OXFAM BIOMETRIC & FOUNDATIONAL IDENTITY POLICY

Approved by/Date	Executive Board 18/05/2021	**Effective Date**	18/05/2021
Document	Policy	**Document Classification**	Public
Policy Category	Organisational	**Last revision**	06/05/2021
Compliance	Mandatory globally	**Next Revision**	18/05/2022
Document owner	COO OIMT	**Key Contacts**	Information Security OI/OGB

Oxfam Biometric & Foundational Identity Policy

Policy statement

As a rights-based organisation, Oxfam is committed to protecting privacy and managing data responsibly to uphold the rights of the individuals, groups, communities and organisations with whom we work.

Oxfam recognises that people have rights over information related to them. The way that information is processed, which informs decisions or behaviour, underpins other broadly recognised rights, including those in the Universal Declaration[1]. Oxfam has a responsibility to uphold those rights.

We recognise that biometric and foundational identity information carries additional risk, so upholding those rights becomes more complex.

This policy outlines our position on upholding people's rights as they apply to a specific type of data – biometric and foundational identity data – as well as information that can be used to generate such data; in particular where it relates to the individuals and communities with whom we work as part of our programming.

This policy supplements, but does not replace, the Data Protection Policy and Responsible Data in Program Policy, and is rooted in existing good practice and frameworks in the areas of Safe Programming and broad Ethical Data Use and Privacy Practice.

Scope

The scope of this policy is as follows:

Systems which by design or their nature are intended or likely to be used to identify individuals and groups of people for the purposes of administering humanitarian programming or other services.

These may typically (but not exclusively) include registration or forms of programming such as Cash, Food Security, Financial Inclusion, In Kind and are typically (but not exclusively) digital.

Definitions

Personal Data means any information relating, directly or indirectly, to an identified or identifiable natural person (a "data subject"). A *natural person* is a living, individual human being.

Biometric Data means Personal Data resulting from specific technical processing relating to the physical, physiological or behavioural characteristics of a natural person, which allow or confirm the unique identification of that natural person, such as (but not limited to) fingerprints and iris or facial recognition.

Data Protection Officer or Focal Point (DPO/FP) is an appointed role at affiliate-level sometimes required by law (Data Protection Officer) and sometimes not required by law but made by delegation within the affiliate (Focal Point). They are generally a senior member of staff responsible for Data Protection, and may have explicit statutory responsibility, e.g. the General Data Protection Regulation (GDPR).

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,

[1] https://www.un.org/en/universal-declaration-human-rights/

dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

Senior Responsible Officer (SRO) should be taken to mean the senior member of staff who is accountable for delivery of the project – for instance the Program Manager. Where this is unclear, the SRO should be assumed to be the Country Director.

Foundational Identity Data means data which is linked to individuals, stored in a database or structured storage system, and used to identify them for the purposes of delivering services or organising activity – for instance, a distribution, provision of financial services or resettlement. Such a database may contain a variety of parameters about individuals, including name, link to state or other ID, vulnerability criteria and potentially also biometric data.

Intent of this Policy

This policy sets out how Oxfam, its management, trustees and staff will meet their obligations under International Humanitarian Law, Data Protection Law, Oxfam's Responsible Data in Program Policy, Safe Programming, a broad Ethical Data Use and Privacy Practice and duty of care to work with Biometric and Foundational Identity data and interact with partners who do.

It sets out:

- The decisions as to whether Biometric or Foundational Identity data processing activities are appropriate and proportionate to introduce;
- The key principles, standards and safeguards which are necessary to follow to work with Biometric data safely;
- The key business processes which need to exist in order to implement these principles and standards;
- The expectations which individuals and communities should have when we work with certain types of data, and how we work in partnership to share accountability for the use of this data;
- The expectations which our partners should have of us when we work with them on projects involving the processing of Biometric or Foundational Identity data.

Associated Policies and Procedures

- Responsible Data in Program Policy
- Data Protection Policy
- Information Security Policy
- Staff and Non-staff Codes of Conduct
- Safe Programming

1. PRINCIPLES

I. We must plan, be proportionate and be responsible

In contexts where Oxfam directly or indirectly processes personal data, we are a duty bearer of the rights of individuals and communities. Our behaviour and actions may have consequences which undermine these rights. These consequences may be particularly acute when using technology designed to identify individuals or communities at scale, given the greater potential for affecting the rights of individuals through large-scale acts or combination with other data.

Through structured planning, we will endeavour to understand what these consequences are and build a foundation which allows us to put in place steps to communicate and risk assess them.

We recognise that without this planning, these further steps are less likely to succeed. We therefore commit to carrying out procurement of and working with identity and biometric systems thoroughly and with enough time and resources to be effective.

Policy Statements:

a. Clear Benefit and Use-Case

i. Before we begin work with identity databases, we must first be clear on the rationale and benefit – presented in terms of organisational effectiveness and operations and crucially the benefit to individuals and communities in using them.

ii. Projects which implement these systems must define a use-case which is linked to this set of benefits.

iii. **We will not** plan or participate in projects where there is not a demonstrable fundamental use-case with benefit to individuals and communities.

b. The likely flow of data is knowable and known

i. We must be clear that we understand the people and parties who will have access to data throughout its life as a result of our planned activities – and that we take into account the potential circumstances and activities.

ii. Our understanding must show due regard for the "foundational" nature of the system – i.e. the more foundational the system is[2], the more it requires a deeper level of understanding and risk assessment than a term with more limited impact or scope.

iii. Where local law, power or regulation requires (or may require) that data is shared with a government or law enforcement body, or there exists another actor which may seek through coercion, intimidation or control to have data transferred to them, we must include this usage in our planning.

iv. **We will not** build systems or collect data in circumstances where we cannot reasonably know or control where data will go or how it will be used[3], or cannot reasonably be known, controlled and contextualised differently.

v. **We will not** build systems or collect data which are intentionally open-ended, in anticipation of unknown use-cases or "just in case".

c. The expected flow of data is linked and proportionate to the use-case

i. Before we begin collecting and working with data, we will understand that the

[2] This is to say, a foundational ID system which processes data on a large community for the purposes of delivering multiple pieces of humanitarian assistance naturally requires a greater understanding than a transactional system which will be used for only one piece of programming.
[3] (and therefore where steps cannot be taken during planning to preserve agency and address risk).

specific content of the exchange of data can be directly linked to the benefits to us, to individuals and their communities.

d. The flow of data is demonstrably responsible

i. Before we begin collecting and working with data, we will ensure that this flow of data is demonstrably responsible – by meeting the Data Protection Principles, Responsible Data Principles, Do No Harm and humanitarian principles and Safe Programming.

ii. **We will not** collect data or build systems where we cannot demonstrate a responsible lifecycle which embraces these principles.

II. We must be accountable to individuals and their community

We believe that without building understanding of the purpose of collecting and details of processing of data, choice, agency and dignity are undermined. We will strive to contextualise, communicate and make clear what we do.

We will listen to those with whom we work, provide spaces for their voices and views to be heard and respond to them.

Our practice will be rooted in existing good practice and frameworks in the areas of Responsible Data, Safe Programming, Data Protection, and broad Ethical Data Use and Privacy Practice.

Policy Statements:

a. The flow of data is communicated, contextualised and represented

i. We must communicate, contextualise and represent our use of data and the surrounding ecosystem of data, people and information systems to individuals and their community where not already common knowledge.

ii. This representation must be appropriate to the circumstance and take into consideration the broader ecosystem of which our use of data is a part.

iii. This representation and any response must be monitored and assessed to ensure that it is effective. This monitoring should be embedded in other program mechanisms, e.g. accountability and impact evaluation.

b. Communities' voices are listened and responded to

i. We must implement systems and processes to understand the level of distress or harm which understanding (or misunderstanding) of the data system is having or could have on communities.

ii. We must respond to this distress or harm, for instance by adapting our programming or iterating our contextualisation of how data is used.

III. We must share control with individuals and their communities

We believe that without genuine choice, agency and dignity are undermined. We also recognise that genuine choice is challenging when the circumstances are, too. Our approach will take into consideration the power and imbalance present when offering or withholding

choice.

We will provide choice where we can, and, where we cannot, make clear our choices and remain accountable for them.

Our practice will be rooted in existing good practice and frameworks in the areas of Responsible Data, Safe Programming, Data Protection and broad Ethical Data Use and Privacy Practice.

Policy Statements:

a. Individuals should have direct choice over providing data

i. Individuals must be offered the choice as to whether programming takes place which involves the use of their data.

ii. The consent of individuals must be requested for the use of their data; this consent must incorporate a contextualisation of how data will be used (i.e. Informed Consent).

iii. This consent must be backed by legal analysis and other procedural steps which acknowledge and attempt to compensate for the power imbalance present[4].

iv. Where consent is not possible, we must make clear our judgments and choices, contextualise how the data will be used (e.g. a Privacy Notice) and be accountable for our choices.

b. Where possible, data storage must be user-controlled

i. New systems, protocols, and applications should be designed in such a way as to offer as much control to individuals over their data[5].

ii. Where features and architecture exist in software which allow for user control of data, this functionality must be used where possible.

IV. We must address risk to individuals and their community

Understanding dataflow and contextualising data collection and processing is foundational to being able to plan and account for the use of data; those plans must also be responsible ones.

We plan responsibly through consideration of risk – technical risk, risk of harm, risk of distress and risk which we indirectly produce through our participation in platforms and ecosystems.

Policy Statements:

a. Possibility for reuse of data is considered

i. When procuring or implementing identity and biometric systems, we must consider how that data may be reused, in particular where data is reused for

[4] Within the EU, or where data falls within scope of the GDPR, we consider that the Consent lawful basis is unlikely to be appropriate, and an alternative lawful basis, such as Legitimate Interest, must be used instead.
[5] For instance, leveraging cryptography or other technology which embeds control at the data layer, or providing direct ongoing access to a user dialogue which outlines how data is used and offers the ability to re-/de-consent.

purposes other than those for which it was originally collected and which have not been represented or contextualised to the individual or their community.

ii. This analysis must be rooted in our planning and accountability practices – being both anticipatory and transparent.

iii. This planning must consider the likelihood of seizure, theft, or other disclosure or acquisition of data (e.g. through writ or statutory power) by government or other authorities.

b. Direct risk of harm as a result of reuse is addressed

i. We must consider what harm – of distress or harm to individuals or their other rights – may be precipitated by reuse.

ii. That consideration must be rooted in an understanding of the local context and the local community and, where possible, involve them.

V. We must address Security Risk

Maintaining confidentiality of data is a foundational discipline without which we cannot make assurances to communities about how their data will be used and in turn how we maintain trust.

Without retaining control of data in our care, it is not possible for us to make responsible use of it or make assertions about that responsible use which are deserving of trust.

Systems will be built which both incorporate and evidence robust security practice designed to prevent inadvertent or malicious loss or theft of data.

Our approach will be rooted in existing robust practice in Information Security in government and industry and guided by appropriate specialist knowledge[6]. Wherever possible, we should do this by adopting a "buy/partner, not build" approach.

Policy Statements:

a. Information Security controls are implemented

i. Applications used to process biometric data must have been designed with due consideration for Security by Design in line with modern principles of Secure Software Development.

ii. All data stored – including Biometric or other sensitive identity data – must be encrypted throughout its lifespan, storage and transmission.

iii. Systems must be maintained with operational security controls in place which are appropriately robust in line with commercial practice.

iv. A breach/incident response policy must be maintained for the relevant system(s) setting out processes and responsibilities for the eventuality of a breach, including the loss or theft of data.

v. Both sets of controls (system and application) must be supported by an adequate assessment of threats the platform may face, and an adequate

[6] Prior to engagement, the security of a system must be assessed by a specialist team or provider, and support where needed can be found via the IT Global Shared Service.

understanding of the underlying risk.

vi. **We will not use** systems which do not employ architecture, design, development and maintenance linked to an understanding of the threats affecting the environment and relevant communities.

b. We can evidence how Information Security Controls are implemented

i. We must be able to demonstrate how systems which we buy, use in conjunction with partners, build or maintain employ robust Information Security Practice.

ii. This should mean in practice that:

1. No system is used which has not been assessed by a specialist team or provider with due consideration for the scope of use of the system[7];

2. No system is used which has not been built with evidenced consideration of Security by Design and Secure Development from an early stage in its lifecycle

3. The system must not be used in the absence of a trained user-base aware of their documented security responsibilities.

iii. Where possible, systems should adhere to relevant codes of conduct or compliance standards – e.g. ISO27001, NIST SP800-53.

iv. **We will not** use, operate, procure or promote systems which do not embrace a documented Information Security approach.

v. **We will not** work with partners or suppliers who do not subscribe to a similar understanding of Information Security – either in terms of the controls they implement, or their commitment to demonstrable ongoing practice.

VI. We must employ responsible biometric practice

Where identity systems employ biometrics, they become more tightly bound to individuals in ways which remove individuals' abilities to avert harm to themselves or avoid harmful consequences in the future.

While our transparent approach, the inclusion of communities, and the responsible steps we take to keep data secure may reduce the chances of these consequences, there are still steps we must take to reduce the pathways to harm which biometric data offers.

Policy Statements:

a. Biometric systems must embrace specific principles of responsible use:

i. Biometric systems must use minimal quantities (i.e. limited to what is necessary) of biometric information for a minimum period of time;

ii. They must have regard to current good practice and standards in technology used to derive stored biometric information;

[7] This may include a range of appropriate assurance activities, including Penetration Testing, Architectural Review, Source Code Review or others.

iii. They must make appropriate use of cryptographic techniques such as encryption and hashing;

iv. They must consider acceptability of the specific biometric factor to the local community;

v. They must consider the understanding the local population have of biometrics;

vi. They must consider and make risk-based choices regarding or in response to:

1. The physical locations in which data is stored (i.e. field offices, country HQ, regional offices or affiliate head offices);

2. The legal framework affecting these physical locations and whether it offers appropriate or adequate privacy protections;

3. The factors on which biometric data is stored (e.g. smartcards belonging to the users, portable computers or server/cloud systems);

4. Other relevant context – e.g. likelihood of theft or seizure of data, or the behaviour of regional or national groups, governmental or otherwise, which may wish to make use of this data;

vii. They must segregate biometric data from other data;

viii. They must incorporate auditing of access to and use of biometric data.

ix. Biometric systems should where possible store data in a user-controllable factor or data structure, removing central control and central points of failure;

x. Where data is user-controllable, biometric systems must ensure this element of control and its implications is well-communicated to communities.

b. Biometric data **must not be processed** in any ways we recognise as likely to be harmful unless we specifically account for why:

i. Aggregated database on any storage device or medium in a field or country office (i.e. biometric data should normally be stored only on a factor held by the user);

ii. Stored in a central or aggregated database in a geographic location with Privacy Legislation which does not have "adequacy" with the EU/EEA;

iii. In unconverted/raw form – i.e. images of the biometric modality rather than a derived/converted data structure;

iv. Encrypted/unencrypted rather than via a one-way or biohashed modality.

VII. Relationships with third parties are defined and controlled

Where we work with partners – as service providers, coalition partners, donors, as local implementing partners or in other capacities, we recognise that our collective behaviour produces consequences – positive or negative – for the communities with whom we work.

We commit to ensuring that our partners' values are compatible with ours, and that our relationships with them are clear and governed.

Policy Statements:

a. Our purpose and intent must be compatible with those of our partners and their sub-processors or partners where they impact our shared work;

b. **We will** share this policy with our partners in advance of engaging in partnership, and seek to resolve bilaterally any differences in intent, approach and responsibility;

c. **We will** explore as part of our planning process our collective responsibilities. These will be documented and outlined both through a data protection lens, and due regard for the experience of the communities with whom we work;

d. **We will** document and reflect these responsibilities in Data Processing Agreements or other appropriate legal documentation which have a basis in appropriate law;

e. These responsibilities **should reflect** the approaches to accountability outlined in this policy;

f. **We will not** work with partners on biometric projects whose approaches to community involvement are not compatible with the policy statements in this policy;

g. **We will not** work with partners whose approaches to risk or security do not allow us to uphold the risk assessment and security assessment policy statements in this policy.

2. Governance and Accountability

We will put in place structures and responsibilities which are designed to embed, reinforce, uphold and support the implementation of this policy.

Policy Statements:

a. The Senior Responsible Officer for the project must maintain a documented impact assessment of their use of biometric data[8].

b. This must be signed off by an appropriate authority – generally the DPO/DPOFP of the affiliate[9].

c. Where the risk assessment is signed off by an authority other than the DPO/DPOFP, this must only be the result of a delegation from the affiliate's Executive Director.

d. This delegation must be outlined in the sign-off process or document.

e. This may be a Data Privacy Impact Assessment or Risk Assessment covering multiple projects; in this case, appropriate, documented consideration must be given to differences in implementation and community.

f. This risk assessment must include at a minimum:

[8] For the avoidance of doubt – the scorecard attached to this policy is not intended as an Impact Assessment Template.
[9] Where appropriate, these may be augmented or replaced by Oxfam International-provided functions or teams.

i. The risk associated with the policy areas in this document, i.e:

1. Planning of dataflow and purpose
2. Minimisation of data and ensuring data is only kept for a proportionate period of time
3. Accountability to individuals and their communities and how feedback is addressed
4. Control provided to individuals and their communities
5. How risk to communities is addressed
6. How Security Risk is Managed and how it has been assessed (this should normally include an assessment by the Oxfam Information Security team).
7. Biometric Practice
8. Relationships with Third Parties

g. This risk assessment must be maintained for the lifetime of the program activity and kept for a relevant and proportionate retention period.

h. Where regulation or statute requires a structured risks assessment (e.g. the Privacy Impact Assessment requirement in GDPR), this assessment should where possible be conducted through the lens of this requirement.

i. This assessment should be conducted in conjunction with other program areas where relevant – e.g. normally this should include consultation with Protection, MEAL and Technology staff[10].

[10] N.b. specialist support may be available to enable this assessment – e.g. through an EA or PA's DPO, ICT4D team, Technology function or in another area.

Appendix A - Sample Biometric Scorecard

This table may form the basis for scoring as part of a PIA or other Risk Assessment as part of the assurance of a particular exercise or activity, or a checklist for implementation planning

Theme	Factor	Description	Addressed	RAG	Notes on Risk Treatment
Plan the use of data	**Clear Benefit and Use-Case**	Any use of data must be proportionate and justified; biometric data especially sensitive (and subject to additional regulation in the EU). Therefore the benefit and use-case must be understood, as they are key to analysing and understanding risk and proportionality	☒	R	
Plan the use of data	**The likely flow of data is knowable and known**	Without a clear understanding of where data goes and how it will be used – particularly in an interagency system – it is impossible to be transparent or understand risk	☒	A	
Plan the use of data	**The data flow is linked to the use-case and proportionate**	Proportionality is a key concept in privacy, and ensures that behavior corresponds to expectation, risk is limited, and cost is reduced.	☒	G	
Plan the use of data	**The flow of data is demonstrably responsible**	The lifecycle of the data has been considered - there is a plan for data retention and destruction at the end of its life. Without considering this, it is challenging to be transparent, and data will be inherently riskier.	☒	R	
Be accountable to the community	**Dataflow contextualised and represented to affected population**	A key principle of privacy is Transparency; in humanitarian contexts, seeking Informed Consent from the affected population requires an abundance of transparency. Without being able to communicate how data is used to beneficiaries, it is unlikely the activity is respectful or safe.	☒	A	

Be accountable to the community	**Communities' voices are listened and responded to.**	Biometric data collection, and collection of data for protection, migratory, or other socio-political reasons at scale, are inherently riskier and in particular may expose populations to risk of harm and distress. Without considering feedback and the risk of distress, it is unlikely that a fair settlement exists between organisations, individuals, and groups – or that risk is effectively addressed.	☒	G
Address risk to the community	**Possibility of Reuse is considered**	Without considering how data may be reused, understanding the risk populations may be exposed to in the event that other controls fail may not be possible.	☒	R
Address risk to the community	**Direct harm as a result of reuse is addressed**	Biometric data renders risks of data reuse – or misuse to affect a population – particularly acute. It may be particularly appealing to state and non-state actors other than those who collected and intend to use it. These risks must be accounted for and assessed in the deployment context to ensure that programming is safe.	☒	A
Address security risk	**Information Security Controls are Implemented**	These risks – as well as broader privacy risks – require a strong technical underpinning (i.e. traditional security controls and technology such as encryption) to mitigate. Without these controls, a deployment is unlikely to be appropriate.	☒	G
Address security risk	**We can evidence how controls are implemented**	As part of our approach to accountability, to uphold our legal obligations, as part of healthy working practice, and as part of our commitment to healthy practice when working with partners, our approach must be evidenced.	☒	R

Responsible Biometric Practice	**Biometric systems must embrace specific principles of responsible use**	A range of more specific concerns apply to biometric data, which must be considered to ensure the biometric platform in use is a robust one. These include that data is stored in a distributed manner / in a factor held by the beneficiary and not in-country; Separate storage from program data; strong and well-considered key management for cryptography applied to data; strong consideration of privacy and security implications of template conversion approach; where data is held centrally, data is protected by technical and organisational measures from extraction and consequent reuse.	☒	A	
Responsible Biometric Practice	**Biometric data must not be processed in any ways we recognize as likely to be harmful unless we specifically account for why**	We recognize a number of specific types of biometric processing as significantly more likely to represent pathways to harm for individuals if other controls fail. These design patterns should be avoided unless we strongly account for why we believe we can mitigate the risk they represent.	☒	G	
Relationships with third parties are defined and controlled	**Defined relationships and responsibilities between partners**	Without clearly understanding responsibilities and dataflow between organisations, it is not possible to put further legal protection – such as contracts or analysis of data protection details – in place. Where these partners are outwith the country in which the data is collected, there may not only need to be consideration for a contractual definition of responsibility and liability, but also consideration for cross-border legal protections - e.g. "Appropriate Safeguards" under European Law.	☒	R	