices that data may be shared with other members of the confederation.

6.2 Inter-affiliate services

If Oxfam GB provides data processing services to OI or another affiliate, or receives data processing services from OI or another affiliate (e.g., the provision of a server or other IT infrastructure or services), this processing will need to be the subject to a written agreement on the terms prescribed by the GDPR. Oxfam GB will need to identify where such arrangements exist and ensure relevant

[7] This will be one of the lawful bases for processing described above.
[8] Oxfam Australia, Oxfam US, Oxfam Canada, Oxfam Quebec, Oxfam South Africa, Oxfam India, Oxfam Japan, Oxfam Hong Kong, Oxfam Brazil….
[9] The EC has issued an 'Adequacy Decision' in relation to the data protection laws in New Zealand.

data processing agreements are in place.

6.3 Regulatory Supervision

Oxfam GB, OI and other EU Affiliates can elect a lead supervisory authority in relation to processing activities that involve more than one Oxfam in the EU. For all processing activities that involve OGB only, the supervisory authority is the Information Commissioners Office.

6.4 National Requirements

While the GDPR applies across EU affiliates and their activities, some derogations and additions are permitted under national laws. Oxfam GB is responsible for identifying any National Add-on requirements or derogations from the GDPR and establishing policies/procedures in relation to these requirements. Oxfam GB should notify OI and other affiliates of any national requirements that may have cross-confederation implications.

6.5 Contribution to confederation strategy and compliance

InfoSec & Privacy Committee
Oxfam GB will nominate a representative to the Inter-Affiliate Privacy Reference Group. This will normally be the DPO or their delegate. The nominated representative will contribute to the group by sharing good practice, reviewing external developments, and monitoring internal compliance. It will contribute to the OIS DPO's annual report to the OI Board.

Training
Since 2018 all Oxfam GB's staff in the EU and senior international staff complete on-line training on privacy and data protection. All Oxfam GB staff outside the EU completes appropriate training on privacy and data protection, referred to as the "Data Rights" training.

Reporting between Affiliates
Under the Global Management Agreement and other protocols between Affiliates, certain reporting of serious incidents is required. Oxfam GB will participate in the development of guidelines for any transfer of personal data to permit such reporting.

Data Protection Focal Points
Oxfam GB will nominate a data protection focal point as the contact point for all confederation communications on data protection, with responsibility for circulating any communications to relevant stakeholders or escalating any issues to the appropriate level. This will normally be the DPO or their delegate.

7. CONSEQUENCES OF NON-COMPLIANCE

7.1 Incidents involving personal data vs breaches of this policy

In order to ensure data protection accountability it is important that all individuals working with and within Oxfam inform the Privacy team of any incidents involving personal data ('data breach'). This is because the Privacy team needs to be able to assess the incident and advise on any actions which may be necessary to mitigate risk, It is also important to enable the team to understand patterns of

systemic vulnerabilities that expose all of us to mishandling data, to ensure Oxfam learns from its vulnerabilities, that may be due to our tools themselves.

Being involved in a data breach may not imply a breach of this policy. Unless one intended to violate this policy or the data breach itself is egregious, which is rare. Cases are assessed on a case by case basis taking into account harm caused, the time taken to inform the Privacy team, the role and seniority of the person, the category of people whose data it is that was mishandled (as the most vulnerable the person, the higher our responsibility of care or the cooperation with the Privacy team). For instance, if you have been told to not share certain type of data and you do so continuously, it is more likely be deemed a violation of this policy.

Mistakes happen and always will. What matters is that Oxfam handles them in an accountable manner. The Privacy team exists to support you, and to ensure Oxfam is accountable when an incident has occured. Which is why transparency with the team is fundamental – to help them help you.

If you suspect that a data breach may have taken place, you must contact the Privacy Team (at privacy@oxfam.org.uk) instantly.

- ## Practical consequences

The Oxfam GB Trustees are responsible for ensuring that Oxfam GB respects privacy rights and meets its legal obligations.

The Oxfam GB Leadership Team, in co-ordination with the Data Protection Officer (DPO), is responsible for the development, implementation, monitoring, and evaluation of procedures and systems to ensure data protection within Oxfam GB, and adherence to this policy.

For all staff members, breaches of this Policy may constitute misconduct under the Dealing with Problems at Work Policy and serious, or repeated minor, breaches may constitute gross misconduct

For volunteers and partners, breaches of this Policy may constitute misconduct that could be taken into consideration in light of their relationship with Oxfam.

VERSION CONTROL			
VERSION NUMBER	**DATE**	**AUTHOR**	**BRIEF DESCRIPTION OF CHANGES**
3	16/5/25	Francesca Smith - Data Protection Officer	Transfer to new template and minor wording changes – introduction of two new definitions
2	15/02/22		Updating of wording, clarification of consequences of breaches of this policy, new section on the use of video and sound surveillance technology
APPROVAL HISTORY			

VERSION NUMBER	DATE APPROVED	REVIEWED/APPROVED BY	COMMENTS
3	8th July 2025	ARC	Minor updates reported to Board