

# UN Secretary-General's Guidance on Human Rights Due Diligence for Digital Technology Use

*Draft 4 - revised June 2023*

## Contents

I. About this guidance	
A. Why has this guidance been developed?	
B. Who is this guidance for?	
C. Why should UN entities implement HRDD for digital technology use?	
II. Using this guidance	
A. How to use this guidance	
B. HRDD for digital technology use: Checklist	
III. About HRDD and digital technology use	
A. What human rights risks are associated with digital technology use?	
B. How can UN entities be involved in these adverse human rights impacts?	
C. What is HRDD for digital technology use?	
IV. Practical approaches to implementing HRDD for digital technology use	
A. Embedding HRDD for digital technology use	
B. Identifying and assessing	
C. Taking action	
D. Tracking	
E. Communicating	
V. Additional support	
A. Frequently asked questions	
B. Resources	

# I. About this guidance

## A. Why has this guidance been developed?

The 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. 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 recognises that a UN entity could potentially be involved in adverse human rights impacts that occur at any point of this lifecycle and value chain, and supports entities to adopt a risk-based approach to prioritisation that focuses energy and resources on addressing the most severe human rights risks and impacts associated with their digital technology use.

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*<sup>1</sup> and *Our Common Agenda*,<sup>2</sup> which call for the application of human rights frameworks to the digital space and basing all UN engagement on human rights risks assessments. It was developed in response to the *Roadmap for Digital Cooperation*,<sup>3</sup> 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.

HRDD is widely recognised as key to credible and effective management of human rights risks to people, as well as management of reputational and operational risks to the UN. It has been embedded in international standards, and it is increasingly reflected in national and supra-national policy and regulatory requirements. There is significant momentum behind the introduction of mandatory human rights and environmental due diligence requirements and mandatory human rights reporting requirements, in particular. There is also growing focus on opportunities to strengthen value chain approaches that encompass downstream as well as upstream human rights risks, as well as the intersections between human rights, the environment and climate change. HRDD was initially developed to support private sector entities to address adverse human rights impacts with which they are involved – and the scale and sophistication of business implementation of HRDD and efforts to address human rights impacts are growing. HRDD is also increasingly implemented by other types of organisations. Indeed, HRDD processes and expectations are already in place within the UN system –

---

<sup>1</sup> United Nations, *The Highest Aspiration: A Call to Action for Human Rights* (2020).

<sup>2</sup> United Nations, *Our Common Agenda: Report of the Secretary-General* (2021).

<sup>3</sup> United Nations, *Road Map for Digital Cooperation: Implementation of the recommendations of the High-level Panel on Digital Cooperation* (2020) at 18, [86].

variously at system-wide and entity levels – and a process is underway to develop a framework United Nations Policy on Human Rights Due Diligence (framework HRDD Policy). HRDD offers a principled and practical approach to identifying and addressing adverse human rights impacts and, in turn, realizing the rights of affected people and groups, thereby promoting the UN’s purposes and principles.

This guidance is not intended to inhibit or limit the use of digital technologies across the UN, many of which are critical to the UN’s operations and other activities. However, it recognises that proactive and effective measures to identify and address adverse human rights impacts connected with 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. This guidance has been developed in coordination and alignment with the process to develop the Framework HRDD Policy.

## **B. Who is this guidance for?**

The guidance has been developed for all UN entities.

It should be applied, in particular, by work units responsible for risk management and digital technology use – as well as those involved in implementing and strengthening HRDD for digital technology use. 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, and digital technology use.

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. 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 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 DMSPC.

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

UN entities should implement HRDD to manage potential or actual adverse human rights impacts that they are involved in through their digital technology use and, in doing so, to help achieve positive human rights outcomes for 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.<sup>4</sup> 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, hazardous working conditions, child labour and discrimination) and by using digital technology in a rights-respecting way to enable and facilitate sustainable development.

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.

The Secretary-General’s 2020 *Call to Action on Human Rights* emphasises that ‘human rights are the responsibility of each and every United Nations actor and that a culture of human rights must permeate everything we do’. The *Call to Action* promotes both ‘a human rights vision that is transformative’ and the ‘application of the human rights frameworks to the digital space’.<sup>5</sup> Follow-up to *Our Common Agenda* includes consideration of the application of human rights frameworks and standards in the digital space. The *Roadmap for Digital Cooperation* recognises that digital technologies ‘provide new means to advocate, defend and exercise human rights, but they can also be used to suppress, limit and violate human rights’.<sup>6</sup>

The *Roadmap for Digital Cooperation* states that HRDD has a critical role to play to enable the human rights risks associated with digital technologies to be managed effectively.<sup>7</sup>

The Office of the High Commissioner for Human Rights recognises that the priorities of UN entities must be to fulfil their individual mandates, including promoting enjoyment of all internationally-recognised human rights, responding to emergencies on an urgent basis, meeting the immediate needs of people they serve 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.

Each UN entity should endeavour 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. The establishment of a centralised, UN support team for HRDD has been proposed during the review process of the expansion of the framework HRDD

---

<sup>4</sup> United Nations, Charter of the United Nations (1945).

<sup>5</sup> United Nations, *The Highest Aspiration: A Call to Action for Human Rights* (2020).

<sup>6</sup> United Nations, *Report of the Secretary-General: Roadmap for Digital Cooperation* (2020).

<sup>7</sup> Ibid.

Policy. Such an implementation support team, working under the guidance of the HRDDP Review Group, could support roll-out and implementation, with additional support structures established in the field as appropriate.

## II. Using this guidance

### A. How to use this guidance

The implementation of HRDD should be an iterative process.

Why? Because addressing human rights impacts associated with digital technology use can be complicated, and the human rights risk landscape of any entity will evolve over time (for example, due to changes in its activities, operating environments, relationships, or the digital technologies that it uses). Effective HRDD 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 strengthen HRDD for digital technology use over time.

Teams involved in implementing HRDD for digital technology use should consider the guidance and then recommend the appropriate next steps for their entity. If the entity is new to HRDD, those steps should 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 the entity is already familiar with human rights impacts connected with its digital technology use, a pilot project may help generate some initial insights and learnings to inform the implementation of more comprehensive HRDD.

Implementation should build on and integrate with existing processes, including the UNSDG Common Approach to Due Diligence in Business Sector Partnerships, the High Level Committee on Management Statement and Guidance to combat trafficking and forced labour in United Nations supply chains, the United Nations Model Environmental and Social Standards, the United Nations Protocol on Allegations of Sexual Exploitation and Abuse against Implementation Partners and the United Nations Partnership Portal, among others. For UN entities with established and relevant HRDD processes in place, the guidance can assist in reviewing those processes and identifying opportunities to

ensure human rights impacts associated with digital technology use are 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 it implements effective HRDD processes based on common standards applied consistently across the UN system, a crucial element for UN policy consistency.

## B. HRDD for digital technology use: Checklist

HRDD for digital technology use should enable an entity to know and show how it is addressing adverse human rights impacts associated with its digital technology use.

HRDD for digital technology use should always:

- ✓ Seek positive human rights outcomes for affected people
- ✓ Be informed by engagement with stakeholders, including affected people
- ✓ Be ongoing and dynamic
- ✓ Be risk-based and context-sensitive
- ✓ Be appropriate to an entity's circumstances

### HRDD FOR DIGITAL TECHNOLOGY USE: KEY STEPS

Meaningful engagement with affected people and other stakeholders

#### A. Embed

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 other components of HRDD.

#### 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 manage the adverse impacts that the entity is (or may be) involved in 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 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 involved and the extent of its leverage to encourage others also to act.

#### D. Track

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

#### E. Communicate

An entity should communicate internally and externally about how it addresses adverse human rights impacts that it identified that it is involved in through its digital technology use. Communication does not necessarily require formal reporting – although an entity may choose to do this.

### III. About HRDD for digital technology use

#### A. What is HRDD for digital technology use?

HRDD 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 are 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 that it is involved in through its use of digital technologies.

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 it is vital for policy consistency that UN entities apply the same standards in implementing HRDD, 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 involvement in severe human rights impacts and the nature and context of its operations.

However, at a minimum, HRDD should always:

- Seek positive human rights outcomes for affected people
- Be informed by engagement 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.

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 ‘fix’ a human rights harm. 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 address an impact, and they are likely to need to work together.



By implementing effective HRDD, a UN entity can help ensure that it is appropriately addressing human rights risks associated with its digital technology use.

## **B. What human rights risks are associated with digital technology use?**

HRDD for digital technology use should encompass **all internationally recognised human rights**, including the fundamental freedoms set out in the International Labour Organisation's (ILO) Declaration on Fundamental Principles and Rights at Work.

As described below, however, and given that the challenges of scale may mean it is not possible to address all identified human rights impacts simultaneously, entities should take a risk-based approach to **prioritisation** and begin by addressing the most severe actual or potential human rights impacts associated with their digital technology use.

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

Why? Because a UN entity can be involved in impacts on virtually 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 AI algorithms reflects systemic discrimination – such, on the basis of race 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 involved in adverse impacts on the right to just and favourable working conditions, modern slavery and the right to adequate housing.

Some situations will be less straightforward – particularly where the use of digital technology may result in both positive and adverse human rights impacts. For example, social media platforms may be leveraged to provide information to displaced or persecuted people on opportunities to access support (supporting realisation of the right to life, liberty and security) but may also result in data collected being collected in breach of the right to privacy or being shared with third parties who use it to target at-risk groups (in turn adversely impacting rights such as the right to life, liberty and security).

Entities should note that their digital technology use may affect children, women, non-binary people and men differently, and that it may amplify risks to people and groups already at heightened risk of vulnerability and marginalisation – including those affected by armed conflict and other types of violence.

**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 be impacted at different stages of the digital technology lifecycle (and value chain).

<b>Digital technology lifecycle</b>	<b>Examples of human rights impacts</b>
Conception	<ul style="list-style-type: none"><li>• Discrimination</li><li>• Privacy</li></ul>
Design and development	<ul style="list-style-type: none"><li>• Bias and discrimination</li><li>• Privacy</li><li>• Life, liberty and personal security</li></ul>
Acquisition (including materials, manufacture, transport and logistics)	<ul style="list-style-type: none"><li>• Children’s rights</li><li>• Hazardous working conditions</li><li>• Modern slavery, forced labour and trafficking</li><li>• Health and safety</li><li>• Livelihoods and housing</li><li>• Environmental impacts</li><li>• Freedom of association</li></ul>
Use, further deployment and sharing	<ul style="list-style-type: none"><li>• Privacy</li><li>• Bias and discrimination</li><li>• Life, liberty and personal security</li><li>• Right to seek and enjoy asylum</li><li>• Clean, healthy and sustainable environment</li></ul>
Disposal (including recycling)	<ul style="list-style-type: none"><li>• Hazardous working conditions</li><li>• Privacy</li><li>• Health and safety</li><li>• Clean, healthy and sustainable environment.</li></ul>

### C. How can UN entities be involved in these adverse impacts?

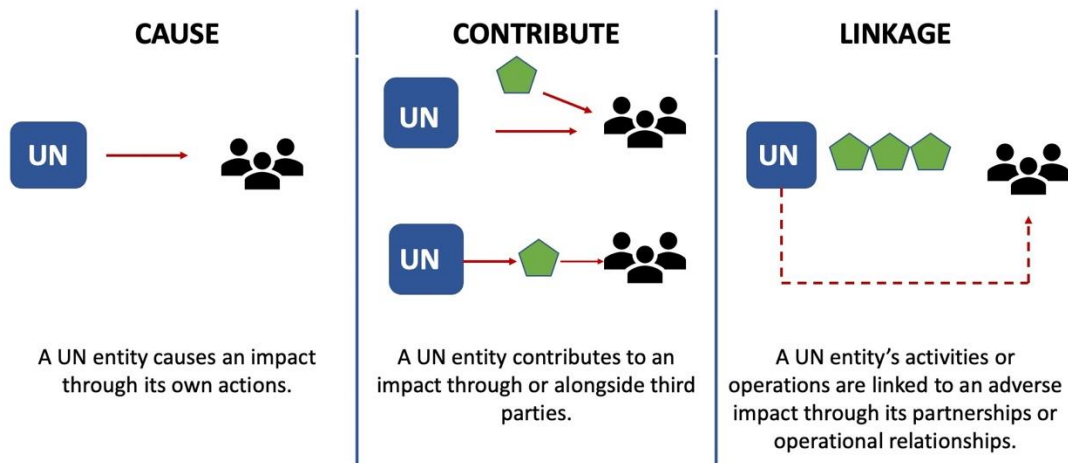
There are three ways in which a UN entity can be involved in an adverse human rights impact through its digital technology use: causation, contribution and linkage. These can be understood as a continuum of involvement.

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 involved in a potential or adverse impact will guide how it should respond.

Importantly, each party involved in 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.

Involvement in adverse human rights impacts is dynamic – **an entity's involvement may shift along the continuum** as a result of its actions and those of other third parties involved in an impact. For example, an entity that takes effective steps to address its contribution may shift to the 'linkage' category. By contrast, an entity that is linked to an impact and takes no action may find its involvement shifts to contribution over time.

**FIGURE 1 | CONTINUUM OF INVOLVEMENT**



## BOX 2 | EXAMPLES OF INVOLVEMENT IN 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 without adequate data protection safeguards, it may cause an adverse impact on the right to privacy.

*Expected action:* The entity should cease or prevent the impact – for example, by putting in place adequate data protection safeguards.

**2. Contribution** | A UN entity contributed 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, it has contributed to an adverse impact (in this scenario, the police service, or support recipient, caused the impact).

*Expected action:* The entity should cease or prevent its contribution and use leverage to mitigate any remaining impacts to the greatest extent possible. That is, it should stop providing the technology to the police service, and identify 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.

**3. Linkage** | A UN entity has not caused or contributed 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 labour, 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 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 labour<sup>8</sup>, engaging with entities in its supply chain to build awareness and know-how to address forced or bonded labour, and by participating in collaborative initiatives to address root cause challenges associated with forced and bonded labour. If the entity is not able to build sufficient leverage, it should consider terminating the relationship, and assess the potential human rights impacts of doing so. See Box 5 for more on building and using leverage.

**4. Not involved** | A UN entity is not involved in 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 support with the communities it serves. 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 entity.

*Expected action:* No action is expected. However, the UN entity may choose to use its leverage to encourage the technology company (and potentially other parties involved) to address the impact, or to partner with a different technology company. Reasons for acting may include managing reputational risks to the UN entity.

See Box 5 for more information on using leverage.

---

<sup>8</sup> Addressing Forced Labour and Human Trafficking in UN Supply Chains: Guidance for UN Staff (<https://unsceb.org/sites/default/files/2023-02/Guidance%20for%20UN%20Staff%20on%20HTFL%20in%20UN%20Supply%20Chains.pdf>)

## IV. Practical approaches to implementing HRDD for digital technology use

### **BOX 3 | ENGAGING WITH STAKEHOLDERS**

Meaningful engagement with stakeholders should inform every stage of an entity's HRDD for digital technology use. It should enable the entity to hear, understand and respond to stakeholders' interests and concerns, including through collaborative approaches.

Relevant stakeholders are likely to include:

- Potentially 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).
- People or actors with relevant human rights and/or digital technology expertise.

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 (for example, using the world food café methodology<sup>9</sup> or via a session at an event), stakeholder advisory groups, online forums, grievance or complaints channels, surveys and worker voice technologies.

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

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

- Power imbalances and relevant cultural or other dynamics.
- The need to pay special attention to groups or individuals at heightened risk of vulnerability or marginalisation, and to be aware that different risks may be faced by women, children, non-binary people and men.
- 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 stakeholders.

### **A. Embedding HRDD for digital technology use**

---

<sup>9</sup> <https://www.theworldcafe.com/wp-content/uploads/2015/07/Cafe-To-Go-Revised.pdf>

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. 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’.

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 colleagues.

## **PRACTICAL ACTIONS**

### **GETTING STARTED**

- > Map existing relevant policies, processes and practices to identify what is already in place, as well as any gaps.
- > Consult with senior leaders, 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.

### **STRENGTHENING PRACTICES OVER TIME**

- > In line with the Secretary-General’s Call to Action for Human Rights, senior leaders 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 involved in 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 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 may be) involved in through its digital technology use.

These processes should enable the entity to **identify any actual and potential impacts that it may be involved in** – 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 affected groups and other relevant stakeholders (see Box 3).

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 involvement in adverse impacts. However UN entities are encouraged to think broadly about potential approaches and 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, NHRIs, 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<sup>10</sup>.

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

### PRACTICAL ACTIONS<sup>11</sup>

GETTING STARTED

<sup>10</sup> UN Hub for Human Rights and Digital Technology.

<https://www.digitalhub.ohchr.org/#:~:text=Welcome%20to%20the%20United%20Nations,apply%20in%20the%20digital%20space.>

<sup>11</sup> Additional resources to assist with these actions are included at the end of this document.



- > 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)
  - Operational contexts (including weak governance, conflict and crisis situations)
  - Partnerships and other relationships (including track record and presence of effective HRDD systems)
  - Presence of groups at heightened risk of vulnerability or marginalisation
- > Identify potentially affected groups and other relevant stakeholders, and make a plan to consult meaningfully with them as appropriate.
- > Assess and prioritise 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 involved (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 to ensure a comprehensive and effective approach.
- > Leverage existing systems and processes – for example, by integrating human rights considerations into new supplier or partner approval processes.
- > 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.

#### **BOX 4 | PRIORITISATION**

Entities should take a risk-based approach to prioritisation and begin by addressing the most severe actual or potential human rights impacts associated with their digital technology use – recognising 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: impact of delayed response on 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 prioritisation.

It is important to consider how scale, scope and remediability may vary among individuals or groups at heightened risk of vulnerability or marginalisation – and to be aware that different groups, such as women, children non-binary people and men, may face different risks.

At a minimum, as 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, human rights law or standards, or refugee law associated with their digital technology use.

### C. Taking action

Entities should **take action that seeks to prevent, mitigate and 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 involved** in an impact (see Part III(C)) 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, 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 involvement in an 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 agencies 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 involved in 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 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**

- > Assign roles and responsibilities for addressing specific risks and impacts.
- > Develop an action plan or proposed response – taking into consideration action any 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 great – i.e. ‘red lines’.

### **STRENGTHENING PRACTICES OVER TIME**

- > 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 a data protection/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 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 harm.

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 incentivise 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 incentivise 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 entity (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 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.

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 analysing information, ensuring effective internal reporting processes and evaluating specific interventions to address human rights impacts in which an entity is involved 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.

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

- > 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 input and feedback from experts and affected people (or their legitimate representatives).

### STRENGTHENING PRACTICES OVER TIME

- > 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 internally and externally about how it addresses adverse impacts** that it identifies that it is involved in through its digital technology use to provide transparency to relevant stakeholders.

Good 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 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). It is crucial to ensure communication does not pose additional risks to affected people, UN personnel or the legitimate requirements of commercial confidentiality.

## PRACTICAL ACTIONS

### GETTING STARTED

- > Map existing relevant internal and external communications channels.
- > Consider what information different stakeholders may require.
- > In the event that the entity has caused or contributed to severe adverse impacts, communicate relevant information with affected people in a timely, accessible and culturally sensitive way.

### STRENGTHENING PRACTICES OVER TIME

- > Engage with colleagues in relevant teams (including communications and legal) on the importance of communicating about HRDD.
- > Seek feedback from external stakeholders on 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 human rights reporting.

## V. Additional information

### A. Frequently asked questions

#### **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 and civil society partners.

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

#### **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 broader, encompassing 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

#### **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 prioritise these and take action to address adverse impacts and achieve meaningful outcomes for affected people.

**Our entity provides life-saving humanitarian support in 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 – recognising both the human rights risks of any 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 result, 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, whether 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 should 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 unknown risks, it should 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.

**Some of our entity’s activities are dependent on a technology that helps those who need our support 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 grievance process is accessible to those who may be adversely impacted.

**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, as 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, human rights law or standards, or refugee law associated with their digital technology use.<sup>12</sup>

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 prioritisation and may help identify any gaps or blind spots in its approach.

**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

---

<sup>12</sup> As per the 1 June 2023 Executive Committee decision.

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 'Framework HRDD policy' by August 2024 that would set out the main parameters and minimum standards that all UN entities must meet.

### **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 (although the UN does not necessarily endorse external content).

## **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, centralised support mechanism. In the meantime, there are a number of existing resources that entities may find it helpful to refer to (although the UN does not necessarily endorse external content).

### **i) Relevant international instruments and standards**

- > [International Bill of Human Rights](#) (United Nations)
- > [Additional international human rights instruments](#) (United Nations)

- > [Guiding Principles on Business and Human Rights](#) (United Nations, 2011)
- > [OECD Guidelines for Multinational Enterprises on Responsible Business Conduct](#) (OECD 2023)

**ii) 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)
- > [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)

**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)
- > [OECD Guidelines for Multinational Enterprises on Responsible Business Conduct | READ online \(oecd-ilibrary.org\)](#) (OECD, 2023)
- > [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)
- > [Valuing Respect](#) (Shift)
- > [Business Practice Portal](#) (Global Business Initiative on Human Rights)

Guidance and other resources on human rights and digital technology use

- > [OECD resources on responsible business conduct and digitalisation](#) (OECD)
- > [Guidance on Human Rights Impact Assessment of Digital Activities](#) (DIHR, 2020)
- > [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
  - [Technology Company Dashboards](#) (Business and Human Rights Resource Centre)
  - [Country reports](#) (Amnesty International)
  - [World reports](#) (Human Rights Watch)
  - [Country reports on human rights practices](#) (US State Department)
  - [Explore the Map](#) (Freedom House)
  - [Global Slavery Index](#) (Walk Free)
- > Benchmarks:
  - [Corporate Human Rights Benchmark](#) (World Benchmarking Alliance)
  - [Digital Inclusion Benchmark](#) (World Benchmarking Alliance)
  - [Know the Chain Benchmark](#) (Know the Chain)
  - [Big Tech Scorecard](#) (Ranking Digital Rights)
  - [Telco Giants Scorecard](#) (Ranking Digital Rights)
  - [Tech and Telecom Benchmark](#) (Global Child Forum)

### iv) Relevant organisations and initiatives

- > [Global Network Initiative](#) (GNI)
- > [Business and Human Rights Resource Centre](#) (BHRRC)
- > [Tech Against Terrorism](#)
- > [Responsible Business Alliance](#) (RBA)