ONE OXFAM DIGITAL SAFEGUARDING POLICY

TALE OF CONTENTS

1. POLICY STATEMENT

At Oxfam, we believe in the inherent freedom, dignity and equality of all people. The world is an increasingly digital place, and Oxfam recognises the opportunity and the challenges presented when communicating, connecting and working online. We must understand the associated risks to ensure the safety, security, and wellbeing of the people involved in our work, and our safeguarding procedures need to be relevant to both offline and online spaces.

This policy outlines Oxfam's expectations for the appropriate use of digital media by Oxfam staff, partners, representatives, supporters, volunteers, project participants and beneficiaries – as well as anybody who comes into contact with us through digital platforms, including children, young people and vulnerable adults. Oxfam has a zero-tolerance policy towards power abuses and sexual harassment, exploitation and abuse, whether this takes place in the online or offline sphere. Oxfam commits to: supporting survivors; improving safeguarding capacity; and reporting, investigating, responding to and preventing power abuses and sexual harassment, exploitation and abuse.

The guidance in this policy should not be taken as an exhaustive list. As the digital world rapidly evolves, it is important that Oxfam staff and those working with Oxfam take responsibility for considering the full range of risks and safeguards required.

Affiliate Safeguarding Leads and Teams will use this Policy in conjunction with relevant employment/labour laws, duty of care and relevant criminal laws to make decisions about how to respond to any complaints and concerns raised. For further advice, please contact your Affiliate's Safeguarding Lead (see Annex 2 of the One Oxfam PSEA Policy for Affiliate specific channels) or local Safeguarding Focal Point.

The policy complements Oxfam's existing safeguarding policies, Oxfam International's Data Protection Policy, Oxfam affiliates' Data Protection Policies, and Oxfam's Responsible Program Data Policy. The policy should also be guided by the Oxfam Staff Code of Conduct and the Oxfam Friends Code of Conduct.

2. SCOPE AND PURPOSE

This policy applies globally to all Oxfam Employees and Related Personnel,[1] both during and outside normal working hours; including Oxfam International, Affiliate HQs, Regional platforms and Country programs. In countries where the policy contravenes local legislation, local legislation must be followed with guidance from the respective affiliate Headquarters. Oxfam policy will apply in the event that it is more stringent than local legislation.

This policy sets out Oxfam's approach to digital safeguarding and covers all digital spaces where Oxfam's work is conducted. This includes, but is not limited to: email; internal and external social media channels and online platforms relating to Oxfam's work (including Facebook, Twitter, Instagram, YouTube, WhatsApp, LinkedIn, Pinterest, Workplace, COMPASS, blogging platforms); websites (including those relating to fundraising and e-commerce); internet services and ICT equipment provided by Oxfam.

This policy covers:

- Our digital safeguarding commitments, including ensuring effective action is taken when problems occur.
- Principles upon which Oxfam will base its decision making and actions.
- Our expectations of all those who work on behalf of Oxfam.

[1] Oxfam Employees and Related Personnel includes anyone with a contractual link to Oxfam, including interns, volunteers, consultants, partners, sub-grantees, etc. See Annex I for further information.

Oxfam's scope of responsibility *may* be limited in the following circumstances, in some instances:

- When Oxfam has no direct involvement in the online activity, is not aware of the activity, it does not take place on Oxfam's official accounts and platforms and/or it does not concern Oxfam's work.
- When Oxfam's control of online spaces or ICT equipment is curbed due to technical limitations and/or management or ownership by third parties – although Oxfam may still be legally responsible in these instances.
- When Oxfam does not have any control over the online space of or personal risk to the person involved in Oxfam's work (e.g. a human rights defender in a politically oppressed context).
- When someone that Oxfam works with turns down or refuses our advice or assistance. In certain cases, this should be recorded in writing.

3. OXFAM DIGITAL SAFEGUARDING PRINCIPLES AND COMMITMENTS

It is Oxfam's responsibility to ensure the health, safety and wellbeing of staff, partners, representatives, volunteers, supporters, project participants and beneficiaries. Based on systematic feedback mechanisms, it is Oxfam's responsibility to monitor this and to take appropriate measures when deemed necessary.

Oxfam's safeguarding commitment is to:

- Create and maintain a safe organisational culture for all those whom Oxfam serves and those working on our behalf.
- Ensure everyone associated with the delivery of our work has access to information about how to report concerns or allegations of child exploitation or abuse.
- Ensure that all concerns or allegations of sexual harassment, exploitation or abuse are responded to in a timely and appropriate manner and there are multiple channels through which people can raise concerns.
- Ensure zero tolerance of sexual harassment, exploitation and abuse in the organisation through robust prevention and response work, offering support to survivors and holding those responsible to account.
- Adopt an approach that respects the confidentiality and decision-making rights of survivors where possible and appropriate to do so.
- Build a culture where all those whom Oxfam serves and who work for Oxfam feel empowered to insist on non- discriminatory and respectful behaviour from each other, where poor behaviour is not accepted, and where power is not abused.
- Be transparent about safeguarding issues occurring within Oxfam, in line with privacy regulations and within legal frameworks.
- Be sensitive in our communications about our practices and open to learning and improving.
- Ensure everyone associated with the delivery of our work will have access to, and be familiar with, all safeguarding policies and know their responsibilities within it.
- Ensure everyone who works on behalf of Oxfam with children and vulnerable populations will receive training in relation to Child Safeguarding. This training will be carried out on a regular basis. In addition, those with specific responsibilities will receive additional training commensurate with their role.

Oxfam's digital safeguarding commitment is to:

- Support the people involved in Oxfam's work to navigate digital spaces and use equipment and digital tools safely and effectively.
- Be proactive in promoting digital safety by giving guidance, tools and training to staff, partners and those working with or on behalf of Oxfam where possible and appropriate.

- Take action on digital safeguarding and data protection incidents when Oxfam is aware of these (see Sections 12 and 13 for more information).

4. DIGITAL SAFEGUARDING

Digital safeguarding refers to the safeguarding policies, procedures and practices relating to online spaces. The same safeguarding principles apply to Oxfam's programmes and activities, whether these take place digitally or physically. However, there are specific considerations to take into account with online initiatives, as digital technology has brought about new safeguarding issues. For example, perpetrators of exploitation, abuse and harassment can hide behind fake photos and profiles, and the online disinhibition effect leads to the proliferation of trolling and cyberbullying. Images, videos and texts can be sent easily to large groups of people, and once images or data have been shared digitally, it is almost impossible to delete or recall them.

The following risks should be taken into account when considering digital safeguarding.[2]

4.1 Content risks

Risks that are produced as a result of the material that people can access online. People may be exposed to this content actively or passively, and it may produce a harmful effect. Content may be illegal to possess or share according to national law, e.g. sexually exploitative images of children or radicalising videos. Inappropriate and offensive content is more subjective, and includes: commercial adverts or spam; violent, extremist or hateful material; sexually exploitative or sexual material; and content which is discriminatory based on someone's race, ethnicity, nationality, class, socioeconomic status, age, sex and gender identity/expression, sexual orientation, (dis)ability, religion, language or other status.

4.2 Contact risks

Risks that are produced as a result of others' online behaviour. Individuals may have information about them shared or may be engaged in ways which lead to harmful consequences. The types of behaviour which people may experience include:

- Bullying online or through mobile phones;
- Harassment and stalking;
- Ideological grooming;
- Exposure to political risk, e.g. government surveillance or having details of online activism shared with authorities in politically oppressed contexts;
- Increased exposure to cybersecurity risks, e.g. by having malicious content shared such as ransomware, apps or other active content or malicious code;
- Harvesting, tracking and illegal sharing and possession of information – including having personal data collected, processed or shared without the individual's consent or on another unlawful basis;
- Distribution of private and sexual images, e.g. the distribution of sexually exploitative images or videos without an individual's permission;
- Non-contact sexual abuse and exploitation – including grooming, flashing, being persuaded to perform sexual acts online, and being exposed to sexually exploitative images or videos.

4.3 Conduct risks

Risks that are produced as a result of people's own online behaviour, which may put themselves and others at risk. People may download something illegally, bully, harass or exploit others, unintentionally reveal their location, create and upload sexual material or sext (send someone sexually explicit photographs or messages via mobile phone). This may also include online activism in politically

[2] This is adapted from the framework developed by Dr Tanya Byron on digital safeguarding of children and is outlined in detail in Byron, T. (2008) *Safer Children in a Digital World: The Report of the Byron Review*

oppressed or conservative contexts, or breaking confidentiality of closed spaces by reposting, sharing, downloading or in other ways transmitting information that leads to harassment, exploitation, or other harm in another setting.

4.4 Technology-based gender-based violence[3]

Oxfam recognizes that online harassment, bullying and sexual exploitation can affect anyone, but is most likely to affect women, girls and LGBTQI+ individuals. These groups face an increased risk of violence through digital technology, which can be considered a form of Gender-Based Violence[4]. Oxfam staff, partners, representatives and others working with Oxfam should be aware of common perpetrators and acts of such violence.

Perpetrators include:

- Individuals or groups who target people on an ideological basis such as fundamentalist, patriarchal, sexist or homophobic groups.
- Governments or companies who find gender justice or LGBTQI+ rights work threatening to their power and authority.
- Acquaintances, intimate partners or family members who wish to harm someone or exercise power over them.

Acts of violence include:

- Online harassment and trolling.
- Cyberstalking (tracking and monitoring of someone's movements and activities online).
- Invasion of privacy by gaining access to phones, devices, and email or other accounts without consent.
- Distribution without consent of private and sexual images, or using these images as leverage and enforcement of power dynamics.

5. ROLES AND RESPONSIBILITIES

- **All Oxfam Employees and Related-Personnel:** Everyone who works on behalf of Oxfam is required to report any digital safeguarding suspicions or incidences (see sections on reporting below). Failure to report these to a relevant person is a breach of Oxfam's policy, and could lead to disciplinary action being taken against employees and the termination of Oxfam's relationship with non-employees. There is no obligation for an individual to report any incident that has happened to them.
- **Trustees and Directors:** Hold overall accountability for this policy and its implementation.
- **Oxfam Affiliate's Executive Director:** Each Oxfam Affiliate's ED is responsible for the application of this policy within their own affiliate.
- **Safeguarding Focal Points:** Provide support to prevent and respond to digital safeguarding incidences alongside their substantive roles. They raise awareness and promote best practices by supporting survivors and receiving and reporting concerns in a confidential manner within their Affiliate channel.
- **Safeguarding Leads/Advisors:** Provide support to Focal Points, staff and programmes to prevent and respond to digital safeguarding concerns. They raise awareness, conduct training and promote best practices, as well as receiving concerns, conducting referrals to specialised services and supporting investigations. Safeguarding Leads/Safeguarding Teams/Advisors and senior management should offer further support to help implement this policy.

[3] Adapted from the Just Associates (JASS) ICTs for Feminist Movement Building Toolkit https://justassociates.org/en/resources/icts-feminist-movement-building-activist-toolkit

[4] Gender-based violence is an umbrella term for any harm that is perpetrated against a person's will, and that results from power inequalities that are based on gender roles, expectations, and norms.

- **Oxfam's Data Protection Officers and Privacy Focal Points:** Offer support on data protection issues and may have explicit legal responsibility for oversight and governance. They must be involved or consulted in relevant privacy notices associated with platforms, required consent, and data security, retention and deletion aspects.
- **Social media, website, channel, shop, project, programme and campaign managers:** Responsible for signing off the creation of official Oxfam online accounts and platforms, and for coordinating sign-off of sensitive content as necessary.
- **Database managers:** Responsible for ensuring that all information stored digitally and online by Oxfam is processed in accordance with Oxfam International's Data Protection Policy, and the relevant Oxfam affiliate's Data Protection Policy, as well as any national or regional laws on which these policies are based. In the case of program data, they must also adhere to Oxfam's Responsible Program Data Policy.
- **Managers:** Responsible for promoting awareness of this policy with people they manage and for supporting and developing systems that create and maintain a safe working environment. This includes the responsibility for ensuring that all Employees and Related Personnel receive regular safeguarding training, with a particular emphasis on staff who are in direct contact with partners, representatives, supporters, volunteers, project participants and beneficiaries. Managers should prioritise digital safeguarding awareness-raising for themselves and their divisions, individual departments or teams, and provide budget lines for some activities.
- **Project Teams:** Consult with partners, representatives, supporters, volunteers, project participants and beneficiaries in a safe, accessible, and culturally appropriate way to ensure that they are familiar with the Oxfam Friends Code of Conduct, how to raise complaints and concerns, and Oxfam's processes and procedures for dealing with these. Project Teams should also clearly explain what goods and/or services those involved in Oxfam's work (e.g. project participants) are entitled to, and how they are selected.
- **OI Associate Director for Safeguarding:** Responsible for ensuring that this policy is reviewed at least every three years. All key stakeholders will be responsible for enhancing this policy and incorporating lessons learned into subsequent versions. Feedback from stakeholders will be sought in the process.

6. USE OF EQUIPMENT, INTERNET AND SOCIAL MEDIA

All Oxfam staff must adhere to the Oxfam Staff Code of Conduct, the terms of their employment and the below guidelines when using equipment, internet, social media or digital platforms on behalf of, or belonging to Oxfam. In addition, partners, representatives, supporters, volunteers, project participants, beneficiaries and all those working with Oxfam must adhere to the Oxfam Friends Code of Conduct as well as the below guidelines, and to any other guidelines which are deemed necessary for their relationship with Oxfam.

Oxfam should carry out a Risk Assessment for all initiatives involving social media or digital platforms, or where Oxfam is providing equipment or internet (see Section 8.1 below). Special consideration should be taken where these initiatives involve children, young people and vulnerable adults, and monitoring of usage may be appropriate. See Section 8 for more details.

Where significant risk may exist to individuals (risk of harm, distress, or the infringement of other rights and freedoms), there may be an explicit legal requirement to carry out a Privacy Impact Assessment (PIA). The Risk Assessment may be carried out in conjunction with a PIA, or may itself be a PIA. Affiliates' Data Protection Officers or Focal Points can advise on how this may be undertaken.

6.1 Use of Oxfam's internet and ICT equipment

Usage of equipment or internet which has been provided by Oxfam must follow the relevant affiliate's Acceptable Usage Policy. In particular, the following should be taken into account:

- It is prohibited for anyone to browse, download, access or share content which is illegal, harmful, violent, extremist, sexually exploitative, abusive, offensive or otherwise inappropriate using equipment or internet which has been provided by Oxfam, unless this is required for their role, e.g. safeguarding and investigator roles.
- Parameters for acceptable usage of equipment should be set by Oxfam, and Oxfam may use software to limit what apps or tools staff, consultants or participants are able to access.
- Equipment provided by Oxfam should ensure that technical solutions are in place to protect the user, e.g. anti-virus, monitoring and filtering software.
- Appropriate monitoring should take place based on the level of risk of the people involved (e.g. children, young people, vulnerable adults), and the content which they will be coming into contact with.
- Oxfam should give advice, support and training in how to mitigate risk when using equipment and internet which it has provided.
- Where Oxfam is giving the equipment to a partner, project participant, beneficiary or others involved in Oxfam's work, e.g. at the end of a project, equipment should be cleaned of any personal data. It should be made clear to them that they are now responsible for the use and maintenance of the equipment. In such a case, these guidelines will no longer apply.

6.2 Use of social media and digital platforms

Staff, partners and others working with Oxfam are personally responsible for what they communicate on social media and digital platforms, and when using Oxfam's internet and equipment – both on behalf of Oxfam and in a personal capacity. Published content is often available for anyone to read, and may reflect negatively on the organisation, while those using online platforms as part of Oxfam's work may be exposed to harmful content.

- Oxfam staff, partners and representatives should not behave in a threatening, bullying or abusive way online – whether in a professional or personal capacity.
- Social media, website, channel, shop, project, programme and campaign managers are responsible for signing off the creation of official social media accounts or digital platforms related to Oxfam's programmes, campaigns or initiatives, and accounts and platforms should not be developed without this sign-off.
- Staff responsible for the creation of online content on Oxfam accounts and platforms (e.g. Tweets and Facebook posts) should seek advice and sign-off from these managers or line managers on sensitive content or where they are concerned about the appropriateness of the content.
- When posting potentially upsetting material on Oxfam's social media accounts and platforms, content warnings should be given.
- Children and vulnerable adults should not be tagged in online or social media posts.
- If illegal, harmful, violent, extremist, sexually exploitative, abusive, offensive or otherwise inappropriate content is posted in Oxfam's groups or platforms, this should be hidden or deleted by group moderators, and where appropriate reported to third-party platform hosts. If Oxfam representatives see or are made aware of such content but do not have administration rights to remove it, they should report it to group moderators following the procedures outlined in Sections 12 and 13 below.
- Oxfam should develop appropriate relationships with online platform and social media providers where possible, so that content which may put others at risk can be removed swiftly.
- Oxfam initiatives using social media should be aware of age limits for corresponding social media platforms (e.g. a campaign using Facebook as a key promotion tool should be aware that the minimum user-age is 13).
- If a profile, group, page or platform is set up directly related to Oxfam's programmes, campaigns or initiatives, a minimum of two members of Oxfam staff or representatives should oversee the content and activity as moderators. Moderators should remove or edit inappropriate content as

soon as possible after it has been posted, and should set up mechanisms to pre-approve content where this is enabled by the third-party provider. Moderators should also provide guidelines on rules of engagement.

- Where possible, staff should not make use of their personal social media accounts to carry out their work for Oxfam-related projects, events or initiatives. Where this does not contravene third-party terms of use, a new account should be opened that enables the staff member to maintain boundaries between their personal and professional lives.
- Oxfam staff can only use their Oxfam email address to set up social media accounts if these will be used on behalf of the organisation. Where this account represents an Oxfam initiative, managers should have access to this account, and login details should be shared with other Oxfam staff members so that this account can be used as a shared resource.
- Oxfam staff, partners and representatives should not have private conversations with under-18s through email, or through accounts on social media or online platforms where these are not official Oxfam accounts accessible to others. Where children get in touch with Oxfam through its official social media or online platform accounts, e.g. to ask for more information about a project, processes should be in place so that at least two other staff members are able to view these messages, and are informed when a message is sent to or received from a child. In other instances, if sending a direct message to a child is unavoidable, e.g. to inform them of a sudden change of itinerary for an Oxfam-related event, an adult with a duty of care towards the child (e.g. parent, guardian or teacher) and a relevant Oxfam staff member (e.g. manager or safeguarding focal point) should be copied into the message.
- Oxfam should provide guidelines on settings and privacy to people engaging in digital spaces for Oxfam initiatives to protect them from harmful behaviour.
- Sharing online content of people involved in Oxfam's work on social media should follow the guidelines on privacy, data protection, informed consent, safe programming and risk management outlined below in Sections 7 and 8.

7. PRIVACY, DATA PROTECTION AND INFORMED CONSENT

Oxfam has a duty of care to protect the digital data and content of staff, partners, representatives, volunteers, supporters, project participants, beneficiaries and others involved in Oxfam's work, even when they make the informed decision to share this content. This duty of care is rooted in privacy law, and includes an obligation to be transparent in explaining how Oxfam will use individuals' data, how Oxfam considers the risk to individuals, and how Oxfam cares for their data throughout the lifespan within which it will be used.

Oxfam must take every reasonable precaution to ensure that any digital data or content does not place people at risk or render them vulnerable to any form of harassment, abuse or exploitation.

Research which involves digital elements, such as online surveys or platforms, must be well thought through and appropriate for the context. Special consideration must be given to data protection concerns and mitigating risk to research participants.

Oxfam staff must adhere to Oxfam International's Data Protection Policy, the relevant Oxfam affiliate's Data Protection Policy – and in the case of program data, Oxfam's Responsible Program Data Policy. They must also adhere to the relevant Oxfam affiliate's Acceptable Usage Policy and Information Security Policy. All information stored digitally and online by Oxfam must be processed in accordance with these policies, which may reflect any national or regional laws on which Data Protection Policies are based, such as the *General Data Protection Regulation (GDPR) in the European Union (2018)*.

7.1 Minimum principles

Standards and guidelines are contained in the above policies where applicable, in each affiliate's Privacy Business Standards, in the accompanying training and material (e.g. Data Rights material, Responsible Data Training Pack), and in other accompanying material which supports their implementation. This Digital Safeguarding Policy does not replace these policies, but any digital activities must embrace the following principles at a minimum, which align with GDPR:

- Oxfam is **transparent, lawful, and fair** with individuals when using their data, and will explain to individuals how it will use data when it collects or obtains it.
- Oxfam will only use data for the **purposes for which it was obtained** and then destroy it appropriately. Oxfam will not retain or use this information to contact or work with people for any other reason.
- Oxfam will only collect the **minimal amount of data** for the purpose at hand.
- Oxfam will retain **accurate data** and keep it for **no longer than necessary.**
- Oxfam will ensure its data is stored **securely** and access is restricted to as small a number of staff as possible.
- Oxfam will always seek written **parental consent** prior to collecting and using data related to children. The consent form must be sensitive to children, it must stipulate what channels the content will be used on, and it must outline that social media content will exist indefinitely unless the parents or child ask for it to be deleted.
- Oxfam will only **disclose personal information outside of Oxfam** in an identifiable form if explicit consent has been given for this or there is a compelling legal reason (or similar overriding interest) which is considered and risk-assessed.
- Oxfam will comply fully with any **local data protection legislation**.
- Oxfam will ensure that, from their inception, **projects and activities which involve data** must include a **planned-in consideration** for the protection of confidentiality of data (**security**) and the privacy and agency of individuals (**privacy**).

7.2 Informed consent

Oxfam should ensure that informed consent is obtained for the gathering of content which will be shared publicly in the digital sphere. This should ensure that the person truly understands what they are consenting to, with full knowledge of the possible risks and benefits. Privacy and data protection law which outlines legal requirements for gathering and using data may in some instances require or present an option for consent, and this should be considered alongside this process of informed consent. However, the below guidelines for gathering and sharing content online represent a requirement for ethical consent which supplement these legal guidelines, and which Oxfam has committed to.

- Oxfam's Ethical Content Guidelines must be followed when gathering content. These include guidelines on Informed Consent which should be followed.
- For children, Oxfam must seek informed consent from a parent or guardian, in addition to attaining informed assent from the child, where they are old enough to understand.
- Adults, children's parents/guardians, and – where possible – children must be given enough context to make this context 'informed'. In particular, they must be able to reasonably understand how their image or likeness may be used, and what the consequences may be.
- Images, stories, recordings or other personal data of children should not be accompanied by identifying information when shared online, e.g. the child's real name or school name. This applies even if a parent/guardian gives informed consent for a child to be interviewed in a way that reveals their identity. Exceptions can only be made in specific circumstances, e.g. where a child has won a prize or led a campaign and this has been widely reported in the media, where a full Risk Assessment has been carried out and the identified risks are minimal, and where informed consent is obtained following this Risk Assessment.

- Identifying information should not be included when content is shared online where this may put people at risk, e.g. political harassment, targeting by religious extremists.
- A story-gatherer (e.g. interviewer, photographer, video-maker) should exercise judgement and creative skills to tell a powerful story in a way that doesn't reveal the identity of a child, young person, vulnerable adult, or someone who may be put at risk due to e.g. political or religious contexts.
- Participants retain the right to remove any pictures or stories about them from online spaces at any stage and should be made aware of this.
- There must be a practical means for adults, children's parents/guardians, and – where possible – children to contact Oxfam to allow them to assert this right.
- Content should receive the appropriate levels of sign-off when gathering content and before sharing it online.
- There are some key areas where Oxfam needs to be extremely alert and sensitive to sharing content online as there may be additional risk, and this may be ongoing.
    - Emergency situations – vulnerable, traumatised or orphaned individuals
    - Conflict situations – as above and combatants
    - Abuse – survivor of any form of abuse
    - Crime – perpetrators or survivors of a crime

8. SAFE PROGRAMMING AND RISK MANAGEMENT

8.1 Digital Risk Assessment

Effective contextual analysis is essential to identify potential risks for staff, partners, representatives, volunteers, supporters, project participants, beneficiaries or others involved in Oxfam's work when operating online. Assessed risks, potential consequences and mitigation strategies should be considered before any programmes, campaign, activities or initiatives which have a digital element begin.

Relevant Oxfam staff can offer support to ensure that these assessments are gender-sensitive and participatory. Oxfam's Data Protection Officers should advise on whether a Privacy Impact Assessment is required to supplement the Risk Assessment.

The following elements should be taken into consideration:

- The social, cultural and political context which may increase risk.
- Campaigning, advocacy and influencing work which entails risk of harassment or targeting by political, religious or cultural actors.
- The individual situation of the people involved in Oxfam's work – including intersectional factors relating to race, ethnicity, religion, age, sex and gender identity/expression, sexual orientation, (dis)ability, political affiliation, and any other status which may put them at risk.
- When working with children, discussions must address how parents or legal guardians will be informed of any significant risks and involved in decision making before they start their engagement with Oxfam.

8.2 Risk Mitigation

The extent of the risks identified in the Risk Assessment will determine whether Oxfam should mitigate against these by restricting Oxfam's online activities, or advising those involved in Oxfam's work against online activity. In addition, they should not undertake online activities through Oxfam if:

- There is a risk of identification through online activities, where this may put them at risk (e.g. political harassment, sexual abuse, targeting by religious extremists).
- It is deemed to put them at risk of violence (e.g. gender-based violence, political violence).
- It involves risk of accidents which they are unlikely to recognise (e.g. due to lack of awareness of online risks or lack of online experience).

- There is any other restriction specific to local legislation or cultural issues, e.g. internet censoring.
- They are of compulsory school age and this would harm school attendance or academic performance.
- There is a risk of child exposure to illegal, harmful, violent, extremist, sexually exploitative, abusive, offensive or otherwise inappropriate content.
- There is no way for Oxfam to mitigate risks.
- The outcome of a Risk Assessment and/or Privacy Impact Assessment indicates that there would be high risk to individuals for these or other factors.

9. CHILDREN AND YOUNG PEOPLE

Oxfam recognises that children and young people are a group who experience specific risks in the digital sphere, and that special measures should be taken to ensure that they are protected from abuse, harm and exploitation when engaging with Oxfam's online work.

Special considerations include:

- Oxfam should obtain informed consent from the child and/or parent or guardian of the child for the processing of children's data. An explanation of how the data will be used must be provided.
- Guidelines on informed consent and identification of children must be followed when gathering content to share publicly (see Section 7.2 above for more information).
- Oxfam should not support children to engage in Oxfam's work through social media or digital platforms when they are under the minimum joining age set by the third-party provider. It is Oxfam's responsibility to be aware of minimum age requirements, which vary across third-party platforms (e.g. on Facebook the minimum user-age is 13). For children over the minimum joining age, a Risk Assessment should determine whether social media platforms are the most appropriate way for Oxfam to engage with them.
- For sensitive programmes and campaigns, children and their parents or guardians may be asked to sign an End User Policy before they can engage with Oxfam digital initiatives.
- Oxfam should provide guidance and tools to children and young people to protect themselves when using equipment, internet, social media or digital platforms to work and engage with Oxfam. Appropriate training should also be provided where possible. This includes, but is not limited to: social media privacy settings, online security, sharing content, and engaging with others online.
- The use of technical equipment, internet, social media or digital platforms not only carries individual and technical risks but also collective and social risks that could increase the gap between people that have access to the digital world and those who do not. It can also push people into groups and promote polarisation, which is particularly relevant for young people who are forming their identities. Whenever Oxfam engages with young people in a way that includes digital work, these elements should be considered and discussed with youth participants.

Any programmes, campaigns or initiatives which work with children or young people should also refer to the One Oxfam Child Safeguarding Policy and the One Oxfam Youth Safeguarding Policy (forthcoming).

10. BREACHES OF THE POLICY

Breaches of the Policy will not be tolerated and may result in disciplinary procedures, change of duties, termination of employment or relationship, and possible legal proceedings, for Oxfam staff, contractors, volunteers or people working in Oxfam's name.

Oxfam will take action against anyone, whether they are the subject of a complaint or not, who seeks to or carries out retaliatory action (such as, but not limited to, harassment, intimidation, unfair disciplinary action or victimisation) against complainants, survivors or other witnesses. Employees who are found to do this will be subject to disciplinary action, up to and including termination of employment. Others who work with Oxfam may have their relationship with Oxfam terminated.

If an Oxfam employee is found to have made an allegation that they knew to be false they will be subject to disciplinary action, up to and including termination of employment. Others who work on behalf of Oxfam will be subject to action that may result in the termination of their relationship with Oxfam.

Further information about the process of investigations and outcomes can be found in the Safeguarding Case Management Standard Operating Procedures (forthcoming).

11. SUPPORT FOR SURVIVORS

Survivors are entitled to specialised support services. Oxfam commits to referring survivors to competent support services as appropriate and available and according to the wants and the needs of the survivor. Support may include specialist psychosocial support such as counselling, medical assistance, legal counselling and access to Oxfam's Employee Assistance Programmes (where available). Assistance will be made available regardless of whether a formal internal response is carried out (such as an internal investigation). For further details, please refer to the One Oxfam Survivor Support Policy (forthcoming).

12. HOW TO RAISE A COMPLAINT OR CONCERN

Anyone can raise a concern about inappropriate or illegal content which has been posted online relating to Oxfam's initiatives. Concerns should be raised with social media, website, channel, shop, project, programme or campaign managers as appropriate, so that they can moderate and remove this content and report to a third-party service provider. In the case of illegal content or a safeguarding concern, this should be raised with Safeguarding Teams and Leads so that they can deal with this appropriately and refer to the police or a support service where necessary.

Oxfam Employees and Related Personnel have a responsibility to report any suspicion or concerns concerning digital safeguarding. Any individual can raise a concern/complaint to Oxfam about an incident they have experienced, witnessed, or heard about concerning an Oxfam staff member or partner (suppliers, partners, contractor, etc.) without fear of retribution. Oxfam Employees and Related Personnel ***must not*** investigate allegations or suspicions themselves.

Issues relating to data protection should be reported to Oxfam's Data Protection Officers and Privacy Focal Points (details on COMPASS – internal to Oxfam staff only). These can also be reported through the contact details specified Oxfam International's Data Protection Policy, and the relevant Oxfam affiliate's Data Protection Policy. For further details regarding reporting a concern, please refer to One Oxfam PSEA Policy.

13. HOW TO RESPOND TO A COMPLAINT OR CONCERN

Oxfam is committed to responding to all complaints and concerns relating to digital safeguarding. Social media, website, channel, shop, project, programme and campaign managers should be contacted in the first instance as they are responsible for moderating and removing inappropriate online content and flagging this with third-party providers where appropriate. They are also responsible for contacting third-party providers to report this content, and where Oxfam is not able to remove content which poses a risk.

Illegal content and safeguarding issues should be referred to Oxfam's Safeguarding Teams and Leads – it will then be established whether a copy or screenshot of the online content should be saved for use in future internal or external investigations. Data Protection Officers and Privacy Focal Points are responsible for responding to issues relating to data protection and privacy, and in some countries may have specific legal responsibilities including a duty to be consulted on matters relating to privacy risk.

Oxfam's Safeguarding Leads are responsible for all other concerns or complaints and have specialist expertise in prevention of and response to exploitation and abuse, including referrals for assistance and investigation. If in doubt, please contact the Safeguarding Teams and Leads (see Annex 2 of the One Oxfam PSEA Policy for Affiliate specific contacts).

Oxfam recognises that disclosures and suspicions should always be acted upon swiftly. If there is an urgent safeguarding situation, e.g. a supporter, project participant or beneficiary shares online that they are in imminent danger of harm or abuse, then immediate protective action must be taken. The Safeguarding Teams and Leads should be contacted immediately in these instances and all reasonable measures should be taken to prevent harm, e.g. by contacting the police or appropriate support service directly where possible.

ANNEX 1: DEFINITIONS

For the purposes of this Policy and Oxfam's approach to Digital Safeguarding, these definitions apply. Further definitions can be found in the One Oxfam PSEA Policy.

- **Data protection:** The process of protecting the rights and freedoms of individuals in respect of the use of their Personal Data. "Personal Data" means any information relating to an identified or identifiable natural person (a "data subject"). Oxfam has an obligation under applicable privacy and data protection laws to protect the personal data which it collects and processes.
- **Child:** A child is defined as anyone under 18 years old. This definition is recognised internationally as identifying a population who are particularly vulnerable and require additional safeguards to protect their rights. The definition of a child for the purposes of safeguarding should not be confused with the legal definition of a child or age limits set out in other relevant laws. The fact that a young person under the age of 18 may have reached the age of e.g. sexual consent, voting age etc. does not alter their inherent vulnerability as a child.
- **Young People/ Youth:** Oxfam defines a young person as being between the ages of 15 and 24, in line with the UN definition. However, we recognise that definitions change between countries and cultural contexts – the African Youth Charter, for example, defines young people as those between the ages of 15 and 35. When using the term youth or young people, we recognise that young people are not a homogeneous group and experience different levels of privilege and marginalisation that should be taken into account.
- **Vulnerable adult:** A vulnerable adult is any person aged 18 years and over who is or may be in need of community care services by reason of mental health issues, learning or physical disability, sensory impairment, or unable to protect themselves due to age or illness and who may be unable to take care of themselves or unable to protect themselves against significant harm or serious exploitation. This includes people encountering domestic abuse, substance misusers and asylum seekers. An elderly person, while they may require extra support, does not necessarily meet the definition of adult at risk.

ANNEX 2: SPEAK-UP CHANNELS

Please see Annex 2 of the One Oxfam PSEA Policy for Affiliate specific speak-up channels.