

Inter-agency Child Protection Case Management Data Protection and Information Sharing Protocol

Child Protection Sub-Sector, Rohingya Response, Bangladesh

Version 3, Revised in January 2026

Contents

1. Overview and Context.....	3
1.1 Purpose and Objectives of this Protocol	3
1.2 Context and Principles.....	3
1.3 Framework.....	3
1.4 Key Terminology used in the DPISP	3
1.5 Scope.....	6
1.6 Regulatory Framework	6
1.6.1 National Laws and Regulations; Organisational Policies; High Level Principles	6
1.6.2 Data Protection Impact Assessment	7
1.7 Process, Adherence, Modification.....	7
1.7.1 Process	7
1.7.2 Participants	7
1.7.3 Review	7
1.7.4 Process for Modification	7
1.8 Data Breaches.....	8
1.8.1 Role of Participants.....	8
1.8.2 Notification.....	8
1.9 Compliance	8
1.9.1 Participant Responsibility.....	8
1.9.2 Monitoring.....	9
1.9.3 Responsibility for Personnel.....	9
1.9.4 Supervision.....	9
1.9.5 Non-Compliance.....	9
1.9.6 Suspension of Information Sharing	9
1.10 Duration, Withdrawal, Termination.....	9
1.10.1 Duration	9
1.10.2 Withdrawal of a Participant.....	9
1.10.3 Consequences of Withdrawal of a Participant	10
1.10.4 Termination of this Protocol and Consequences	10
1.11 Settlement of Disputes	10
2. Key Data Protection Obligations	10
2.1 Do No Harm and Best Interests of the Child	10

2.2 Personal Data Protection Principles.....	11
3. Personal Data Points to be Shared.....	12
3.1 Case Referrals to Service Providers for Child Protection Case Management.....	12
3.2 Case Transfers.....	13
3.3 Case Conferences/Best Interests Determination (BID) Panels	13
4. Sharing Anonymous or Aggregated Data and other Sensitive Non-Personal Data	14
4.1 Local Authorities	14
4.2 Child Protection Coordination Mechanisms	15
4.3 Other Sectors	15
4.4 Donors.....	16
5. Special Considerations for Sensitive Non-Personal Data.....	17
6. Sharing Personal Data with and from UNHCR in Refugee Settings	17
6.1 Purposes for which UNHCR processes Personal Data received from Participants	18
6.2 Sharing of Personal Data between UNHCR and Participants	21
Annex 1 Information Security	23
Annex 2 CP Coordination Group, Coordinators and Consultation Process	27
Annex 3 Form of Adherence/Signature.....	28

1. Overview and Context

1.1 Purpose and Objectives of this Protocol

The purpose of this Data Protection and Information Sharing Protocol (DPISP or Protocol) is to provide specific guidance to enable an agreement to be reached on data protection and information sharing in the context of inter-agency child protection case management and related activities in Rohingya Response. This Protocol establishes agreed-upon guiding principles and specific provisions on data protection. It also details appropriate practices for data protection, including the safe, secure, and ethical collection, processing, storage, sharing and destruction of personal and non-personal data of vulnerable children in accordance with each participant's applicable data protection framework¹. 'Participants' refers to child protection agencies who are signatories to this protocol². This Protocol further describes the specific data points to be collected and shared by participants, on a need-to-know basis, with whom and under what circumstances, for what purpose, and based on an appropriate legitimate basis. These principles and provisions serve the objective of protecting against and mitigating potential risks to children and their families by ensuring the correct use and processing of data and information in the implementation of child protection case management.

1.2 Context and Principles

This DPISP is informed by the following principles:

- the general guiding principles of survival and development
- the best interests of the child
- the principles of child participation and non-discrimination
- the principle of 'do no harm'
- international principles and standards of personal data protection and privacy and respect for data subject rights

All these principles require that information is only shared on a 'need to know' basis.

Please refer to the principles defined in the [Inter Agency Guidelines for Case Management and Child Protection](#), Section 1, Page 10 and the [UNHCR Best Interests Procedure Guidelines](#), Section 3.5, Page 110 on Information Management.

Please see Section 2 on Key Data Protection Principles.

1.3 Framework

This DPISP aligns with applicable international and national legal frameworks and is informed by inter-agency guidance and policies including the Inter-Agency Case Management Guidelines and UNHCR Best Interests Procedure Guidelines. The approach contained in this DPISP is guided by the Convention on the Rights of the Child and aligned with the guidelines of the Inter-Agency Standing Committee, Global Protection Cluster and the Alliance for Child Protection in Humanitarian Action.

1.4 Key Terminology used in the DPISP

Anonymous Data means information that cannot be attributed as relating to an identifiable individual, by any means reasonably likely to be used, based on the data alone or in combination with other data. A person may sometimes be identifiable, even if they have not been named in the information, in which case the information would not be constituted as 'anonymous' but as Personal Data (see below). Data

¹ In respect to UN-system organizations, the High-Level Committee on Management (HLCM) has adopted the Personal Data Protection and Privacy Principles, which should serve as a foundational framework for the processing of personal data by UN entities, along with their specific policies. For organizations that do not enjoy privileges and immunities, reference should be made to applicable data protection legislation as well as sets of principles and other guidance such organizations are subject to..

² 'Participants' refer to child protection agencies and actors engaged in inter-agency child protection case management and/or Best Interest Procedure who are signatories to the protocol

is anonymous when it has undergone a process of removing or modifying all personal identifiers and codes that may be identifying in such a way that individual data subjects cannot be identified by any means reasonably likely to be used based on the data alone or in combination with other data.

Pseudonymised Data refers to data that has been anonymised by using a non-identifying code or name which cannot lead to the identification of the individual to whom it refers, without additional data being provided (e.g., a number sequence code + a code against geographical location or first two letters of the individual's home address).

Best interest of the child ensuring the full and effective enjoyment of all the rights recognized in the Convention on the Rights of the Child and the holistic development of the child. Among these rights, the right of the child to physical and emotional safety (their well-being) are of particular importance.³ In line with Article 3 of the United Nations Convention on the Rights of the Child (“**UNCRC**”), the best interests of the child should provide the basis for all decisions, actions, and interactions between the service providers with children and their families.

Caregiver in this DPISP refers to the child's parent, legal guardian or customary caregiver whom is responsible for the child's care and protection, biologically or as legally or otherwise designated.

Case Referral (as part of case management processes) is the process of formally requesting services for a child or their family from another agency (e.g., education, food, cash assistance, health care, etc.) through an established procedure such as an inter-agency referral pathway and/or standard referral form(s). The Child Protection case worker maintains overall responsibility and accountability for the child's case for which they are making referrals, and therefore responsibility for ensuring that referrals are made to quality service providers in a safe, ethical, and secure manner.

Case Transfer is the process that wherein cases are not closed but transferred from one Participant to another Participant. Often this happens when a child moves to another known location, but still needs case management to ensure care continuum and protection. Case Transfers also take place where the original caseworker or Participant is no longer best placed to lead, manage, and coordinate a child's case, or has concluded their employment in this role. Furthermore, Case Transfers can occur when an agency concludes operations or service provision in a country or location, and a new or other agency takes on their caseload to sustain service provision.

Child Protection Case Management is an approach for addressing the needs of an individual child who is at risk of harm or has been harmed. The child and their family are supported by a caseworker in a systematic and timely manner through direct support and referrals. Case Management provides individualized, coordinated, holistic, multisectoral support for complex and often connected child protection concerns. Case Management systems are an essential part of the child protection response.

Caseworker is the key frontline worker who must be trained on case management and responsible for coordinating, implementing, and following up on all actions needed to address an individual child's protection needs through the case management process.

Coordinator(s) refers to the inter-agency child protection coordinator(s)⁴ who are responsible for the coordination of child protection case management within a given Operational context or country. A Coordinator's role is to facilitate a collaborative process that ensures a well-coordinated and effective child protection response, ensuring quality programming and integration with other sectors.

Data Subject refers to a living individual whose Personal Data is being processed.

Data Breach means a breach of data security leading to the accidental or unlawful destruction, loss, alteration, or unauthorised disclosure of, or access to, Personal Data or Sensitive Non-Personal Data.

³ Committee on the Rights of the Child, General comment no. 14 (2013) on the right of the child to have his or her best interests taken as primary consideration (art. 3, para. 1), CRC/C/GC/14, 29 May 2013

⁴ According to the Child Protection Coordination Handbook, “Different contexts require different levels of staffing to ensure effective coordination. Coordination teams can comprise a coordinator who is dedicated to the role on a full-time or part-time basis”. CP AoR

https://www.cpaor.net/sites/default/files/2020-04/Child%20Protection%20Coordination%20Handbook_En.pdf

Data and Information – **Data** refers to ‘individual facts’ or units of information (data points) that don’t necessarily have meaning without interpretation. **Information** refers to organised data and/or an interpretation/analysis of combining facts or data points. The terms “data” and “information” are frequently used interchangeably but differ in what they constitute. Data can be interpreted as individual facts, while information is a combination of facts with meaning.

Informed Assent means the expressed willingness to participate in services by those persons who are assessed, by a child protection specialist or specialised agency, as i) not having capacity to give consent to participation but ii) as able to learn about, ask questions, and agree or decline to the collection and sharing of their personal data for the purpose of service provision.

Informed Consent means any freely given, specific and informed indication of an agreement by the Data Subject to the Processing of their Personal Data, which may be given either by a written or oral statement or by a clear affirmative action⁵. This applies to both the collection and sharing of personal data which constitutes Processing of personal data (see Processing below).

Mandatory reporting refers to the requirement under some legal or statutory systems for service providers to report certain categories of crimes or abuse (e.g., sexual violence, child abuse, etc.) or even report children’s status (e.g., arrival in country). The best interests of the child should be considered when Participants are considering whether to comply with such laws.

Participant means each agency or authority that signs this Protocol, whether on the date that this Protocol comes into effect or subsequently. A list of Participants and their official signatories is maintained up to date by the Coordinators as set out in this DPISP.

Personal Data means any information relating to an identified or identifiable individual (Data Subject, see above). An **identifiable individual** is one who can be identified, directly or indirectly, including by reference to (a) an identifier such as a name, an identification number, audio-visual materials, location data, an online identifier, (b) one or more factors specific to the physical, physiological, genetic, mental, economic, cultural, or social identity of the individual or (c) assessments of the status and/or specific needs, such as in the context of assistance programs.

It is important to note that a single data source may not make an individual identifiable. However, in combination, and with the application of new technologies, data sources may make the individual identifiable. Therefore, each data source should be assessed for actual or potential Personal Data content. Although different standards apply to Personal and Non-Personal Data, Non-personal data can also be sensitive (see Sensitive Non-Personal Data below), and its sharing should be assessed and limited accordingly.

Processing means any operation, or set of operations, automated or not, which is performed on Personal Data, including, but not limited to, the collection, recording, organization, structuring, storage, adaption or alteration, retrieval, consultation, use, transfer, dissemination or otherwise making available, correction, restriction, or destruction (partial or full).

Sensitive Non-Personal Data means data regarding a vulnerable group, that, if disclosed, could lead to risks for that group, or for individuals in that group. This can include data and information collected, used, stored, or shared by humanitarian and human rights organizations relating to protection risks, rights violations or the protection situation of specific groups. Or it could relate to the location of a specific individual and/or group. Examples include anonymous details of protection incidents, specific needs codes or other structured data about protection issues or vulnerabilities, details of assessed protection risks and needs, and information about protection services that have been provided to a group. This type of data may be in aggregate or anonymous form.

⁵ In many legislations, notably General Data Protection Regulation (GDPR), consent as a legitimate basis for personal data processing should be distinguished from ‘informed consent’ requested from a child and/or caregiver by a child protection case worker as an expressed agreement to participate in or be provided with a service. See e.g., EDPB Guidelines on consent: https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_202005_consent_en.pdf

Sensitive Personal Data means personal data that affects the Data Subject's most intimate sphere (i.e., most private thoughts, feelings and actions – relating to the person's sense of self) or relates to their unchangeable characteristics (e.g., race or ethnicity) and which, if misused or subject to a Data Breach, may result in discrimination against, or serious harm for, the Data Subject, or a breach of their fundamental rights. This could, for example, include data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union/staff association membership, genetic data, and biometric data capable of uniquely identifying a natural person, data concerning health, or data concerning an individual's sex life or sexual orientation.

Service Provider refers to organisations, actors, agencies, and individuals providing child protection case management or services related to child protection and child protection case management for the purpose of this DPISP.

Need-to-know principle refers to participants only having access to personal data when this specific information is necessary for them to take action on behalf of an individual child, such as providing appropriate services or referrals, or ensuring appropriate follow-up in line with the child's best interests. Participants may access need-to-know aggregate data (non-identifiable) when this information is required to support actions, planning or decision-making act on behalf of children generally, also in line with their best interests.

1.5 Scope

Child Protection Case Management: This DPISP is specific to child protection case management programming for Rohingya Refugees in Cox's Bazar and Bhasan Char, Bangladesh.

SOPs for Case Management: This DPISP is complementary and integral to the Standard Operating Procedures ("SOPs") for Child Protection Case Management in Cox's Bazar and Bhasan Char in the context the Rohingya Refugee Response of the finalised in July 2021.

Information Management Systems: This DPISP is not limited to any single digital information management system and is applicable to all relevant data protection and information sharing practices, in line with inter-agency case management SOPs, regardless of modality, when used for inter-agency child protection case management and related activities.

Data: This DPISP applies to all Personal Data and Sensitive Non-Personal Data that is collected, stored, shared, retained, destroyed, or otherwise processed in the context of inter-agency child protection case management and related activities, and in connection with the objective and purpose of this DPISP.

Relationship of the DPISP to other agreements or arrangements: It is recognized that Participants to this DPISP may have other agreements and arrangements governing or covering the sharing of non-personal data and/or personal data and which may overlap with this DPISP. It is encouraged that such parties reach arrangements on a bilateral level to ensure that this DPISP can be carried out without conflict to those other agreements.

1.6 Regulatory Framework

1.6.1 National Laws and Regulations; Organisational Policies; High Level Principles

- a) The following national laws and regulations have been considered in the development of this DPISP: Data Protection Act, 2023; the Digital Security Act, 2018; and the Children Act, 2013
- b) The DPISP has been developed with consideration high-level principles, internal and/or organisational codes of conduct, policies or guidelines related to data protection for Participants. It is further informed by humanitarian and child protection principles, inter-agency guidelines, and organisational policies, including inter-agency CP Case Management Guidelines, PSEA, child safeguarding and Personal Data Protection policies.

- c) Participants recognise that UN agencies, who are Participants to this protocol are subsidiaries of the United Nations, an international organisation established by treaty, and that as a result of its status it has certain privileges and immunities as described in the 1946 Convention of the Privileges and Immunities of the United Nations (the “General Convention”). This means that data and information shared between UN entities and Participants cannot be disclosed, provided, or otherwise made available to, or searched, confiscated or otherwise interfered with by a governmental body, agency or other authority, including any court or other tribunal, unless such privileges and immunities are expressly waived in writing by the respective UN agency.

1.6.2 Data Protection Impact Assessment.

This DPISP is informed by the Data Protection Impact Assessment (“**DPIA**”) which was conducted in October 2018 and to be reviewed based on the changing context and any new risk arising.

1.7 Process, Adherence, Modification

1.7.1 Process.

This DPISP was developed and endorsed on 15th April 2026 by the Case Management Technical Working Group (CMTWG) under the leadership of the Child Protection Sub Sector (CPSS), hereafter referred to as the CPSS. This Protocol was developed in collaboration with each Participant. All the Child Protection Case Management agencies were given the opportunity to contribute to the content of this Protocol. Details of the process of consultation and membership of the CMTWG and CPSS, and the coordinators are set out in Annex 2.

1.7.2 Participants.

It is mandatory for all Participants, including Participants that join the CMTWG of the CPSS by signing this Protocol after the Effective Date of this Protocol, to adhere to and comply with this DPISP.

- Each Participant is required to confirm its agreement to adhere to and comply with this Protocol by signature of its authorized representative of an Adherence Document in the form set out in Annex 3.
- The CPSS coordinator is responsible for sharing the final endorsed version of this Protocol with each Participant, maintaining the list of Participants and the record of the Adherence Document signed by each Participant, and storing the PDF of this Protocol and each Adherence Document in hardcopy and/or digital softcopy.

1.7.3 Review.

This Protocol will be reviewed periodically, annually if possible, from the effective Date. The first review will be scheduled and facilitated under the coordination of the CMTWG of the CPSS. If there is a significant change in the context, the Participants, the child protection laws and procedures, or the data protection regulations in the country, this Protocol (and the related SOPs) should be reviewed by the CMTWG prior to the next scheduled review. All such reviews will be conducted in consultation with the Participants.

1.7.4 Process for Modification.

If, following review and consultation, the CPSS considers that this Protocol should be modified, the following steps will apply:

- a) The CPSS will develop and endorse the proposed modifications to this DPISP, and the Coordinators will communicate the proposed modifications with all Participants.
- b) If any Participant objects to the proposed modifications, it must communicate the reasons for its objections in writing to the Coordinators within 14 days of receiving notice of the proposed modifications or such longer time period provided by the CPSS (the Modification Notice Period).

- c) If no objections are received during the Modification Notice Period, the proposed modifications will be submitted to CPSS SAG for approval.
- d) If any objections are received by the Coordinators during the Modification Notice Period, the CPSS will give due consideration to the reasons for the objections. They will decide whether to proceed with the modifications as originally proposed, or to adapt the modifications to reflect some or all the objections received. If the CPSS decides to proceed with the modifications as originally proposed, then the coordinators will, in writing, notify the Participants that the modifications will take effect seven days after such notification. If the CPSS decides to adapt the modifications, the process set out in this Section 1.7. will be repeated.
- e) The Coordinator will share the final endorsed modified version of the DPISP with each Participant and will store the pdf of the modified version in digital softcopy.
- f) Each Participant will be expected to comply with the updated DPISP from the effective date of the modifications as set out in this Section 1.7.4. The signature of a new Adherence Document by Participants is not required for any such updated version of this DPISP.

If urgent changes are required, the CMTWG may shorten the periods mentioned in this Section as the CMTWG considers appropriate. The coordinator will ensure that such shorter periods are promptly communicated to the Participants.

1.8 Data Breaches

1.8.1 Role of Participants

Each Participant commits to the following provisions:

- If the Participant is the presumed source of a Data Breach, it will investigate such incidents and implement all necessary damage mitigation and remedial actions to remedy the Data Breach as soon as possible in compliance with this DPISP.
- If the Participant is not the presumed source of a Data Breach, it will promptly provide its reasonable cooperation for the investigation of such incident and for the implementation of all necessary damage mitigation and remedial actions to remedy Data Breach.

1.8.2 Notification

Each Participant will, in writing, notify Case Management Technical Working Group (CMTWG) under the leadership of the Child Protection Sub Sector (CPSS) within 24 hours of becoming aware of any actual, suspected or threatened Data Breach relating to Personal Data or Sensitive Non-Personal Data shared under this DPISP.

If the scope of Data Breach includes personal data of persons of concern to UNHCR, the Participant shall directly notify UNHCR copying CPSS coordinator about the Data Breach as soon as possible upon its discovery and coordinate with UNHCR the investigation of the Data Breach and implementation of mitigating measures.

Noting: This DPISP is not intended to represent compliance with requirements under national legal frameworks and regulations that may be applicable to a Participant. Thus, while the DPISP is designed to be aligned with the relevant national legal framework, each Participant should comply with data breach notification measures under applicable law.

Further, bilateral agreements between Participants outside of the scope of the DPISP may require particular notifications and remedial actions in the event of a data breach and this DPISP should not affect adherence to such bilateral agreements.

1.9 Compliance

1.9.1 Participant Responsibility.

Compliance by a Participant and its personnel with this Protocol is the responsibility of the individual agency or authority concerned. Each Participant commits to take a proactive approach to asking for support from the CMTWG or the CPSS on compliance with the DPISP including data protection and

information sharing, which shall rely on advice by each Participant's Data Protection Officer or Focal Person, where such officer or focal person has been designated.

1.9.2 Monitoring.

Each Participant will independently monitor and evaluate its compliance with this DPISP and cooperate with any joint and/or independent reviews in line with the provisions of this DPISP.

1.9.3 Responsibility for Personnel.

Each Participant confirms its commitment to ensure that its personnel with access to child protection case management data:

- a) Are aware of, understand, and comply with the contents of and obligations in this DPISP, including the obligations to comply with the Participant's internal policies and regulations, including data protection and privacy policies as applicable.
- b) Are trained on the content of this Protocol (and other relevant data management and sharing documents), including on how to handle confidential information and on the consequences of breaching this Protocol; how to identify, assess, and report Data Breaches; how to fulfil Data Subject Rights.

1.9.4 Supervision.

Compliance with this Protocol will be supervised by the CPSS Coordinator.

1.9.5 Non-Compliance.

If any Participant becomes aware of any suspected non-compliance with this Protocol, it will immediately notify the CPSS Coordinators who will in turn promptly notify the CPSS members. The CPSS Coordinator will work with the affected Participants to address the suspected non-compliance. Actions to address the suspected non-compliance may include, but are not limited to, additional data security requirements for the non-compliant Participant or capacity building provided to the non-compliant Participant.

In addition, the CPSS may temporarily suspend information sharing under this Protocol in line with the procedures set out in 1.9.6. In the case of an inter-agency digital case management system, the CPSS may suspend user access rights to the system in a manner consistent with the key Data Protection Principles set out in this DPISP.

In exceptional circumstances, the CPSS may require the withdrawal of the non-compliant Participant from this DPISP and the provisions of Section 1.10.2.

1.9.6 Suspension of Information Sharing.

If this DPISP is breached, each Participant reserves the right, with good intention, to escalate the suspected non-compliance to the CPSS for collective decision making. This may include temporarily stopping of information sharing for both Personal Data and Sensitive Non-Personal Data. Before doing so, it will inform CPSS in writing of the reasons for stopping data and information sharing.

1.10 Duration, Withdrawal, Termination

1.10.1 Duration

This Protocol will enter into force on the date that it is signed by at least two Participants and will continue to remain in force for so long as there are at least two Participants signatory to this Protocol.

1.10.2 Withdrawal of a Participant

If a Participant withdraws from this Protocol due to the normal cessation of its child protection activities in the country or for any other reason, it will provide the CPSS Coordinators as much advance notice as possible and in any case no less than 30 days' prior notice of its withdrawal. The withdrawal notice should specify the reasons for the withdrawal of the Participant and a proposal for the smooth transfer of activities to other Participants.

1.10.3 Consequences of Withdrawal of a Participant

If a Participant withdraws for any reason (including but not limited to non-compliance to this DPISP, phasing out) from this Protocol or is required to withdraw as provided in 1.9.5

- a) This Protocol will not automatically terminate and will remain in full force and effect for the remaining Participants.
- b) The withdrawing Participant will work together with the coordinator and the other Participants in good faith to agree and implement a plan to manage the case load transferral and handover prior to the effective date of withdrawal of the withdrawing Participant and to stop active access to this data ("**Transition Plan**").
- c) The withdrawing Participant commits not to remove any personal and non-personal data from the country.
- d) On the effective date of withdrawal, access by the withdrawing Participant (and its personnel) to digital information management systems will be revoked, and/or all paper-based filing systems will be safely transferred by the withdrawing Participant in accordance with the Transition Plan.
- e) The withdrawing Participant will continue to comply with the key principles set out in Section 2 when processing the data that is subject to this Protocol.

Note: In the case that the withdrawal or required withdrawal of the Participant requires a caseload transfer, please see below Section 3.2. on Case Transfer.

1.10.4 Termination of this Protocol and Consequences

If the case management work is concluded, the Participants will work together under the guidance of the CPSS to ensure the smooth closure of the case management system in a manner consistent with the key Data Protection Principles set out in this DPISP.

1.11 Settlement of Disputes

- a) The Participants shall use their best efforts to settle amicably any dispute, controversy or claim arising out of or relating to this Agreement (a Dispute).
- b) If an amicable settlement of a Dispute is not reached pursuant to Article 6(a), the Dispute shall be settled by an agreed non-judicial mode of resolution (including arbitration).
- c) If a United Nations System organization is involved in a Dispute that also involves a Participant that is not a United Nations System organization, the non-judicial mode of resolution of such Dispute will consist of binding arbitration in accordance with the Arbitration Rules then obtaining of the United Nations Commission on International Trade ("UNCITRAL"). Any award rendered under such binding arbitration will be the final adjudication of any such Dispute. The arbitral tribunal will have no authority to award punitive damages. In addition, the arbitral tribunal will have no authority to award interest in excess of the London Inter-Bank Offered Rate ("LIBOR"), or any successor rate, then prevailing, and any such interest will be simple interest only.

Nothing in this DPISP will be deemed a waiver, express or implied, of the privileges and immunities under international law or otherwise of the United Nations, or any Participant that is a subsidiary organ of the United Nations or a United Nations system organization.

2. Key Data Protection Obligations

2.1 Do No Harm and Best Interests of the Child.

The protection of the Personal Data of children and their families will be guided by the highest ethical principles, including the principles of **do no harm** and the **best interest of the child**. The protection of children and their safety will be paramount considerations. All Participants will take all precautions to do no harm (including circumstances leading to statelessness and for raising concerns of non-refoulement) and undertake all possible mitigation measures against foreseeable risks, with particular attention to avoiding harms to children.

2.2 Personal Data Protection Principles.

The following core principles must be followed when collecting, sharing and otherwise processing Personal Data:

- a) **Legitimate and fair processing:** Processing of Personal Data may only be carried out on a **legitimate basis** and in a fair and transparent manner in relation to the specific purpose. Each Participant will process Personal Data on an appropriate legitimate basis in accordance with its regulatory framework, including but not limited to consent, or the best or vital interests⁶ of the particular child. Consent for the processing of a child's personal data, when applicable, should generally be sought from the child's caregiver with the child being sufficiently informed about the processing according to the child's age and maturity. Regardless of the applicable legitimate basis, Data Subjects must be informed, in an easily understandable manner, about what type of Personal Data needs to be collected, for which purpose, with whom the data may be shared and with whom it will not be shared, whether there will be any detriment if they object to the processing, who will have access to their data, including under this DPISP, and whom they can contact if they want to exercise their data subject rights and/or if they have concerns with respect to the processing of their data. The legitimate basis and the information provided should be recorded in an appropriate manner.
- b) **Purpose specification:** Personal Data will only be processed by Participants for specific and legitimate purposes. Within the scope of this Protocol, this means purposes that are ensuring children and their families are able to receive child protection case management services and enabling the provision of holistic, multi-sector services and durable solutions as needed, based on the best interests of the child. Personal Data should not be processed in any way that is incompatible with those purposes originally specified. Section 3 below sets out which Personal Data points can be shared for these purposes.
- c) **Data Minimisation - Necessity and proportionality:** The processing of Personal Data will be adequate, relevant, and not excessive to the original specific purpose(s) for which it is being processed.
- d) **Respect for the Data Subject's rights:** Children and families have rights in relation to information, access, correction and, deletion of their Personal Data and objection to its processing during all stages of such processing, as elaborated within the 1989 Convention on the Rights of the Child, General Data Protection Regulation and relevant global, regional or national data protection frameworks. All Data Subjects will be clearly informed of these rights, ensuring understanding and enabling them to exercise these rights meaningfully and safely.
- e) **Confidentiality and Security:** In order to ensure the confidentiality, availability, and integrity of Personal Data (and Sensitive Non-Personal Data), each Participant (and Service Provider) shall consult with an information security specialist or designated focal person for information security in their organisation, and put in place physical, technical and organizational information security measures (for any Personal Data when stored, in use or in transit) which are appropriate for the risks caused by the processing and in line with international best practice. Annex 1 sets out examples of organizational, technical, and physical information security measures which shall be implemented to the extent applicable to the type of processing. Given that the appropriateness of information security measures depends on the type of processing, those measures are not an exhaustive list and do not relieve the Participant from its obligation to determine appropriate security measures for the type of processing and associated risks. One important security measure is **access management procedures to ensure that data is only accessed by authorised personnel on a need-to-know basis**. It requires that only those personnel should obtain access to the Personal Data which needs to know such data in order to perform necessary activities to

⁶ Vital interests generally refer to circumstances of "life or death" wherein it may be absolutely necessary to process an individual's personal data if their life and survival is at risk, without their informed consent, with procedural safeguards as set out in case management standard operation procedures and abiding to inter-agency guidelines on breaking confidentiality.

reach the purpose of processing. For Sensitive Personal Data, additional organizational and technical safeguards should be used to protect data subjects against identified risks associated with the processing of that data. These can include strict access controls and role-based permissions, strong internal data sharing protocols and confidentiality agreements, specialised training for staff, safe data collection practices, secure physical storage, internal accountability and incident reporting.

- f) **Accuracy:** Personal data should be maintained, accurate and up to date in relation to the purpose(s) for which it is processed.
- g) **Retention Limitation:** Personal Data shall be deleted from any and all systems once it is no longer necessary for the purposes for which it is being processed or compatible purposes. There may be specific requirements for retention for refugees, asylum seekers, children associated with armed forces or armed groups, children affected by armed conflict and the monitoring and reporting mechanism for grave violations of children's rights.
- h) **Accountability.** Each Participant responsible for personal data processing should be able to demonstrate its compliance with the principles and assign a supervisor.

See Annex 1 on Information Security

3. Personal Data Points to be Shared

3.1 Case Referrals to Service Providers for Child Protection Case Management

- a) **Personal Data of a child is shared with a Service Provider, including a government service provider, which is receiving a referral for the provision of services** as needed based on the best interests of the individual child.
 - Personal Data shared must be limited to only the information necessary for the service provider to provide that service effectively (from the list of Personal Data points set out in paragraph (b) below). Personal Data will be shared from the case worker managing the case directly to the responsible focal point/service provider
 - Personal Data should only be shared provided that the service provider can afford the same level of data protection as outlined in this DPISP.
 - Personal Data sharing shall be done by secure means, to the furthest extent possible, as established in Annex 1 to this Protocol.
 - The child and caregiver must be informed about the Personal Data necessary for provision of the service, the implications of refusing the Personal Data transfer, and given an opportunity to object prior to the sharing of Personal Data.
- b) **The following data may be shared, when necessary and appropriate for the referral:**
 - **Basic Biographical data including** Name, date of birth, age (or estimated age), sex, country of origin, child's name, and the caregiver's name, unless not in the best interests of the child.
 - **Unique Identifier:** National Identity ("ID") number, case number, UNHCR ID/proGres number, or Primero CPIMS+ generated number.
 - **Contact Details and Address:** current contact information and preferred method for contact, address, and current location / place of residence (the latter if safe and necessary).
 - **Confirmation of the child and/or caregiver's Consent or Assent** for the service by a specific Service Provider (in line with referral form), or confirmation that the referral is being done without Consent or Assent in the best interests of the child as per agreed processes.

- **Personal vulnerabilities or specific needs:** (e.g., unaccompanied child, separated child, child not in school, health condition, disability etc) limited to the specific need(s) for which the referral is being made, and strictly relevant information based on the need-to-know principle.
- c) Participants are responsible to ensure compliance with the principles as set out in the Protocol and applicable data protection framework in response to data subject requests.

3.2 Case Transfers

a) **Case Transfers can take place within the organization.**

Personal Data is shared within an organisation on a need-to-know basis and through secure means, from a case worker or case supervisor to another case worker, or to a case worker/case supervisor in another organisation when it has been agreed that that a new case worker or agency will be managing the case.

The child and the child's caregiver (where relevant and appropriate) must be consulted and provide Consent to a change of case worker prior to the case transfer taking place. Children and their caregiver should be given the opportunity to request that specific information is withheld, this should be done unless it is not in the best interest of the child to do so and has been determined through relevant processes to be so.

- All relevant data, with the consent/assent of the child or caregiver, will be securely shared unless it is not in the best interests of the child. Normally, unless there is an objection to sharing or limitation to consent, the type of data should be minimised to only that which is proportional and necessary. Where no consent/assent can be obtained, sharing should again be limited to only data which is proportional and necessary for the specified purpose.

b) **Case transfers between Participants**

- Data subjects need to be informed about the purposes of Personal Data transfer, the implications of refusing the transfer, and given an opportunity to object to the transfer partially or in full. In particular, it needs to be clearly communicated to the Data Subjects that the data receiving Participant is responsible for the secure processing of their data from the point of transfer and where and how they can exercise their data subject rights.
- Personal Data sharing between the Participants shall be done by secure means as established in Annex 1 to this Protocol.

c) **Case transfers across borders, outside the locations for Case Management relevant to this DPISP**

In the event of cross-border case transfers beyond the geographical scope of this DPISP a specific data sharing agreement⁷ needs to be in place or developed between the agencies and relevant authorities in the respective locations which are not Participants to this DPISP. Personal Data should only be shared if the other party can demonstrate that they can provide the same level of data protection and confidentiality outlined in this DPISP. Consent of the caregiver and assent of the child and must be obtained before sharing information.

3.3 Case Conferences/Best Interests Determination (BID) Panels

Case Conferences can take place within the organization or amongst multiple Participants, according to internal and inter-agency standard operating procedures (SOPs). They may also include a specific

⁷ A data sharing agreement or data protection agreement is normally a bilateral agreement between two parties governing specific types of data transfers for specified purposes. This can be between two or more parties.

service provider that is not from a Participant agency but who may have worked with a child and be asked to relay specific inputs/insights on the case.

- The child (and the child's caregiver where relevant and appropriate) must be consulted and provide Consent to participation prior to the case conferencing taking place. Once informed about the purposes of the Case Conference/BID Panel, the personal data required, and the implications of not providing this Personal Data, children and their caregiver should be given the opportunity to request that specific information is withheld. This should be done unless it is not in the best interest of the child to do so and has been determined through relevant processes to be so. Please see the [Inter-agency Case Management Guidelines](#) and [UNHCR Best Interests Procedure Guidelines](#) for detailed information on the roles and responsibilities in case conferencing and BID panels.
- A case conference/BID Panel would normally only require the processing of Personal Data without the Data Subject being able to be identified (e.g. via the use of 'pseudonyms' and other efforts to anonymised the data). Identifying information may only be shared with particular panel members on a 'need to know' basis proportionate to the purpose.

4. Sharing Anonymous or Aggregated Data and other Sensitive Non-Personal Data

4.1 Local Authorities

- a) **Only Anonymous Data (e.g., aggregated data) can be shared with Local Authorities to fulfil their role and mandate, for the purpose of coordination for the provision of services,** based on the provisions below⁸:

Note: For the purpose of this section, the local authorities include, inter alia: Refugee Relief and Repatriation Commissioner (RRRC), Department of Social Services (DSS), Camp in Charge (CIC) and Police.

- Aggregated data will be shared based on the 'need-to-know' principle, the best interests of the child, and the 'do no harm' principle.
 - Aggregated data may be shared unless context specific circumstances require further assessment before agreeing to this.
 - Aggregated data will only be shared from and by the CPSS Coordinator to the agreed authority at the local or national level.
- b) When sharing aggregated data with local authorities for the purpose of coordination, **the following data may be shared, if needed:**
- Total number of children receiving child protection case management services, disaggregated by sex, age, legal status or category (e.g., national, asylum seeker, refugee, internally displaced person)
 - Type of protection concerns (noting the importance to consider and mitigate the risk incurred by sharing certain types of information based on the real or potential risk for identification and/or harm of the Data Subject)
 - Type of care arrangements
 - Type of services needed
 - Type of services provided

The following provisions for sharing aggregated data with local authorities have been agreed by the Participants. Ad hoc requests for information by local authorities should not be provided without first gaining approval by the CPSS/Protection Sector, this includes at camp level as well and other authorities.

⁸ Noting that Personal Data can be shared with Local Authorities for the purpose of making a referral for service provisions, wherein the relevant Authority is a participant to the DPISP and a service provider.

4.2 Child Protection Coordination Mechanisms

Aggregated data can be shared with relevant Child Protection Coordination Mechanisms to allow for situation and response monitoring. The analysis of anonymous, aggregated, and sex/age disaggregated data provides valuable means for CP Coordination forums (like the Child Protection Sub-Sector, Case Management Technical Working Group for example) to derive a context specific understanding of the child protection situation and response in the specific location.

- Aggregated data can be shared based on the 'need-to-know' principle, the best interests of the child, and the 'do no harm' principle.
- Aggregated data will only be shared by a designated focal person per agency to the relevant Coordinator.

When sharing anonymous data with the CPSS for the purpose of situation and response monitoring, the following data may be shared (if needed, as agreed):

- Total number of children receiving child protection case management services, disaggregated by sex, age, legal status or category (e.g., national, asylum seeker, refugee, internally displaced person)
- Percentage of cases by geographical areas (governorate/district/sub-district/camp)
- Total number of open cases disaggregated by sex, age, legal status, or category
- Total number of closed cases disaggregated by sex, age, legal status, or category.
- Total number of transferred cases disaggregated by sex, age, legal status, or category.
- Number of cases reopened.
- Total number of separated children disaggregated by sex, age, legal status, or category.
- Total number of unaccompanied children disaggregated by sex, age, legal status, or category.
- Type of care arrangements (% of cases per care arrangement) disaggregated by sex, age, legal status, or category.
- Type of protection concerns, % of protection concerns (e.g., child labour, children associated with armed forces or armed groups, MHPSS, gender-based violence etc.) disaggregated by sex, age, legal status, or category.
- Case risk level (low, medium, high) disaggregated by sex, age, legal status, or category.
- Cases requiring family tracing and reunification (disaggregated by sex, age, legal status, or category).
- Type of services provided (disaggregated by sex, age, legal status, or category).
- Type of services needed (disaggregated by sex, age, legal status, or category).
- Number of referrals made per category e.g., health, education, psychosocial support, cash assistance etc (disaggregated by sex, age, legal status, or category).

4.3 Other Sectors

Anonymous and aggregated data can be shared with other sectors such as coordination mechanisms for the purpose of joint coordination on service provision and joint situation and response monitoring. Such information can be shared with other sectors such as, for example: Protection, GBV, Education, CCCM/Shelter, WASH and Livelihoods.

- Anonymous and aggregated data will be shared based on the 'need-to-know' principle, the best interests of the child, and the 'do no harm' principle.
- Anonymous and aggregated data will be shared only from the CPSS/CMTWG to the other coordination body/bodies/sector(s).

When sharing anonymous and aggregated data with other coordination bodies or focal persons, for the purpose of coordination and joint situation and response monitoring, the following data may be shared (if needed):

- Total number of children receiving child protection case management services, disaggregated by sex, age, legal status or category (e.g., national, asylum seeker, refugee, internally displaced person)

- Total number of open cases disaggregated by sex, age, legal status, or category
- Total number of closed cases disaggregated by sex, age, legal status, or category.
- Total number of separated children disaggregated by sex, age, legal status, or category.
- Total number of unaccompanied children disaggregated by sex, age, legal status, or category.
- Type of care arrangements (% of cases per care arrangement) disaggregated by sex, age, legal status, or category.
- Type of protection concerns, % of protection concerns (e.g., child labour, children associated with armed forces or armed groups, MHPSS, gender-based violence etc.) disaggregated by sex, age, legal status, or category.
- Case risk level (low, medium, high) disaggregated by sex, age, legal status, or category.
- Cases requiring family tracing and reunification (disaggregated by sex, age, legal status, or category).
- Type of services provided (disaggregated by sex, age, legal status, or category).
- Type of services needed (disaggregated by sex, age, legal status, or category).
- Number of referrals made per category e.g., health, education, psychosocial support, cash assistance etc. (disaggregated by sex, age, legal status, or category).

4.4 Donors

Only Aggregated data can be shared with Donors to ensure accountability for the appropriate use of funds and to demonstrate progress in the provision of child protection case management services, as well as to highlight specific gaps and needs for further funding.

- Aggregated data will be shared based on the 'need-to-know' principle, the best interests of the child, and the 'do no harm' principle
- Aggregated data can only be shared by an agency's designated focal persons to the designated donor focal person or technical expert.
- Aggregated data may be shared using the donor's reporting template, so long as it complies with the provisions as set out in this DPISP.

Noting: The provision of funding by a donor(s) does not in itself entitle the donor to access to personal data and confidential information. Providing access to personal data for purposes that can be fulfilled by anonymous data would constitute a violation of the data protection principle of data minimisation and 'do no harm' principles and would be a significant child safeguarding risk, due to the vulnerable status of children and families receiving child protection case management services. Personal data will not be shared with donors. .

When sharing aggregated data with donors the following data may be shared (if needed, as agreed):

- Total number of children receiving child protection case management services, disaggregated by sex, age, legal status or category (e.g., national, asylum seeker, refugee, internally displaced person).
- Total number of open cases disaggregated by sex, age, legal status, or category.
- Average time elapsed from case opening to closure for low-medium risk cases.
- Average time elapsed from case opening to closure for high-risk cases.
- Number of cases reopened.
- Percentage of cases by geographical areas (governorate/district/sub-district/camp)
- Type of reasons for case reopening disaggregated by sex, age, legal status, or category.
- Total number of closed cases disaggregated by sex, age, legal status, or category.
- Total number of separated children disaggregated by sex, age, legal status, or category.
- Total number of unaccompanied children disaggregated by sex, age, legal status, or category.
- Type of care arrangements (% of cases per care arrangement) disaggregated by sex, age, legal status, or category.
- Type of protection concerns, % of protection concerns (e.g., child labour, children associated with armed forces or armed groups, MHPSS, gender-based violence etc.) disaggregated by sex, age, legal status, or category.
- Case risk level (low, medium, high) disaggregated by sex, age, legal status, or category.

- Type of cases requiring family tracing and reunification (disaggregated by sex, age, legal status, or category)
- Type of services provided (disaggregated by sex, age, legal status, or category).
- Type of services needed (disaggregated by sex, age, legal status, or category).
- Number of referrals made per category e.g., health, education, psychosocial support, cash assistance etc. (disaggregated by sex, age, legal status, or category).

In exceptional circumstances, such as the specific purposes of donation monitoring including programme monitoring, requests to view case files can only be complied with if they are redacted and contain no identifying information.

5. Special Considerations for Sensitive Non-Personal Data

The Participants recall that if Non-Personal Data is capable, either on its own or together with other information available to the recipient of the data, of identifying an individual, then such data is Personal Data and can only be shared or otherwise processed in accordance with Section 2 and 3.

This can include data (and information) collected, used, stored, or shared by humanitarian and human rights organizations relating to protection risks, rights violations or the [protection] situation of specific groups or it could relate to the location of a specific individual and/or group. Examples include details of protection incidents, specific needs codes or other structured data about protection issues or vulnerabilities, details of assessed protection risks and needs, and information about protection services that have been provided to a group. This type of data may be in aggregate or anonymous form.

The Participants have agreed that the following types of Non-Personal Data are to be classified as Sensitive Non-Personal Data:

- Children in conflict with the law
- Child survivors of sexual violence
- Children recruited, abducted and other violations perpetrated by armed groups or armed forces and criminal gangs
- New-born unaccompanied child (abandoned new-born)
- Geographical (block level and camp level) number of missing/lost child
- Children identified as victims of trafficking

This is covered by safeguards as set out in this agreement

6. Sharing Personal Data with and from UNHCR in Refugee Settings

In line with each agency's applicable data protection framework, this DPISP, and all applicable data protection and information security policies and regulations, Participants will share personal data with UNHCR in a predictable and timely manner in refugee and mixed settings for the purpose of:

- Delivering child protection case management services and Best Interests Procedures.
- Contributing to effective coordination of Best Interests Procedure including situation, response, and child protection case management programme monitoring.
- Prioritising children for assistance and durable solutions, including those provided exclusively by UNHCR.

The sharing of personal data between each specific agency and UNHCR may additionally be regulated in this DPISP and aligned with governing Data Protection Policies bilateral data sharing agreements and partnership agreements. This section is informed by and aligned with Section 3.5. of the [2021 UNHCR Best Interests Procedure Guidelines for Assessing and Determining the Best Interests of the Child](#) and takes into account all relevant principles applicable to the context of child protection case management in refugee settings within the implementation of BIP for refugee and asylum-seeking children.

Please see Section 3.5. on Information Management for Case Management (Best Interests Procedure) which further details the following:

- Data elements to be shared for specific purpose for protection services and assistance immediately and in the future for which referrals to UNHCR can be made, and examples of protection services and assistance services that are provided either immediately or in the future, based on information known to UNHCR, for which referrals to UNHCR can be made.
- Example data elements to be shared with UNHCR by partners implementing Best Interests Procedures
- Example data elements to be shared with partners by UNHCR in Best Interests Procedure cases managed by that partner.
- Overall guidance on information management in the context of Best Interests Procedures

In line with its Data Protection Policy⁹, UNHCR will share Personal Data of children in the context of implementing Case Management (Best Interests Procedure) and refugee protection case management, generally based on consent or the vital or best interests as relevant legitimate bases for specific purposes, as described below. Consent or Assent for provision of service needs to be received, unless – in exceptional cases – where consent or assent cannot be obtained, and the referral is in the best interests of the child. The child/caregiver needs to be informed about the data sharing required for provision of service and given an opportunity to express any concerns or objections before any personal data about an individual child, or other individual, is shared. This should be done in accordance with the Inter-agency Case Management guidelines and UNHCR BIP Guidelines, and Case Management Standard Operating Procedures of Cox's Bazar and Bhasan Char, Bangladesh.

Before making any referrals for services, UNHCR informs the child and caregiver about the purposes of referral and data sharing, what Personal Data is required for it, and the available alternatives in case of refusal. UNHCR should also obtain consent or assent for provision of service from caregivers before making a referral to a partner. Whether UNHCR process personal data based on consent or the best interest, assent of the child in question should be sought depending on his/her level of maturity (UNHCR BIP Guidelines, 2021, Page 117).

All information, including related case data, shall be stored securely in UNHCR's designated system (proGres) in accordance with UNHCR's Data Protection Policy. Access will be restricted to authorized personnel only, and appropriate technical and organizational measures shall be applied to ensure confidentiality, integrity, and protection against unauthorized access or disclosure.

6.1 Purposes for which UNHCR processes Personal Data received from Participants

Pursuant to UNHCR's mandate to provide international protection and to seek permanent solutions for persons within the Office's mandate responsibilities, UNHCR may process personal data received from Participants:

- a) To deliver long-term protection and solutions to children at risk with UNHCR mandate as the legitimate basis for personal data processing, in addition to best interests of the data subject. The fulfilment of this purpose may involve several data processing operations, including data collection, best interest determination procedures, and sharing to and from relevant stakeholders.

The minimum necessary personal data to be shared with UNHCR on children at risk and children receiving case management (Best Interests Procedure) for whom UNHCR may provide durable solutions is as follows:

- Basic Biographical data including Name, date of birth, age (or estimated age), sex, country of origin

⁹ [General Policy on Personal Data Protection and Privacy | Refworld](#) [Policy on the Protection of Personal Data of Persons of Concern to UNHCR | Refworld](#)

- Unique Identifier: UNHCR Individual proGres number [if not available, the Child's full name with the Family Counting Number (FCN)/Master Registration Card (MRC) Number can be provided] or any other UNHCR identifiers
- Contact Details and Address: current contact information and preferred method for contact, address, and current location / place of residence)
- Current Care Arrangement/ Living Arrangements including details of the Parent/Caregiver
- Disability Status
- Education
- Personal vulnerabilities or specific needs: [This includes the status of the child i.e. Unaccompanied Child; Separated child, Child-headed household, Child in foster care, Child Parent, Child Carer, Child Headed Household)
- Status of Child Protection Case Management [i.e. Active Case; Closed Case; Child Protection Assessment also referred to as Best Interests Assessment (BIA) Completed; BID initiated; BID Approved by BID panel)
- Referral Information [Summary of the child protection concerns and reasons for referral]

UNHCR Child Protection focal person(s) may request additional personal data for a child at heightened risk to ensure timely referral implementation and information sharing for the purposes of supporting long-term protection and solutions, and where applicable to support the implementation of the Best Interests Determination (BID) process. Such requests shall be made to ensuring compliance with data protection principles of necessity, proportionality and confidentiality, as well as upholding the Do no Harm principle and Best Interests of the child while minimizing duplication. UNHCR may request the following additional personal data from a Participant:

- Summary of the Child Protection Case at present
 - Completed Child Protection comprehensive assessment also referred to as Best Interests Assessment (BIA) [Noting, in some circumstances, BID is not required, and a Child Protection comprehensive assessment may suffice]
 - Where applicable and available, the Best Interests Determination (BID) Report as part of the established Best Interests Determination Process in Bangladesh, in accordance with the BID Terms of Reference and Inter-Agency Case Management SOPs.
- b) To provide protection services and assistance for individual referrals including but not limited to Registration, Legal Protection, NFIs and any other services within UNHCR mandate as the legitimate basis for personal data processing. The fulfilment of this purpose may involve several data processing operations, including data collection, best interest determination procedures, and sharing to and from relevant stakeholders.
- a. The minimum necessary personal data to be shared with UNHCR for provision of protection services and assistance is as follows:
- Basic Biographical data including Name, date of birth, age (or estimated age), sex, country of origin
 - Unique Identifier: UNHCR Individual proGres number [if not available, the Child's full name with the Family Counting Number (FCN)/Master Registration Card (MRC) Number can be provided] or any other UNHCR identifiers
 - Contact Details and Address: current contact information and preferred method for contact, address, and current location / place of residence)
 - Current Care Arrangement/ Living Arrangements: including details of the Parent/Caregiver
 - Disability Status
 - Education
 - Personal vulnerabilities or specific needs: [This includes the status of the child i.e. Unaccompanied Child; Separated child, Child-headed household, Child in foster care, Child Parent, Child Carer, Child Headed Household)

- Status of Child Protection Case Management [i.e. Active Case; Closed Case; Child Protection Assessment also referred to as Best Interests Assessment (BIA) Completed; BID initiated; BID Approved by BID panel]
- Referral Information [Summary of the child protection concerns and reasons for referral]

UNHCR Child Protection focal person(s) may request additional personal data for a child at heightened risk if identified to require long-term protection, solutions and where applicable to support the implementation of the Best Interests Determination (BID) process. Such requests shall be made ensuring compliance with data protection principles of necessity, proportionality and confidentiality, as well as upholding the Do no Harm principle and Best Interests of the Child while minimizing duplication. UNHCR may request the following additional personal data from a Participant:

- Summary of the Child Protection Case at present
 - Completed Child Protection comprehensive assessment also referred to as Best Interests Assessment (BIA) [Noting, in some circumstances, BID is not required, and a Child Protection comprehensive assessment may suffice]
 - Where applicable and available, the Best Interests Determination (BID) Report as part of the established Best Interests Determination Process in Bangladesh, in accordance with the BID panel Terms of Reference and Inter-Agency Case Management SOPs.
- c) Under exceptional circumstances including but not limited to changes in the operational context that would require information of refugee children to be systematically updated, UNHCR may request the routine and systematic sharing of a minimum set of data points, for children receiving Child Protection Services. The purpose of routinely and systematically sharing the requested information with UNHCR will be to ensure that the child's registration information is accurate and up to date, as well as support any services that may need to be delivered for children.

Noting, that routine and systematic does not equate to “automatic” or “bulk” sharing – this refers to having an established and agreed-to process to share the requested information with UNHCR and as agreed upon within CPSS and the CMTWG. The minimum necessary personal data to be shared with UNHCR for this purpose may include:

- Basic Biographical data including Name, date of birth, age (or estimated age), sex, country of origin
- Unique Identifier: UNHCR Individual proGres number [if not available, the Child's full name with the Family Counting Number (FCN)/Master Registration Card (MRC) Number can be provided] or any other UNHCR identifiers
- Contact Details and Address: current contact information and preferred method for contact, address, and current location / place of residence)
- Current Care Arrangement/ Living Arrangements: including details of the Parent/Caregiver
- Disability Status
- Education
- Personal vulnerabilities or specific needs: [This includes the status of the child i.e. Unaccompanied Child; Separated child, Child-headed household, Child in foster care, Child Parent, Child Carer, Child Headed Household)
- Status of Child Protection Case Management [i.e. Active Case; Closed Case; Child Protection Assessment also referred to as Best Interests Assessment (BIA) Completed; BID initiated; BID Approved by BID panel]

The data sharing is performed in accordance with the data protection framework applicable to each Participant. In all instances, personal data requested and shared must observe data protection principles outlined in this agreement including informing the concerned child/caregiver of the purposes

of data sharing and the implications of refusing to share personal data with UNHCR¹⁰, allowing them to object to the data sharing, and ensuring the sharing of information is in the best interests of the child and Do No Harm principle.

Data requested to be provided to UNHCR should only be that data which is necessary for UNHCR to carry out its protection objectives and not exceed the legitimate purpose or compatible purposes in line with UNHCR personal data protection framework.

6.2 Sharing of Personal Data between UNHCR and Participants

- a) The sharing of Personal Data between UNHCR and the Participant shall normally be regulated by a bilateral data sharing agreement between UNHCR and the Participant. Where such agreement does not exist, the below arrangements apply.
- b) UNHCR may share to a Participant as part of a referral for the provision of services (immediately and in the future) as needed based on the best interests of the individual child:
 - Personal Data shared must be limited to only the information necessary for the referral agency to provide that service effectively (from the list of Personal Data points set out in paragraph (b) below).
 - Personal Data will be shared from the UNHCR's designated focal point managing the case to the direct service provider (this may include a focal point within a service provider).
 - The following data may be shared:
 - Basic Biographical data including Name, date of birth, age (or estimated age), sex, country of origin
 - Unique Identifier: UNHCR Individual proGres number [if not available, the Child's full name with the Family Counting Number (FCN)/Master Registration Card (MRC) Number can be provided] or any other UNHCR identifiers
 - Contact Details and Address: current contact information and preferred method for contact, address, and current location / place of residence)
 - Current Care Arrangement/ Living Arrangements: including details of the Parent/Caregiver
 - Disability Status
 - Personal vulnerabilities or specific needs: [This includes the status of the child i.e. Unaccompanied Child; Separated child, Child-headed household, Child in foster care, Child Parent, Child Carer, Child Headed Household)
 - Status of Child Protection Case Management [i.e. Active Case; Closed Case; Child Protection Assessment also referred to as Best Interests Assessment (BIA) Completed; BID initiated; BID Approved by BID panel)
 - Referral Information: [Summary of the child protection concerns and reasons for referral]
 - Where applicable and for the purpose of ensuring the child's physical case file and electronic case management system is complete, the Best Interests Determination (BID) once approved by the Panel may be shared to the relevant Participant by UNHCR, in accordance with the BID panel Terms of Reference and Inter-Agency Case Management SOPs.

- c) The Participant may share with UNHCR:

- Personal Data for the purposes as laid out in 6.1(a) and (b) above

¹⁰ Such as, for example, that UNHCR may not be able to prioritise them for assistance and durable solutions.

- The following Personal Data for the purpose of monitoring and feedback on referrals made by UNHCR to the Participant:
 - Basic Biographical data including Name, date of birth, age (or estimated age), sex, country of origin
 - Unique Identifier: UNHCR Individual proGres number [if not available, the Child's full name with the Family Counting Number (FCN)/Master Registration Card (MRC) Number can be provided] or any other UNHCR identifiers
 - Contact Details and Address: current contact information and preferred method for contact, address, and current location / place of residence)
 - Current Care Arrangement/ Living Arrangements: including details of the Parent/Caregiver
 - Disability Status
 - Education
 - Personal vulnerabilities or specific needs: [This includes the status of the child i.e. Unaccompanied Child; Separated child, Child-headed household, Child in foster care, Child Parent, Child Carer, Child Headed Household)
 - Referral Action Taken: Summary of the referral action taken and any further assistance needed from UNHCR including information required to support children at risk as per UNHCR's mandate, as specified and in accordance with section 6.1.

Please see further detailed data elements and descriptions in Section 3.5.3 of the [2021 UNHCR Best Interests Procedure Guidelines](#) for more information. Please also see the [Inter-Agency Guidance Note on Data Protection and Information Sharing in Humanitarian Settings including Specific Considerations for Settings with Refugees](#).

Annex 1 Information Security

This Information Security Annex forms an integral part of the DPISP to which it is attached. Any capitalized terms not otherwise defined herein shall have the meanings set forth in the Protocol. In all efforts to secure information the physical safety of staff and individuals who are operating on behalf of the Participants in processing information must be considered. Participants are responsible for ensuring protection of critical information systems, including paper-based or other information management tools, that contain confidential information.

Each Participant shall put in place appropriate physical, technical, and organizational data information security measures (for any Personal Data when at rest, in use or in transit) which are appropriate for the risks that may result in the processing and in line with international best practice.

This Information Security Annex sets out best practice in organizational, technical, and physical information security measures which shall be implemented to the furthest extent by participants. These measures are not an exhaustive list and do not relieve the Participant from its obligation to determine appropriate security measures for the type of processing and the risks at stake.

1. Organizational security measures

1.1. Have in place an established security and privacy program that includes but may not be limited to the following:

- a. Procedures ensuring compliance with identified legislative, regulatory, and contractual requirements related to intellectual property rights and protection of personal information.
- b. Background verification policies and procedures of all new employees (including remote employees, contractors, and third parties) established proportional to the type of data to be accessed.
- c. Written job descriptions for employees with access to confidential or sensitive information with processes in place to ensure that access to data is granted solely on a "need-to-know" basis.
- d. Assigned roles and responsibilities of maintaining information security in your organisation clearly defined, documented, and widely communicated to all staff, contractors, and third parties.
- e. Security and privacy trainings for all employees, including temporary and volunteer staff as well as contractors, who will have access to sensitive information covering at minimum the practices mentioned in this annex in addition to protection against phishing, social engineering, ransomware, and other cyber-attacks.
- f. Processes and procedures to discover and respond to information security incidents in a timely manner and include stakeholder notification.
- g. If applicable and organization manages their own systems and applications, the program should include baseline requirements to secure systems and applications

2. Measures relating to data collection / processing through a system.

2.1. Some minimum requirements are:

- a. System requires login for all features that manage sensitive information.
- b. Hosted information is not publicly available and is only accessible by authorized logged in users.
- c. Appropriate authentication and authorization mechanism implemented such as integration with single-sign on mechanisms, automatic session timeout, and/or MFA (multi-factor authentication).
- d. The web application is reachable exclusively over HTTPS. If the user manually edits the URL to start with http://, it will redirect to https://.
- e. System provides reliable services and system maintenance is effectively managed, communicated to users and downtime is limited.
- f. System provides automatic backups or archiving of data to prevent data loss in the event of an incident.
- g. System provides guarantees of permanently removing all associated resources and information as part of decommissioning when engagement / use of system has terminated.

- 2.2. Use only systems for data collection and hosting that offers functionality that assigns a unique case code to all children of whom information is gathered.
 - a. The system should keep an “action log” or “audit log” of all updates made to a case, and should include what was the change, when was the change made, and who made the change.
 - b. The case code should be used to refer to the case verbally, electronically, or on paper instead of referring to personal data as defined in the Protocol.
 - 2.3. Spreadsheet programs such as Excel or Google Docs are not recommended for data collection or data processing. Further information and guidance about the use of these programs can be found on this annex on the “**Out of system activities**” section.
 - 2.4. Social media, chat groups or email should not be used to share case personal identifiable information.
 - 2.5. Apply the following system access procedures:
 - a. Credentials (username and password) are unique and must not be shared between individuals.
 - b. When user self-registration is granted, individuals should follow the minimum requirements ensure that passwords are not similar to their usernames, at least 8 characters in length and do not contain sequential characters (i.e., 123, abc)
 - c. Authorization and authentication should follow the principle of least privilege, which maintains that a user or entity should only have access to the specific data, resources and applications needed to complete a required task.
 - i. Users should be granted access to the system only for the duration of their engagement with the programme, employment contract or role in case management.
 - ii. If user has finished their required tasks or terminated their engagement with the programme, access to the system should be revoked.
 - iii. The authorization to the system to be granted to individuals based on their roles and responsibilities using the principle of least privilege.
 - 2.6. If applicable and organization manages their own systems and applications to host, collect and manage information, the system should meet baseline requirements to secure systems and applications such as [OWASP Proactive controls](#) or [Application Security Verification Standard \(ASVS\)](#), for example.
- 3. Device management:**
- 3.1. Ensure that organization-owned devices (mobile phones, tablets, laptops, and desktop computers) used for any data collection, storing, and/or processing activities are securely managed.
 - a. Devices should have an antivirus and licensed software/applications. Users should not be allowed to install unsanctioned applications.
 - b. Operating system and software installed on devices should be regularly updated.
 - c. Devices should be password protected.
 - d. Devices should not be used for personal activities.
 - 3.2. Deletion of data should be done not only from a mobile device used for data collection, but also from any cloud provider used for data backup (i.e. OneDrive, Google One, Dropbox, iCloud, etc.)
 - 3.3. Participants should provide organization-owned devices and avoid the use of personal devices. If personal devices are being used for this engagement, in addition to the guidelines specified on point 1, the following should also be applied:
 - a. Users should only have the bare minimum level of access to organization’s systems or data.
 - b. If user will not participate in planned activities, all collected, processed data should be handed over and permanently deleted from personal devices.
 - c. Users should be made aware of the risks associated and the importance of protecting the data.
- 4. Paper-based and “Out of System” Activities:**
- 4.1. In addition to the computer itself, all electronic files (e.g., Word, Excel) must be password protected. Passwords should follow the minimum requirements: ensure that passwords are not similar to their usernames, at least 8 characters in length and do not contain sequential characters (i.e., 123, abc)]

- 4.2. Electronic files with personal information should be stored on a Cloud storage service that automatically creates backups of the information and maintain a version control which keeps track of all the changes that have been done to the documents.
 - a. Some popular Cloud storage services are OneDrive, Dropbox, Google Drive, or Citrix.
 - b. The tier selected from these cloud storage services should be private and not make the hosted information publicly available.
 - c. All electronic files with personal information stored on these Cloud storage service must be password protected.
 - d. If other type of files such as photos, emails, etc. need to be stored, these can be saved in a password protected zip file.
 - e. A password management tool is recommended to store/manage passwords and prevent loss of access to the encrypted files.
 - f. Data must be deleted from public cloud storage on the termination or conclusion of activities for which the information was retained or otherwise processed.
- 4.3. Manage hard copy forms and files securely and should consider the following minimum recommendations:
 - a. Each case and all related forms and paperwork should be stored in its own individual file, clearly labelled with the individual case code on the outside of the file.
 - b. Paper files should be stored and labelled according to the allocated case code. It is imperative that the child's name does not appear on the outside of the file.
 - c. Paper files should be kept in a secure place, accessible only to the caseworker(s) and supervisor(s) responsible for the information. This requires a secure lockable filing cabinet, with arrangements for the keys to be kept with the person with responsibility for the information. No one else should be given independent access, unless on a need-to-know basis and permission is provided.
 - d. Paper files should be transferred by hand between only the people responsible for the information (for example when required for use in case conferences and case review meetings). During transit and transfer, the files should be stored in a sealed box or sealed envelope.
 - e. original documents such as ID cards or medical reports. Instead, original documents must either be photographed or scanned and returned to the child/family.

5. Measures to ensure secure transfer of Personal Data:

- 5.1. Comply with data encryption measures while the information is "in transit" – being sent.
 - a. All files that contain sensitive information should be password protected.
 - b. Password used to encrypt the file should not be shared using the same channel. For example, if file is shared using OneDrive and link is shared through email, the password to the file can be shared through Signal, Whatsapp, SMS, etc.
 - i. The password used to encrypt the file should comply with the minimum requirements abovementioned.
- 5.2. Personal data should not be shared in attachments or as embedded text in email. Instead, the organization should limit data transit modalities through tools that allow to create a temporary and limited access. Common Cloud Storage Services with these capabilities are OneDrive, Dropbox, Google Drive, or Citrix. The following steps are recommended:
 - a. Sender protects the electronic file with a password in compliance with the minimum password requirements previously mentioned.
 - b. Sender uploads the electronic file to OneDrive folder (or other Cloud Storage Service).
 - c. Sender creates a shared link of the electronic file and specifies the email address of only the recipient(s) who should have access to the file.
 - d. Sender sends email to only the recipient(s) with the link to the file.
 - e. Sender sends a message through Signal with the password.
 - f. After confirmation that the file has been successfully downloaded and safely stored by the recipient, the access to the shared link should be revoked.
- 5.3. Do not store personal data on external hard drives, USB or "flash drives".

6. Managing Exceptions

Communicate to the Coordination Group the inability to comply with any of these measures due to extenuating circumstances. Exceptions to any of these guidelines must be approved by the Coordination Group and will prioritize:

- a. Physical safety of staff and individuals who are operating on behalf of the Participants.
- b. Protection of critical information systems that contain confidential information.

Annex 2 CP Coordination Group, Coordinators and Consultation Process

Consultation The development of this Protocol is a contextualized and consultative inter-agency process, which has utilized the following methodology:

A task team was established to revise the DPISP in November 2022. The Task Team comprised of UNHCR, IOM, Save the Children, UNICEF, and CODEC. The CMTWG chairs facilitated the revision process which included:

- Sharing of the previous DPISP to all the CMTWG members for review and feedback
- Upon receiving the feedback from the members, the task team held a three-hour workshop to draft the second version, within the newly developed format provided by the global Case Management Task Force.
- The updated draft version was shared with the global CMTF DPISP focal persons for feedback and revised thereafter.
- Feedback has been incorporated and final revisions made in consultation with UNCHR and UNICEF including the global team members.
- A final review meeting was held on 15th March 2026 and shared with the CPSS Strategic Advisory Group (SAG) on 29th March 2026 for approval. The signing ceremony was held on 22nd June 2026.

Annex 3 Form of Adherence/Signature

DPISP for Child Protection in Rohingya Response

This document constitutes the confirmation, by the undersigned organization, to adhere to the Data Protection and Information Sharing Protocol specific to child protection case management programming in Cox's Bazar and Bhasan Char endorsed on 5th April by the Strategic Advisory Group (SAG) of Child Protection Sub Sector (CPSS)

By signing this Adherence Document, the undersigned organization agrees to adhere to the DPISP and understands that it will be bound to comply with any future modification to the DPISP; provided that such modification is made in accordance with the consultation and review procedure set out in the DPISP.

Signatories:

Name: _____ Date: _____

Title:

[Name of Agency/Entity]

Name: _____ Date: _____

Title:

[Name of Agency/Entity]

Name: _____ Date: _____

Title:

[Name of Agency/Entity]

Name: _____ Date: _____

Title:

[Name of Agency/Entity]

Name: _____ Date: _____

Title:

[Name of Agency/Entity]

Name: _____ Date: _____

Title:

[Name of Agency/Entity]

Name: _____ Date: _____

Title:

[Name of Agency/Entity]

Date: _____

Name:

Title:

[Name of Agency/Entity]

Name: Date: _____

Title:

[Name of Agency/Entity]

Name: Date: _____

Title:

[Name of Agency/Entity]

Name: Date: _____

Title:

[Name of Agency/Entity]

Date: _____

Name:

Title:

[Name of Agency/Entity]

Name:

Date: _____

Title:

[Name of Agency/Entity]

Name:

Date: _____

Title:

[Name of Agency/Entity]