Guidance of the Secretary-General

Human Rights Due Diligence for Digital Technology Use

Call to Action for Human Rights
May 2024

United Nations

Table of Contents

I. About this guidance

A. Why has this guidance been developed?

Guidance on Human Rights Due Diligence for Digital Technology Use (the guidance) has been developed to support all United Nations (UN) entities to implement and strengthen human rights due diligence (HRDD) policies, processes and practices for the use of digital technologies. This guidance should be read in conjunction with the 1 June 2023 Executive Committee Decision regarding Expansion of Human Rights Due Diligence in the United Nations. The principles and parameters outlined in the 1 June Decision apply to the Guidance on HRDD for Digital Technology Use. The scope of the guidance encompasses the full digital technology lifecycle and value chain - including the conception, design, development, acquisition, use, further deployment, sharing and disposal of digital technologies. It recognizes that a UN entity could potentially be connected with adverse human rights impacts that occur at any point of this lifecycle and value chain. It seeks to support UN entities to adopt a risk-based approach that prioritizes action to address the most severe human rights risks and impacts associated with digital technology use, commensurate with the nature of the human rights risks or impacts, how the entity is connected with the risks or impacts, and the entity's resources.

The guidance has been developed by the Office of the High Commissioner for Human Rights, in consultation with UN entities and external stakeholders. The guidance is grounded in the Secretary-General's *Call to Action for Human Rights*[1] and *Our Common Agenda,*[2] which call for the application of human rights frameworks to the digital space and basing all UN engagement in this area on human rights risk assessments. It was developed in response to the *Roadmap for Digital Cooperation,*[3] in which the Secretary-General tasked the Office of the High Commissioner for Human Rights with developing guidance on HRDD and impact assessments for the use of digital technologies. Both the Call to Action and the Roadmap recognise that digital technologies provide new means to advocate for, defend and exercise human rights. The guidance aims to assist UN entities to achieve those positive impacts in their digital technology use, consistent with the UN's purposes and principles.

HRDD is important for credible and effective management of human rights risks to people, as well as management of reputational and operational risks. It has been embedded in international standards, and it is increasingly reflected in national and supra-national policy and regulatory requirements. HRDD processes and expectations are already in place within the UN system – variously at Secretariat-wide and entity levels – and a process is underway to develop the Secretary-General's Human Rights Due Diligence Framework Policy (HRDD Framework Policy). HRDD offers a principled and practical approach to identifying and

[1] United Nations, The Highest Aspiration: A Call to Action for Human Rights (2020).
[2] United Nations, Our Common Agenda: Report of the Secretary-General (2021).
[3] United Nations, Roadmap for Digital Cooperation: Implementation of the recommendations of the High-level Panel on Digital Cooperation (2020) at 18, [86].

addressing adverse human rights impacts and, in turn, realizing the rights of affected people and groups[4] (also known as rightsholders), thereby promoting the UN's purposes and principles.

This guidance is not intended to inhibit or limit the use of digital technologies or digital innovation across the UN, many of which are critical to the UN's operations and other activities. However, it recognizes that proactive and effective measures to identify prevent, mitigate and address adverse human rights risks and impacts connected to digital technology use are important to achieve positive outcomes for affected people, manage unplanned operational and reputational risks to the UN, and strengthen relationships with relevant stakeholders.

As noted above, this guidance has been developed in coordination and alignment with the process to develop the HRDD Framework Policy, and – as guidance – does not alter or supersede laws, policies or other rules that bind UN entities. Where elements of this guidance conflict with applicable laws, policies or rules, UN entities shall observe applicable laws, policies and rules, and are encouraged to strive to meet the spirit of this guidance to the extent possible.

B. Who is this guidance for?

The guidance has been developed for all UN entities and, in particular, the work units that will be responsible for or otherwise involved in the implementation of HRDD for digital technology use by their UN entity.

This guidance also offers information about the UN's HRDD approach to third parties, such as partner organisations, private sector partnerships (including donation, shared value and non-financial partnerships), suppliers and Member States.

The guidance provides a practical introduction to HRDD to assist in the design, development, implementation and strengthening of each UN entity's HRDD for digital technology use. Each UN entity should endeavor to build its resources and capability to implement this guidance on a progressive and phased basis, and in a manner that gives due regard to and does not compromise its mandate(s).

The Office of the High Commissioner for Human Rights recognises that UN entities working to implement the guidance may benefit from additional tools and resources to support roll-out and implementation of this work, as well as mechanisms to support peer learning and sharing of insights and approaches within and between UN entities. Proposals to develop such additional support will be developed in coordination with a working group including members of the HRDDP Review Group and the Department of Management Strategy, Policy and Compliance. It is anticipated that such an implementation support team would collaborate closely with the HRDDP Review Group to ensure complementarity with the HRDD Framework Policy, and that additional support structures could be established in the field as appropriate.

C. Why should UN entities implement HRDD for digital technology use?

UN entities should implement HRDD to identify, prevent, mitigate and address potential or actual adverse human rights impacts to which they

[4] For the purposes of this guidance, the term 'affected people and groups' refers to people and groups whose human rights have been adversely impacted.

may be connected through their digital technology use and, in doing so, align with broader UN prevention efforts and help achieve positive human rights outcomes for the relevant affected people and groups.

Article 1 of the UN Charter establishes that a fundamental purpose of the UN is to promote and encourage respect for human rights and fundamental freedoms.[5] HRDD supports UN entities to know and show that they themselves operate with respect for human rights in their use of digital technology – helping ensure a credible foundation from which to promote and encourage respect for human rights and fundamental freedoms by others, States and businesses alike. Further, actively addressing human rights risks and impacts can substantially contribute to an entity's efforts to help achieve the Sustainable Development Goals by addressing systemic issues that leave people behind (for example, gender and racial inequality, hazardous working conditions, violence against women and girls, child labor and discrimination) and by using digital technology in a rights-respecting way to enable and facilitate sustainable development.

As discussed above, embedding respect for human rights in relation to digital technology use, in particular, has been identified as a priority for the UN system by the Secretary-General.[6]

It is recognized that the priorities of UN entities must be to fulfil their individual mandates, which vary extensively across entities and include maintaining international peace and security, promoting conditions of economic and social progress and development, promoting enjoyment of all internationally-recognized human rights, responding to emergencies on an urgent basis, meeting the immediate needs of affected people and taking into account the humanitarian principles of humanity, neutrality, impartiality and independence. Implementing effective HRDD for digital technology use should assist UN entities to fulfil their mandates.

[5] United Nations, Charter of the United Nations (1945).

[6] United Nations, Roadmap for Digital Cooperation: Implementation of the recommendations of the High-level Panel on Digital Cooperation (2020) at 18, [86].

II. Using this guidance

A. How to use this guidance

The implementation of HRDD should be an iterative and progressive process.

Why? Because identifying and addressing human rights risks and impacts associated with digital technology use can be complicated, and the human rights risk landscape of any entity will likely evolve over time (for example, due to changes in its activities, operating environments, relationships or the digital technologies that it uses). Effective HRDD is an ongoing process and recognises that complexity and is responsive to changing circumstances. This is discussed further below.

Because of this complexity, implementing HRDD for digital technology use is unlikely to be a neat, linear process or a standalone piece of work. Instead, it should involve taking initial steps, reflecting on what has been learned, and working to expand, strengthen and refresh processes to ensure HRDD is effective.

This guidance therefore offers practical guidance on:

- Five key components of effective HRDD for digital technology use.
- How to get started and then over time strengthen HRDD for digital technology use.

Teams involved in implementing HRDD for digital technology use should consider this and any other applicable frameworks or guidance and then recommend the appropriate next steps for their entity. For example, if their entity is new to HRDD, those steps may include desktop research and conversations with internal and relevant external stakeholders, or an internal workshop, to learn about key human rights risks and issues related to the entity's digital technology use. If their entity is already familiar with human rights risks and impacts connected to its digital technology use, it may find it is helpful to develop a pilot initiative to generate some initial insights and learnings to inform the implementation of more comprehensive HRDD.

Implementation should build on and integrate with relevant existing Policies, Guidance and Processes at UN System and entity level, including the UNSDG Common Approach to Due Diligence in Business Sector Partnerships,[7] the High Level Committee on Management Statement and Guidance to combat trafficking and forced labor in United Nations supply chains,[8] the United Nations Model Environmental and Social Standards,[9] the United Nations Protocol on Allegations of Sexual Exploitation and Abuse against Implementation Partners,[10] the UN Principles for the Ethical Use of Artificial Intelligence in the UN System[11], UNESCO's Ethical Impact Assessmentand[12], and the United Nations Partnership Portal,[13] among

[7] https://unsdg.un.org/resources/unsdg-common-approach-prospect-research-and-due-diligence-business-sector-partnerships
[8] https://unsceb.org/combatting-human-trafficking-and-forced-labour-un-supply-chains
[9] https://www.undp.org/publications/undp-social-and-environmental-standards
[10] https://www.un.org/en/pdfs/UN%20Protocol%20on%20SEA%20Allegations%20involving%20Implementing%20Partners%20-%20English_Final.pdf
[11] https://unsceb.org/principles-ethical-use-artificial-intelligence-united-nations-system
[12] https://unesdoc.unesco.org/ark:/48223/pf0000386276
[13] https://www.unpartnerportal.org/landing/

others. UN entities can develop their own policies, guidance and standard operating procedures to implement HRDD for digital technology use. For UN entities with established and relevant HRDD processes in place, this guidance may assist in reviewing those processes and identifying opportunities to ensure human rights risks and impacts associated with digital technology use are identified, prevented, mitigated and/or addressed effectively, while simultaneously building policy coherence across the UN system.

What matters most is that the entity is committed to taking a rights-based approach to its digital technology use and achieving positive outcomes for affected people – and that the entity implements effective HRDD processes based on common standards[14] applied consistently across the UN system, a crucial element for UN policy coherence. By doing so, UN entities can strive to ensure that technical support and cooperation from the United Nations, including its agencies, funds and programmes, is not connected with human rights risks or violations.

B. HRDD for digital technology use: Overview

HRDD for digital technology use should enable an entity to know and show how it is identifying, preventing, mitigating and addressing actual and potential adverse human rights impacts connected with its digital technology use.

HRDD for digital technology use should always:

- Seek positive human rights outcomes for affected people.
- Be informed by efforts to identify and engage with stakeholders, including affected people.
- Be ongoing and dynamic.
- Be risk-based and context-sensitive.
- Be based on common standards, outlined below in this document.
- Apply a gender lens and principles of inclusion and intersectionality.

Provided below is a high-level overview of the key components of effective HRDD for digital technology use. More information about each is provided in section IV, below.

[14] Of note, the principles and parameters of the current Human Rights Due Diligence Policy and ongoing work to develop an HRDD Framework Policy.

HRDD FOR DIGITAL TECHNOLOGY USE: FIVE KEY COMPONENTS

Meaningful engagement with affected people and other stakeholders

A. Embed

Human rights risk management should be embedded within the entity to establish the foundations for effective HRDD for digital technology use.

Embedding should progress concurrently with other components of HRDD. As a first step, the entity should decide which individual(s), team(s) or function(s) will play a role in designing and implementing HRDD for digital technology use, and identify the lead(s) with overall responsibility for this work.

B. Identify and assess

Processes to identify and assess actual and potential human rights impacts should support the entity to make and implement a plan to address the adverse impacts with which the entity is (or may be) connected through its digital technology use across the full digital technology lifecycle and value chain.

C. Take action

An entity should take action that seeks to prevent, mitigate and, where applicable, appropriately redress the actual and potential adverse human rights impacts that it has identified.

What constitutes an appropriate response will vary with how the entity is connected and the extent of its leverage to encourage others also to act (or refrain from acting).

D. Track

An entity should take steps to track both the implementation and effectiveness of its HRDD for digital technology use across the technology lifecycle.

E. Communicate

An entity should communicate clearly internally and externally about how it addresses adverse human rights impacts connected to its digital technology use. Communication does not necessarily require formal reporting – although an entity may choose to do this, including to affected stakeholders.

III. About HRDD for digital technology use

A. What is HRDD for digital technology use?

HRDD is a process that enables an entity to identify and address its human rights risks and impacts effectively. It encompasses the measures the entity takes to know what its human rights impacts may be and to show how it is addressing them. It can complement and be implemented alongside broader human rights-based approaches used by an entity.

HRDD for digital technology use enables an entity to manage potential and actual human rights impacts with which it is connected through its use of digital technologies.

As noted above and discussed in more detail below, HRDD should be implemented via policies, processes and practices that enable an entity to systematically take the following steps:

- Embed HRDD for digital technology use.
- Identify and assess actual and potential adverse impacts.
- Take action to cease, prevent or mitigate impacts.
- Track implementation and effectiveness.
- Communicate how it addresses impacts.

While UN entities should apply the same broad standards in implementing HRDD to support consistency and coherence, there is no 'one right way' to implement HRDD for digital technology use. To be effective, HRDD needs to be tailored to and commensurate with the entity's size, its risk of connection with human rights impacts, the nature and context of its operations and the way in which digital technologies are deployed to fulfil its mandate.

However, at a minimum, HRDD should always:

- Seek positive human rights outcomes for affected people.
- Be informed by efforts to identify and engage with stakeholders, including affected people.
- Be ongoing and dynamic.
- Be risk-based and context-sensitive.
- Be based on common standards, outlined below in this document.
- Apply a gender lens and principles of inclusion and intersectionality.

It will take time, effort and creativity to learn what works best for the entity and to build internal capacity and capability to implement HRDD for digital technology use effectively.

While HRDD should focus on achieving positive outcomes for affected people, it will not always be possible for an entity, acting alone, to manage identified risks or address/'fix' an adverse human rights impact. Often, many actors – including other UN entities, private sector entities, government authorities and civil society stakeholders (including human rights defenders) – will have a role to play to identify and address an impact, and they are likely to need to work together.

B. Which human rights risks are associated with digital technology use?

HRDD for digital technology use should encompass all internationally recognized human rights.

Why? Because a UN entity could potentially be conncted to impacts on any internationally recognised human right through its digital technology use across the lifecycles of the technologies that it uses.

For example, where material used to train artificial intelligence algorithms reflects systemic discrimination on the basis of race, age or gender, the development and use of that technology may adversely impact the right to freedom from discrimination. Where electronic devices are manufactured at a facility that retains the passports of migrant workers and provides substandard worker accommodation, an entity that procures the devices may become associated with modern slavery, adverse impacts on the right to just and favorable working conditions, and the right to adequate housing.

Some situations will be less straightforward – particularly where the use of digital technology may involve both positive and adverse human rights impacts. For example, social media platforms may be leveraged to share information with forcibly displaced people on how to avoid protection risks, such as trafficking or forced labor, and how to access humanitarian assistance, supporting realization of the right to life, liberty and security. However, an entity using social media platforms to engage with forcibly displaced communities must also to identify and address the risks of relying on a platform whose personal data collection and sharing model may be in breach of the right to privacy and data protection principles and that could otherwise single out, identify and target at-risk individuals (potentially creating risks to the right to life, liberty and security). Digital technologies present certain challenges to the data protection principles of fair and legitimate processing, purpose specification, proportionality and necessity, retention, accuracy, confidentiality, security, transparency, transfers and accountability.[15]

Entities should recognize that their digital technology use may affect individuals and groups differently on the basis of age, actual or perceived sexual orientation, gender identity, gender expression or sex characteristics. Technology may amplify risks to people and groups already at heightened risk of vulnerability and marginalization – including ethnic, racial and religious minorities, Indigenous peoples, and those affected by armed conflict and other types of violence, and exacerbate the digital divide. For example, digital technology can facilitate the use of online spaces to identify and recruit children and young people to join non-State armed groups.

HRDD should aim to prevent and address the risk that digital technology use (across the lifecycle) may exacerbate inequalities or biases, or result in adverse impacts on groups at risk of vulnerability and marginalization.

Given that the challenges of scale may mean it is not possible to address all identified human rights risks and impacts simultaneously, entities should take a risk-based approach to prioritization and begin by addressing the most severe actual or potential human rights risks and impacts associated with their digital technology use. (See Box 4 for more on assessing severity.)

[15] Personal Data Protection and Privacy Principles. Adopted by the UN High-Level Committee on Management (HLCM) at its 36th Meeting, October 2018.

At a minimum and as required by their mandates, UN entities should take action to prevent and address all grave violations or grave abuses[16] of international humanitarian law, international human rights law or standards, or international refugee law associated with their digital technology use.

Other identified human rights risks and impacts should be subsequently addressed and best efforts should be made to prevent and mitigate them in a comprehensive and timely manner.

BOX 1 | ILLUSTRATIVE POTENTIAL IMPACTS ACROSS THE LIFECYCLE

The list below is not intended to be comprehensive, but rather to illustrate at a high level some examples of human rights that may potentially be impacted at different stages of the digital technology lifecycle (and value chain).

Digital technology lifecycle	Examples of potential human rights impacts
Conception	• Bias and discrimination • Privacy
Design and development	• Bias and discrimination • Hazardous working conditions • Life, liberty and personal security • Privacy • Right to an effective remedy
Acquisition (including materials, manufacture, transport and logistics)	• Children's rights • Clean, healthy and sustainable environment • Freedom of association • Hazardous working conditions • Health and safety • Livelihoods and housing • Modern slavery, forced labor and trafficking
Use, further deployment and sharing	• Bias and discrimination • Clean, healthy and sustainable environment • Freedom of expression, access to information • Health and safety • Life, liberty and personal security • Privacy • Right to an effective remedy • Right to seek and enjoy asylum
Disposal (including recycling)	• Clean, healthy and sustainable environment. • Hazardous working conditions • Health and safety • Privacy

[16] https://unsdg.un.org/sites/default/files/Inter-Agency-HRDDP-Guidance-Note-2015.pdf, para 12.

C. How can UN entities be connected to these adverse impacts?

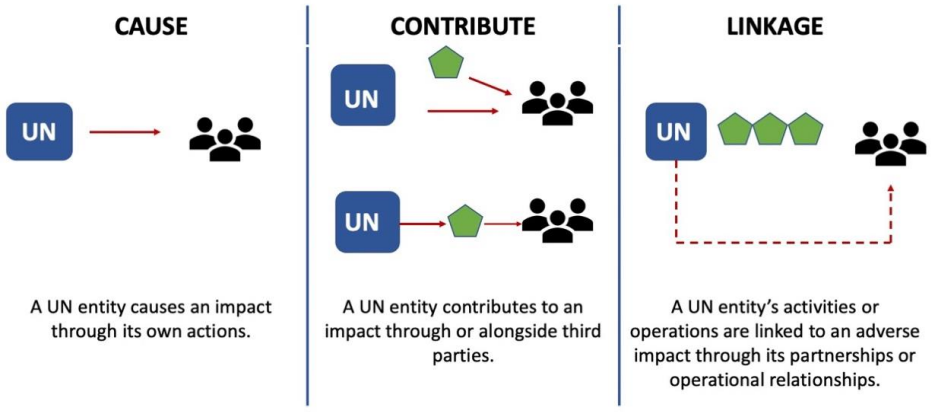
There are three ways in which a UN entity can be connected to an adverse human rights impact through its digital technology use: causation, contribution and linkage (Figure 1).[17] These can be understood as a continuum – an entity may shift between categories based on its actions or inactions, including through its implementation of HRDD for digital technology use.

An entity's HRDD for digital technology use should enable it to identify and address impacts that it has caused or contributed to, or with which it is linked. How it is connected to a potential or actual adverse impact will guide how it should respond.

Importantly, each party connected to an impact has its own responsibility to respond. For example, where a UN entity is linked to an impact, there will be one or more third parties that have caused or contributed to the impact that also have their own responsibility to discharge. Action by the UN entity to address the impact does not displace the responsibility of the third parties – nor does action by a third-party shift or alter the UN entity's responsibility. Effective efforts by all parties connected to the impact should ideally result in the sum of those actions preventing, mitigating and/or redressing the impact.

Connection with adverse human rights impacts is dynamic – a UN entity's connection may shift along the continuum as a result of its actions or inactions, as well as those of other third parties connected to an adverse impact. For example, an entity that takes effective steps to address its contribution may shift to the 'linkage' category. By contrast, a UN entity that is linked to an impact and takes no action may find its connection shifts to contribution over time.

FIGURE 1 | CONTINUUM OF CONNECTION



[17] These terms reflect and seek to align with well-established approaches to conceptualizing an organization's connection to (or involvement in) adverse human rights impacts, as reflected in the UN Guiding Principles on Business and Human Rights (2011) and other authoritative HRDD standards and guidance resources. The terms 'causation' and 'contribution' are not intended to imply or establish legal liability in respect of an impact, but rather to provide a practical basis on which to understand a UN entity's potential connection and consider how it should respond as it implements HRDD for digital technology use.

BOX 2 | EXAMPLES OF CONNECTION WITH ADVERSE HUMAN RIGHTS IMPACTS

1. Causation | A UN entity causes an adverse impact through its own activities.

Example: Where an entity collects or shares personal data of individuals that is processed in digital systems without adequate data protection safeguards, it may cause an adverse impact on the right to privacy, (and possibly other human rights).

Expected action: The entity should seek to prevent or mitigate the impact – for example, by putting in place adequate data protection safeguards. If the adverse impact nonetheless remains severe, it should consider ceasing the activities (see Box 5).

2. Contribution | A UN entity contributes to an adverse impact through or alongside third parties (including operational partners, business or partnership relationships with the private sector or State entities).

Example: Where a UN entity provides biometric data collection technology to a police service that uses the technology to track and persecute human rights defenders, the UN entity may have contributed to an adverse impact (in this scenario, the police service, or support recipient, would have caused the impact). As noted, this is not a legal conclusion but a normative one, reflecting expectations of the UN similar to those found in the UN Guiding Principles on Business and Human Rights for businesses.

Expected action: The UN entity should cease or prevent its contribution and use leverage to mitigate any remaining impacts to the greatest extent possible. In this example, such actions may include ceasing the provision of the technology to the police service, and identifying ways to encourage the service to cease using the technology to persecute human rights defenders. It should also consider providing, participating in or encouraging the provision of remedy to affected people by the responsible State.

3. Linkage | A UN entity is not causing or contributing to an adverse impact, but its activities or operations are linked to it through the entity's partnerships or operational relationships.

Example: Where an entity sources and uses a technology product that contains components that were manufactured by workers in a situation of forced labor, the entity will be in a situation of linkage.

Expected action: The entity should use its leverage to advocate with the manufacturer (and any third parties that have contributed to the impact) to prevent, cease and mitigate the impact. If it does not have sufficient leverage, it should seek to build or strengthen its leverage. For example, it could do this by setting and enforcing clear expectations of suppliers regarding forced or bonded labor,[18] engaging with entities in its supply chain to build awareness and know-how to address forced or bonded labor, and by participating in collaborative initiatives to address root cause challenges associated with forced and bonded labor.

4. Not connected | A UN entity is not connected to an adverse impact.

Example: A UN entity partners with a technology company to develop an algorithm that enables it to use social media platforms to share information about access to the UN entity's assistance and services with the communities it works with and for. The technology company is alleged to source widgets from a supplier that requires excessive overtime from workers. There is no connection between the widgets and the algorithm the company helps the UN entity to develop.

Expected action: No action is expected. However, the UN entity may choose to encourage the technology company (and potentially other parties connected) to address the impact, or to partner with a different technology company. In addition to the positive impact on workers' rights, the UN entity may act to manage its reputational risks.

See Box 5 for more information on using leverage.

[18] Addressing Forced Labour and Human Trafficking in UN Supply Chains: Guidance for UN Staff

IV. Practical approaches to implementing HRDD for digital technology use

In the sub-sections below, additional detail and practical guidance is provided to support UN entities to implement the five key components of effective HRDD for digital technology use.

BOX 3 | ENGAGING WITH STAKEHOLDERS

Meaningful engagement with stakeholders – and, in particular, potentially affected people and groups - should inform every stage of an entity's HRDD for digital technology use. It should enable the entity to receive, understand and respond to stakeholders' interests and concerns, including through collaborative approaches.

Relevant stakeholders are likely to include, but are not limited to:

- Potentially and actually affected people and groups (or their legitimate representatives).
- Credible proxies for the views of affected people or groups (which may include civil society organisations, trade unions and faith-based organisations).
- Individuals and organisations with relevant human rights (including digital rights) and/or digital technology expertise.
- Partners involved in the entity's digital technology use, including developers, suppliers and partners involved in program implementation.
- Relevant UN Member States (including relevant UN Member State governments, administrations and other public institutions).
- End-users (who may or may not include affected people or groups).

There are many ways in which an entity may engage with stakeholders, and what will be most effective will depend on the aim of the engagement and the context in which it takes place. However, options include 1-1 and small-group dialogues, larger consultations, stakeholder advisory groups, online forums, feedback, complaints and response mechanisms, surveys and worker voice technologies.

UN entities should consider establishing opportunities for ongoing and regular dialogue, alongside ad hoc engagement opportunities.

When engaging with stakeholders, an entity should be mindful of:

- Power imbalances and relevant cultural diversity or other dynamics.
- Barriers to participation and the accessibility of all to stakeholder engagement initiatives, including that stakeholders may not enjoy equal access to digital technologies and may have differing levels of digital literacy.

- The need to pay special attention to groups or individuals at heightened risk of vulnerability or marginalization, bringing an intersectional approach, and to be aware that different risks may be faced by individuals and groups on the basis of characteristics of their identity, including age, actual or perceived sexual orientation, gender identity, gender expression and sex characteristics.
- The importance of trust – and of not overestimating trust.
- The value of involving specialist expertise to support stakeholder engagement.
- The purpose of specific efforts to engage with diverse stakeholders across digital divides.
- The duty of care to prevent any possible retribution for stakeholders' engagement.

A. Embedding HRDD for digital technology use

Human rights risk management needs to be embedded within the entity to establish the foundations for effective HRDD for digital technology use.

Embedding should progress concurrently with the other components of effective HRDD and be informed by lessons learned from the entity's own experiences and those of peers. Over time, the entity will need to ensure effective oversight of its implementation of HRDD for digital technology use, enable coordination among teams involved in delivering HRDD for digital technology use, and build internal expertise and know-how.

The entity should consider what will be needed to establish a robust foundation for effective HRDD. For example, strong and visible support from senior leaders can establish 'tone from the top'. Further – and importantly – the entity should consider who will be involved in the development and implementation of HRDD for digital technology use, and seek to ensure representation from people from different backgrounds and functions, and with consideration of other characteristics of their identity (such as age, actual or perceived sexual orientation, gender identity, gender expression and sex characteristics).

When communicating with colleagues about HRDD, terms such as 'working conditions', 'cultural practices' and 'bias' may be easier to understand than the technical language of international human rights standards, particularly when communicating with colleagues with different areas of expertise. Case studies and scenarios can also help bring the entity's expectations and policies to life and ensure they resonate with all relevant colleagues.

PRACTICAL ACTIONS

GETTING STARTED	STRENGTHENING PRACTICES OVER TIME
• Map (and assess the application and effectiveness of) existing relevant policies, processes and practices (for example, those relating to procurement, data protection and privacy, data security, digital technologies, risk and impact assessment, etc.) to identify what is already in place, as well as any gaps. • Consult with the entity's senior leadership, relevant colleagues and external stakeholders on how the entity should approach HRDD for digital technology use. • Develop an initial plan or roadmap to implement HRDD for digital technology use. • Identify teams or functions that will need to be involved in implementation. • Assess internal expertise and the need for training or external support. • Allocate roles and responsibilities. • Consider how those involved will coordinate – a working group may be helpful.	• In line with the Secretary-General's Call to Action for Human Rights, senior leadership should nurture a rights-respecting culture – for example, by communicating internally and externally about the importance of addressing human rights impacts associated with the entity's digital technology use. • Raise awareness across the entity of why HRDD for digital technology use is important, how the entity can be connected to adverse impacts and its approach to HRDD for digital technology use. • Build deeper knowledge and capability among relevant colleagues and teams. • Ensure internal coherence across policies, processes, strategic priorities, budget allocation, recruitment and performance incentives. • Ensure effective oversight and accountability processes are in place.

B. Identifying and assessing

Processes to identify and assess actual and potential human rights impacts should support the entity to make and implement a plan to manage the adverse impacts that the entity is (or could be) connected to through its digital technology use.

These processes should enable the entity to identify any actual and potential adverse impacts that it may be connected to – i.e., that it may cause, contribute to or be linked to – across the full digital technology lifecycle and value chain. When identifying and assessing impacts, the entity should draw on appropriate internal and/or external expertise and consult meaningfully with potentially and actually affected groups and other relevant stakeholders (see Box 3).

Entities are encouraged to identify and leverage existing risk assessment tools and processes within their organization or across the UN system – it may be more efficient and effective to supplement or adapt existing processes than develop new ones. It may also be helpful to develop specific terms of reference or a Standard Operating Procedure to support the entity's efforts to identify and assess adverse human rights impacts that it may be connected to through its digital technology use.

When adapting existing processes or developing new ones, there are diverse tools and methodologies that entities can draw on. Human rights risk and impact assessments may contribute to efforts to identify and assess an entity's risk of connection with adverse impacts. However, UN entities are encouraged to think broadly about potential approaches – which

could include deep dives, salient human rights issues assessments and the ongoing implementation and monitoring of social audits and grievance processes – as well as potential information sources. Sources of information may include data from any relevant audit processes or grievance/complaint mechanisms the entity has in place, business and civil society reports, human rights benchmarks, country and sector human rights risk analyses, media articles and social media posts. Partner organisations, suppliers, government authorities, national and regional human rights institutions, donors, civil society organisations, affected groups and industry organisations may also be able to provide relevant information. UN entities should seek to rely on objective and reliable sources, including from within the UN System[19] and make a record of sources used, noting their limitations in terms of accuracy and objectivity.

Typically, it will not be possible to address all adverse human rights impacts simultaneously, and the entity will need to prioritize (see Box 4 on prioritization).

PRACTICAL ACTIONS [20]

GETTING STARTED

- Map key human rights risks associated with the entity's digital technology use, considering sources of potential risk such as:
- Digital technology use and related activities (including those commonly associated with human rights risks, such as data collection and sharing practices)
- Operational contexts (including weak governance, human rights record of host government, civic space, conflict and crisis situations)
- Partnerships, affiliations and other relationships (including track record and presence of effective HRDD systems)
- Presence of groups at heightened risk of vulnerability or marginalization
- Identify potentially affected groups and other relevant stakeholders and make a plan to consult meaningfully with them as appropriate.
- Assess and prioritize the entity's most severe human rights risks.
- Conduct deeper assessments to better understand the entity's highest priority human rights risks and how the entity may be connected (once the highest priority risks have been assessed in more depth, seek to undertake similar assessments on lower priority risks over time and as resources permit).

STRENGTHENING PRACTICES OVER TIME

- Building on initial steps and learnings, expand and strengthen processes to identify and assess actual and potential human rights impacts working towards a comprehensive and effective approach.
- Leverage existing systems and processes – for example, by integrating human rights considerations into new supplier or partner approval processes, or in contractual arrangements.
- Review and strengthen efforts to engage meaningfully with relevant stakeholders.
- Ensure initial high-level mapping and more in-depth identification and assessment processes are repeated periodically – and ideally prior to new activities, new technology development, procurement or use, major decisions and other changes affecting the entity or its operational contexts.
- Consider and address any gaps or blind spots in high-level mapping and deeper risk assessment processes.

[19] For example, UN Hub for Human Rights and Digital Technology.

[20] Additional resources to assist with these actions are included at the end of this document.

BOX 4 | PRIORITISATION

Entities should take a risk-based approach to prioritization and begin by addressing the most severe actual or potential human rights impacts associated with their digital technology use – recognizing that the challenges of scale may mean it is not possible to address all identified human rights impacts simultaneously.

Assess severity with reference to:

- Scale: gravity of the impact.
- Scope: number of individuals that are or will be affected.
- Remediability: the remediability of the impact.

Where an entity has identified a number of equally severe adverse human rights impacts, an assessment of their likelihood may also be used to inform prioritization.

It is important to consider how scale, scope and remediability may vary among individuals or groups at heightened risk of vulnerability or marginalization, bringing an intersectional approach – and to be aware that individuals and groups may face different risks on the basis of their age, actual or perceived sexual orientation, gender identity, gender expression and sex characteristics.

At a minimum and to the extent required by their mandates, UN entities should take action to prevent and address all grave violations or grave abuses, as defined in the current HRDD Policy, of international humanitarian law, international human rights law or standards, or international refugee law associated with their digital technology use.

C. Taking action

Entities should take action that seeks to prevent, mitigate and, where applicable, appropriately redress the actual and potential adverse impacts that they have identified (including, at a minimum, all grave violations or grave abuses – see Box 4). Entities should put in place systems and resources to ensure that this happens.

What constitutes an appropriate response will vary with how the entity is connected to an impact (see Part IIII) and the extent of its leverage – or influence – to encourage others also to take action to address the impact. Generally, if an entity is able to fully prevent or mitigate the impact itself because it is in a situation of "causation", it should do so. If an entity is not able to address the impact singlehandedly because third parties are involved, it should prevent or cease any contribution of its own, and then use its leverage to encourage the third parties to take effective action (see Box 5). If an entity does not have sufficient leverage to affect the actions of the third parties (and thus achieve positive outcomes for affected people and groups), it should take steps to try to increase it. Building leverage early in the establishment of a partnership or operational relationship can position an entity to act more effectively in the event of connection with adverse impacts.

Some human rights impacts may be straightforward to address. Others will be more complicated and may require collaboration with other parties, such as partner organisations, civil society organisations, government authorities and suppliers or other operational partners. Often, there will not be easy answers, and both effort and creativity will be needed to weigh competing considerations and achieve positive outcomes for affected people.

Importantly, being connected to an adverse impact does not necessarily mean that the conception, design, development, acquisition, use, further deployment, sharing or disposal of a digital technology must cease or cannot go ahead. Instead, it should shape how it happens – that is, with action to prevent, mitigate and/or address the impact. However, where there is no action that can be taken to address an adverse impact, the entity should consider not proceeding.

Sometimes, action taken in response to an adverse impact will not succeed – or will not yield immediate or fast results. Consider the human rights impacts of the entity's next steps in such situations. For example, staying in a relationship and working to build leverage and address impacts over time may achieve better outcomes for affected people than terminating the relationship. In such cases, an entity should be prepared to communicate with relevant stakeholders about the entity's approach. In other situations, it may be more appropriate for an entity to terminate the relationship.

PRACTICAL ACTIONS

GETTING STARTED	STRENGTHENING PRACTICES OVER TIME
• Assign roles and responsibilities for addressing specific risks and impacts. • Develop an action plan or proposed response – taking into consideration action any partners or other third parties involved in the impact may be pursuing (or planning to pursue). • Before implementing the plan or response, seek feedback and input from relevant internal and external stakeholders – including affected people or their legitimate representatives. • Initiate internal discussion about whether there are digital technologies that should not be used because the human rights risks are too severe and cannot effectively be prevented or otherwise mitigated – i.e., 'red lines'.	• Set clear expectations regarding human rights and the use of digital technologies when entering into new business or operational relationships – in addition to contractual and other similar measures, consider opportunities to set expectations with and gauge the human rights know-how of a proposed partner early in the relationship. • Identify other opportunities to build and strengthen leverage with partners (including business and operational relationships). • Put in place an effective data protection impact assessments and privacy by design and by default approach where relevant. • Explore opportunities to collaborate with partners or other third parties to achieve positive outcomes by working together. • Consider the circumstances in which the entity would seek to exit a relationship if human rights impacts cannot be satisfactorily addressed – and how a rights-respecting exit might be approached.

BOX 5 | BUILDING AND USING LEVERAGE

Where a UN entity contributes or is linked to an adverse human rights impact, it should build and use its leverage seeking to prevent, mitigate, cease and redress the impact.

What is leverage?

An entity has leverage where it has the ability to effect change in the wrongful practices of a third party that causes or contributes to an adverse impact.

It may reflect:

- The degree of direct control over the third party.
- The contractual terms between the entity and the third party.
- The proportion of business or spend the entity represents for the third party.
- The ability of the entity to incentivize the third party to improve its human rights performance (for example, through terms of future business, reputational advantage or capacity building assistance).
- The reputational benefits for the third party of working with the entity.
- The ability of the entity to incentivize other organisations to improve their human rights performance (for example, through multistakeholder initiatives).
- The ability of the entity to engage relevant government authorities to require improved human rights performance by the third party (for example, by implementing regulatory requirements, monitoring or sanctions).

How can an entity build and use leverage?

There are many ways to build and use leverage – and UN entities are encouraged to apply effort and creativity to doing so.

For example, an entity could:

- Assess the human rights performance and 'know-how' of a potential operational partner or supplier at the outset of a new relationship.
- Establish clear expectations regarding HRDD for digital technology use.
- Use contracting processes to set expectations, ensure access to information and establish leverage in the event that adverse human rights impacts are identified.
- Offer incentives, such as the prospect of a longer-term relationship, and – where needed – capacity building or other support.
- Partner with the third party to address the impact (an offer to work together may elicit a more open and cooperative response than a 'policing' approach).
- Collaborate with other actors, including peers, private sector actors, civil society organisations and/or government authorities – for example, to 'raise the bar' on expected performance at an industry level or to address root cause issues.

D. Tracking

An entity should take steps to track both the implementation and effectiveness of its HRDD for digital technology use (including in relation to outcomes for affected people and groups).

Over time, tracking is likely to involve a range of processes and activities which will vary across diverse country contexts, including setting goals, targets and indicators, collecting and analyzing information, ensuring effective internal reporting processes and evaluating specific interventions to address human rights impacts with which an entity is connected through its digital technology use. Tracking should be based on appropriate qualitative and quantitative indicators and draw on feedback from both internal and external stakeholders, as well as feedback, complaints and response mechanisms.

UN entities should ensure that lessons learned are applied to support the continuous improvement of their HRDD for digital technology use.

PRACTICAL ACTIONS

GETTING STARTED	STRENGTHENING PRACTICES OVER TIME
• Consider potential approaches to tracking – ideally, early in the development of the entity's approach to HRDD for digital technology use. • Set measurable goals or targets for implementing HRDD for digital technology use and define key performance indicators (KPIs). • Track the progress and effectiveness of the entity's own implementation of HRDD for digital technology use, and identify any lessons learned. • Engage partners (including technology providers) to track whether they are meeting the entity's expectations regarding HRDD for digital technology use. • Seek and respond to input and feedback from experts and affected people (or their legitimate representatives).	• Review the effectiveness of internal reporting channels and opportunities to strengthen these. • Explore opportunities to integrate consideration of tracking processes early in the design of interventions to address adverse impacts. • Conduct an in-depth, bespoke evaluation of specific projects or interventions. • Ensure effective feedback loops are in place to enable the entity to integrate lessons learned from tracking.

E. Communicating

An entity should communicate clearly internally and externally about how it addresses adverse impacts that it is connected to through its digital technology use to provide transparency to relevant stakeholders.

Good and timely communication can also build trust and strengthen relationships with partners, affected people and communities, and other

stakeholders. It helps stakeholders understand the entity's approach – including any challenges it has confronted in its HRDD for digital technology use and how it has responded or is responding to them.

Communication can take a number of forms and does not necessarily require formal reporting – although an entity may choose to do this. An entity's approach should reflect relevant adverse impacts, be accessible to its intended audience and provide information that enables stakeholders to evaluate the adequacy of the entity's approach (including responses to actual or potential impacts), including as regards outcomes for affected people and groups.

PRACTICAL ACTIONS

GETTING STARTED	STRENGTHENING PRACTICES OVER TIME
• Map existing relevant internal and external stakeholders and their communications channels. • Consider what information different stakeholders may require, when and why. • In the event that the entity has caused or contributed to severe adverse impacts, communicate relevant information to affected people in a timely, accessible for all, context-appropriate and culturally sensitive way while maintaining privacy rights and data safeguards	• Engage with colleagues in relevant teams (including communications and legal) on the importance of communicating about HRDD. • Seek feedback from external stakeholders on the adequacy and effectiveness of the entity's approach to communicating about HRDD for digital technology use. • Consider developing a standalone publication focused on the entity's HRDD for digital technology use. • Consider independent verification of the entity's human rights reporting.

Annex A | Frequently asked questions

1. How does this Guidance intersect with other toolkits, assessments, and human rights and ethical principles for Artificial Intelligence, already developed by UN entities?

This guidance should reinforce, rather than replace, existing internal processes and entity-specific guidance and procedures regarding digital technologies. There is much good work being done on HRDD and ethical approaches across the UN system.

The guidance is intended to provide broad direction, going beyond the use of Artificial Intelligence, to all UN digital technology design, development, and use, as well as during procurement of digital technologies and in developing partnerships with tech companies.

It aligns with and builds on the parameters endorsed in June 2023 by the Secretary-General's Executive Committee regarding the development of a United Nations HRDD Framework Policy that establishes broad HRDD principles and implementation modalities for all UN programs and operations. The Framework Policy and this Guidance are designed to establish common approaches and policy coherence across the UN in our approaches to the use of digital technology.

Grounding the UN approach to digital technology on the human rights framework gives us the common ground and clarity of the UN Charter and international human rights law, where there is broad agreement from Member States on definitions and legally binding obligations which apply across borders. In using this foundation for our internal-facing policies and guidance, it provides the UN with the opportunity to provide an example to Member States in how to approach their own use and regulation of digital technology.

2. Are there reputational risks associated with implementing HRDD, or not doing so?

UN entities are increasingly subject to scrutiny on their human rights impacts – including from business, development partners and civil society partners.

Effective HRDD enables your entity to know what its adverse impacts are, and to be able to communicate about how it is addressing them. Entities that implement HRDD for digital technology use in an active and committed manner should be better placed to manage reputational risks associated with connection to adverse human rights impacts.

3. What's the difference between HRDD, human rights impact assessments and human rights risk and opportunity assessments?

A human rights impact assessment is a standalone assessment of the human rights impacts associated with a project, operation or other activity. A human rights risk and opportunity assessment also considers opportunities to advance human rights through a project, operation or other activity. Both of these types of assessments can contribute to HRDD efforts to identify and assess human rights risks and impacts.

HRDD itself is a broader, iterative risk management approach, which encompasses efforts to:

- Embed human rights risk management.
- Identify and assess actual and potential adverse impacts.
- Take action to cease, prevent or mitigate impacts.
- Track implementation and effectiveness.
- Communicate how it addresses impacts.

4. Our entity's digital technology use is expansive – do we need to do HRDD for every laptop or mobile device purchase?

HRDD for digital technology use should be principled but also pragmatic – and commensurate with the size, sector, operational

context and structure of the entity, as well as the severity of the adverse human rights impacts associated with its digital technology use. It should enable the entity to identify and address human rights risks and impacts associated with its digital technology use.

That does not mean that HRDD needs to be conducted for every laptop or mobile device purchase. Instead, the entity should take a higher-level look at its activities, partnerships, operational relationships (including supply chain) to identify human rights risks and impacts, then prioritize these and take action to address adverse impacts and achieve meaningful positive outcomes for affected people.

5. Our entity provides life-saving humanitarian protection and assistance in emergency and crisis situations – often in high-risk contexts. How can we do HRDD for digital technology use without delaying our response?

The entity will need to consider carefully how it approaches HRDD for digital technology use in such situations – recognizing both the human rights risks of delays to the entity's response, as well as the risks its digital technology use might pose, particularly in high-risks contexts. HRDD for digital technology use should always be implemented in a rights-respecting way that seeks to ensure that the HRDD process itself does not result in adverse human rights impacts.

For example, where the entity has identified a new technology that has potential application in emergency response situations – and before such a situation arises – it could seek to identify and understand any potential human rights risks the use of the new technology may pose, consider whether there are particular types of crisis situation or context in which these risks are more likely to materialize, and identify potential mitigation options. Once this more general initial assessment has been conducted, it should enable the entity to more rapidly consider whether the use of the technology in a specific situation may give rise to human rights impacts and, if so, how to proceed and what mitigation measures may need to be put in place.

There may be situations in which the use of a digital technology may result in human rights impacts while also saving lives or achieving other positive human rights outcomes. In these situations, the entity may consider carefully how to weigh the potential human rights risks and benefits of using the technology, and be prepared to communicate with stakeholders about its approach.

Where a prior risk assessment is not possible and the entity deems the potential benefits of using the technology to outweigh the expected potential risks, it should aim to conduct a human rights impact assessment as soon as possible afterwards and be prepared to communicate with stakeholders about its approach – including any adverse impacts that resulted.

6. Some of our entity's activities are dependent on a technology that helps those who need our support to access it – but the entity's use of this technology may itself give rise to adverse human rights impacts. What can we do?

Sometimes, an entity will be faced with difficult or imperfect choices. If alternative technology that supports access to the entity's services is, or becomes, available and it is practicable to implement it, the entity should consider doing so.

If it is not, the entity should consider (in consultation with affected people and other relevant stakeholders) both the human rights risks posed by the technology and the adverse impacts that may result if the entity ceased using the technology. If the entity decides to keep using the technology, it should put in place measures to prevent and mitigate the human rights risks associated with the technology's use, and monitor the situation to assess the effectiveness of those measures. It should also ensure that a feedback, complaints and response mechanism is accessible to those who may be adversely impacted.

7. If there's no 'one right way' to implement HRDD for digital technology use, does that mean there's no minimum standard? How do we know we're doing it right?

There is no 'one right way' to implement HRDD for digital technology use, but it needs to be effective and reflect agreed-to minimum standards. At a minimum and to the extent required by their mandates, UN entities should take action to prevent and address all grave violations or grave abuses, as defined in the current HRDD Policy, of international humanitarian law, international human rights law or standards, or international refugee law associated with their digital technology use.

Effective HRDD should enable the entity to know what its human rights impacts are and to show how it is addressing them. HRDD should also be based on meaningful engagement with affected people and groups.

To assess whether it is on the right track, the entity should seek feedback from relevant stakeholders (including affected people or their legitimate representatives). This guidance and relevant international standards can be used as a basis for those discussions. Communicate about the entity's approach and ask what is working well – and where it could improve. Stakeholders can also provide valuable feedback on the entity's prioritization and may help identify any gaps or blind spots in its approach.

8. Why is HRDD typically implemented using multiple policies and processes? Wouldn't it be simpler to implement a single HRDD policy and process?

Some entities may find that it is practicable – and indeed simpler – to implement HRDD for digital technology use via a single policy and process that encompass HRDD for digital technology use across all of the entity's activities and relationships. However, most entities – including, in particular, larger UN entities – are likely to find that multiple policies and processes are needed.

For example, while an entity might develop a standalone HRDD for digital technology use policy, it may also be necessary to revise existing policies – for example, supplier codes of conduct or data protection policies. Similarly, different HRDD processes and activities may be needed to effectively address the different human rights impacts that the entity has identified. A process that works to address risks in the supply chain might not be fit-for-purpose when applied to risks associated with the end use of technologies. Many entities also find that there are opportunities to leverage or adapt existing processes and systems to implement HRDD for digital technology use more efficiently.

When developing entity-level HRDD policies and processes, it is important to recognize the risks of having disparate policies and processes across the UN system, which may lead to policy incoherence, an extremely uneven HRDD implementation landscape, and perceptions of bias vis-à-vis Member States or companies. These risks underscore the importance of the Secretary-General's June 2023 decision to develop a HRDD Framework Policy by August 2024 that would set out the main parameters and minimum standards that all UN entities must meet.

9. There are lots of HRDD resources and tools for business – can UN entities use these?

Yes, UN entities may find many of the tools and resources developed for business helpful.

While there are differences between business enterprises and UN entities, many of the challenges associated with implementing HRDD are common across large, complex organisations. As there are currently few existing resources developed specifically for international institutions implementing HRDD, there may be much value in exploring materials developed for business and the insights they provide - although the UN does not necessarily endorse external content. See Annex B for a list of further resources.

Annex B | Resources

This guidance has been developed to support UN entities to implement HRDD for digital technology use and to strengthen practice over time.

The Executive Office of the Secretary General and the Office of the High Commissioner for Human Rights recognise that there will likely be need for additional guidance and other resources – for example, addressing key areas of work in more depth – as well as concrete tools and a system-wide, centralized support mechanism. In the meantime, there are a number of existing resources that entities may find helpful to refer to.

UN entities should note that the UN does not endorse external content – these resources are provided for information purposes only.

i) Relevant international instruments and standards

- International Bill of Human Rights (United Nations)
- Additional international human rights instruments (United Nations)
- General comment no. 25 (2021) on children's rights in relation to the digital environment (United Nations)
- Declaration on Fundamental Principles and Rights at Work (ILO 1998 as revised in 2022)
- Guiding Principles on Business and Human Rights (United Nations, 2011)
- OECD Guidelines for Multinational Enterprises on Responsible Business Conduct (OECD, 2023)
- Tripartite Declaration of Principles concerning Multinational Enterprises and Social Policy (ILO, 2022)
- Recommendation on the Ethics of Artificial Intelligence (UNESCO, 2021)

ii) Policies, mechanisms and resources produced by the UN

- Human rights due diligence policy on United Nations support to non-United Nations security forces
- High-level Panel on Digital Cooperation
- Office of the Secretary-General's Envoy on Technology (United Nations)
- Human Rights and Digital Technology: Resource Hub (United Nations)
- Guidelines for the governance of digital platforms: safeguarding freedom of expression and access to information through a multi-stakeholder approach (UNESCO, 2023)
- Principles for the Ethical Use of AI in the UN System (United Nations, 2022)
- B-Tech Project (UN Human Rights)
    - The UN Guiding Principles in the Age of Technology
    - Identifying and Assessing Human Rights Risks related to End-Use
    - Taking Action to Address Human Rights Risks Related to End-Use
- Addressing Forced Labor and Human Trafficking in UN Supply Chains: Guidance for UN Staff (HLCM-PN Taskforce for the Development of a Joint Approach to Combatting Human Trafficking and Forced Labor in Supply Chains, 2022)
- Business and Human Rights in Challenging Contexts: Considerations for Remaining and Exiting (OHCHR, 2023)
- Guidance Note on Data Impact Assessments (OCHA, 2020)
- Guidance on the Safe and Ethical Use of Technology to Address Gender-based Violence and Harmful Practices (UNFPA, 2023)

- IASC Operational Guidance on Data Responsibility and Humanitarian Action (United Nations, 2023)
- Innovation and technological change, and education in the digital age for achieving gender equality and the empowerment of all women and girls: Report of the Secretary-General (United Nations, 2022)
- Policy Guidance on AI for Children (UNICEF, 2021)
- UN Principles on Personal Data Protection and Privacy (United Nations, 2018)

iii) Resources produced by non-UN organisations.

General guidance on implementing human rights due diligence

- OECD Due Diligence Guidance for Responsible Business Conduct (OECD, 2018)
- Doing Business with Respect for Human Rights: A Guidance Tool for Companies (Shift, Global Compact Netherlands and Oxfam, 2016)
- UN Guiding Principles Reporting Framework (Shift and Mazars)
- Business Practice Portal (Global Business Initiative on Human Rights)
- Valuing Respect (Shift)

Guidance and other resources on human rights and digital technology use

AI Blind Spots (MIT)
- Gender x Innovation Guide (Action Coalition on Technology and Innovation for Gender Equality)
- Guidance on Human Rights Impact Assessment of Digital Activities (DIHR, 2020)
- Principles for Digital Development
- OECD resources on responsible business conduct and digitalization (OECD)
- Technology & Human Rights (Business and Human Rights Resource Centre)
    - Digital Freedom
    - Automation
    - Artificial Intelligence
- Technology and Rights (Human Rights Watch)
- Technology and Human Rights (Danish Institute for Human Rights)
- Technology (Institute for Human Rights and Business)

Potential source material to support human rights risk assessments

- Information about human rights-related risks:
    - Country reports (Amnesty International)
    - Country reports on human rights practices (US State Department)
    - Explore the Map (Freedom House)
    - Global Slavery Index (Walk Free)
    - Technology Company Dashboards (Business and Human Rights Resource Centre)
    - World reports (Human Rights Watch)
- Benchmarks:
    - Big Tech Scorecard (Ranking Digital Rights)
    - Corporate Human Rights Benchmark (World Benchmarking Alliance)
    - Digital Inclusion Benchmark (World Benchmarking Alliance)
    - Know the Chain Benchmark (Know the Chain)
    - Tech and Telecom Benchmark (Global Child Forum)
    - Telco Giants Scorecard (Ranking Digital Rights)