Information Commissioner
NORTHERN TERRITORY

Privacy Code of Practice

for the use of data matching technology in the 360VoC Project

Privacy Code of Practice for the use of data matching technology in the 360VoC Project

1. Overview

1.1 This is a privacy code of practice (**Code**) made under Part 5, Division 3 of the *Information Act 2002* (Northern Territory) (NT) (**Information Act**).

1.2 The Information Act sets out information privacy principles (in Schedule 2) (**IPPs**) that apply to "public sector organisations" as defined in the Information Act.

1.3 This Code:

(a) applies to the public sector organisations specified in section 5 of this Code;

(b) applies to the personal information and activities specified in section 6 of this Code;

(c) modifies the application of the IPPs as specified in section 7 of this Code; and

(d) provides for the control of data matching and data linkage for the purpose of producing or verifying personal information for 360 Degree View of the Child (**360VoC**) Project as described in sections 3 and 4.20 to 4.24 of this Code.

1.4 A public sector organisation specified in section 5 of this Code can rely on this Code, if an IPP that applies to it is modified in the circumstances set out in this Code.

1.5 This Code does not affect the operation of any exemption provided under the Information Act. All statutory exemptions remain available to public sector organisations regardless of the provisions of this Code.

1.6 This Code does not provide authority for any activity that constitutes a criminal offence or is otherwise prohibited or unlawful under any legislation other than the Information Act. If you are in doubt as to whether any particular handling of information relating to identity security is permitted, please seek legal advice.

1.7 This Code takes effect on the later of the date the notice of approval is published in the Gazette; or the date specified in that notice.

2. Background to the 360VoC Project

Project objectives

2.1 The Department of Children and Families (**DCF**) is a public sector organisation in the Northern Territory (**NT**) that was established on 10 September 2024 to provide (amongst other things) human services and support programs for child protection, domestic and family violence and foster and kinship care.

2.2 DCF is the successor entity to the Department of Territory Families, Housing and Communities (**TFHC**) which was established on 7 September 2020, and which (in addition to the above) provided youth justice services, housing, and social inclusion services. References to TFHC in legislation or supporting material should be interpreted as references to DCF, following the *Administrative Arrangements Order (No. 3) 2024*, effective from 10 September 2024.

2.3 As part of its functions and responsibilities under the *Care and Protection of Children Act 2007* (NT) (**CPC Act**), DCF provides child protection services which are aimed at preventing, identifying and responding to child harm and exploitation. More specifically, these child protection services include (amongst other things):

(a) handling child protection notifications associated with domestic and family violence, including re-directing notifications to other government agencies and support services, where appropriate;

(b) undertaking investigations into child protection notifications, developing response plans, and assessing levels of risk to determine if out-of-home care is appropriate;

(c) supporting children within DCF's care, to ensure their needs are met and improve their overall outcomes; and

(d) providing early intervention and targeted services to reduce criminal offending and re-offending by young people.

2.4 A key focus of DCF, since its (and TFHC's) establishment, has been improving child protection services in the NT, in line with the key findings and recommendations from the *2016-2017 Royal Commission into the Protection and Detention of Children in the Northern Territory* (**Royal Commission**). In particular, the Royal Commission identified the sharing and reporting of information relating to vulnerable children and youth as a critical and urgent area for improvement, with several recommendations specifically addressed to data and information sharing.

2.5 The current process of information sharing and reporting is a manual one, which is both labour-intensive and time-intensive, and means that DCF caseworkers do not have accurate, complete and up-to-date information about children and youth in vulnerable circumstances. This has limited DCF's ability to effectively and efficiently collect, analyse and use relevant and reliable data, to gain a holistic view of vulnerable children and identify opportunities for early intervention and diversion.

2.6 DCF's 360VoC Project (**Project**) is a major financial investment, with the key objectives being to:

(a) ensure the appropriate legislation, within the parameters of acceptable privacy provisions, policy and governance is in place to enhance information sharing within DCF, and with relevant government agencies (those represented on the Data Governance Sharing Committee) and external service providers to support better outcomes for the child;

(b) ensure business processes enable proactive information sharing to support better outcomes for the child;

(c) inform, educate and increase awareness of NT Government staff and service providers on the parameter in which information can be shared for the purpose of supporting better outcomes for the child; and

(d) develop an organisational culture of proactive information sharing to support better outcomes for the child.

2.7 The aim of the Project is to design and build a new, secure, technology-driven solution, called the **360VoC Solution**, that will replace the existing manual, labour and time intensive process of inter-agency data sharing. The 360VoC Solution will facilitate automated inter-agency data sharing with DCF, by the Data Providers, to achieve the following objectives:

(a) to enable an individual in a Data Provider's operating system (**Agency Database**) to be matched to:

(i) a child:

(A) for whom information has been received which raises a concern about the child's safety and wellbeing; and

(B) whom the CEO believes on reasonable grounds might be in need of protection,

(together, a **Child of Attention**);

(ii) a child:

(A) in the CEO's care, whether under a temporary placement arrangement or provisional protection; or

(B) under the daily care and control of the CEO under an order of the Court (for example, a protection order) or another law of the NT,

(each, a **Child in Care**); or

(iii) a person who is, in respect of a Child:

(A) a sibling, a parent or a current or prospective legal guardian or carer;

(B) other family members of the Child (including as understood under the Aboriginal kinship system) identified as relevant to the safety and wellbeing of the Child;

(C) a household member at any premises where that Child habitually resides; or

(D) a Person Believed Responsible,

(each, a **Close Connection**);

(b) to enable automated notifications to be given to DCF when specific forms of data are uploaded into the Agency Database, about incidents or events involving a Child or their Close Connection; and

(c) to establish a single data repository for information about the safety, health and wellbeing of a Child (**360VoC Data Hub**).

2.8 A new contemporary case management system, known as CARE, has been developed which enables DCF to manage Child Protection and Adoptions in a central system, owned and managed by DCF (**CARE**). DCF replaces TFHC's former case management tool, CCIS, which is an ageing, legacy system no longer supported by the vendor.

2.9 The Project is being delivered through a partnership between DCF, as the frontline agency responsible for child protection services, and the Department of Corporate and Digital Development (**DCDD**), as the lead NT Government agency for digital technology.

Legislative basis for Project

2.10 Authorisation for the sharing of data between NT public sector organisations to enable the Project is anchored in legislation, and subordinate documentation that has been developed pursuant to the legislative frameworks provided by the Information Act and CPC Act.

2.11 The CPC Act provides the legislative basis to share information between NT Government agencies for the care and protection of Children. The CPC Act was amended by the *Territory Families Legislation Amendment Bill 2021*, to (amongst other objectives):

(a) improve government coordination and information sharing for child safety and wellbeing purposes; and

(b) introduce a new Child Safety Data Access and Exchange Scheme to enable child protection practitioners to access relevant child safety information and make timely and informed decisions.

2.12 Specifically, new Part 5.1 was inserted into the CPC Act, which enables the CEO of DCF to enter into data access agreements with other NT agencies, to facilitate timely access to information to ensure the safety and wellbeing of Children (**Data Access Agreements**). These amendments to the CPC Act were tabled in NT Parliamentary Sittings in 2022 and were passed with the full support of Members.

2.13 Comprehensive Data Access Agreements were developed between DCF, DCDD and the Data Providers covered by this Code, in consultation with the NT Information Commissioner (**Information Commissioner**).The Data Access Agreements for the public sector organisations identified in sections 5.1(c)(i) to (iv) of this Code were finalised and executed on 29 July 2024. Data Access Agreements for public sector organisations established under *Administrative Arrangements Order (No. 3) 2024* will be entered into on the same terms as the existing Data Access Agreements. These are expected to be finalised late 2024. These documents will be published and reviewed periodically to ensure that they maintain their currency and reflect best practice.

2.14 The Data Access Agreements prescribe the specific data sets and alerts about Children of Attention, Children in Care and Close Connections, that will be shared between the Data Providers and DCF within the 360VoC Solution (defined as **Schedule 1 Data** in the Data Access Agreements).

Purpose of this Code

2.15 As described in sections 2.10 to 2.13 above, the Data Providers will be permitted to share Schedule 1 Data about Children of Attention, Children in Care and Close Connections, with DCF, in accordance with the CPC Act and relevant Data Access Agreements. The Schedule 1 Data is not the subject matter of this Code, nor does the Code independently authorise the sharing of Schedule 1 Data in the 360VoC Solution, before the Data Access Agreements are operational.

2.16 This Code addresses the sharing of the data sets specified in 6.1, in the MDM environment, to match the identity of individuals within DCF's source system, with individuals in the Data Providers' source systems, through algorithmic programming.

2.17 This data matching process is a critical aspect of the Project, as it ensures that DCF collects only Schedule 1 Data, as will be permitted under the Data Access Agreements once operational – and not data about broader NT residents. It will also improve the uniformity, accuracy and data quality of the information shared with DCF by the Data Providers.

3. Overview of Project software and MDM technology

3.1 To ensure that the Schedule 1 Data shared within the 360VoC Solution only relates to NT residents who are a Child of Attention, Child in Care or Close Connection (and no other NT residents), and to improve data quality, uniformity and accuracy, MDM technology will be used to analyse and compare the basic identity information of individuals in the Agency Database (**Agency Identity Data**), against the basic identity information of individuals recorded in DCF's system (**CARE Identity Data**), to identify:

(a) Agency Identity Data that has a confirmed match with CARE Identity Data (which in other words, are either a Child of Attention, Child in Care or Close Connection); and

(b) Agency Identity Data that has no confirmed match with CARE Identity Data (which in other words, is the data of any other NT resident that is not a Child of Attention, Child in Care or Close Connection).

3.2 The MDM is a 'back end' technology that undertakes these automated functions using business logic and algorithms to perform the matching process. Importantly, it is separate software from both the 360VoC Solution or CARE System, and it is not a system where either the Data Providers or DCF can collect, access or use one another's data. Only appropriately authorised technical specialists will have access to the MDM environment, for restricted purposes (as set out in the Data Access Agreements).

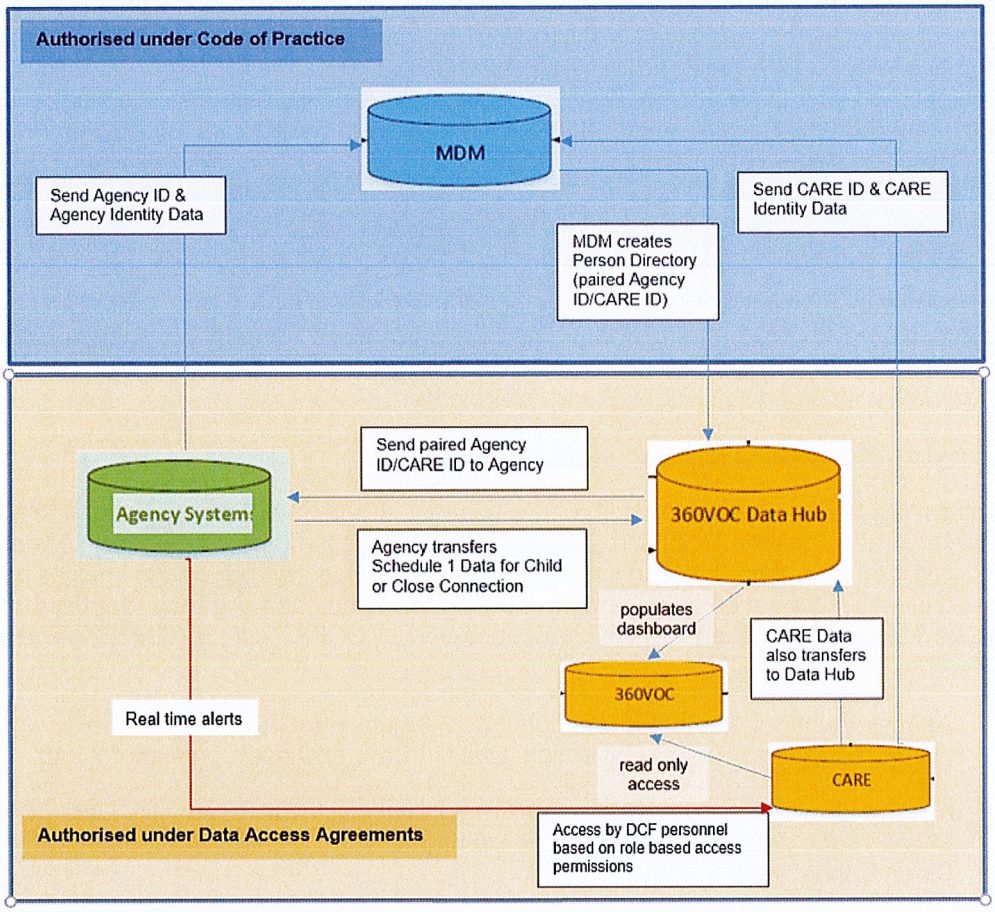
3.3 The matching process will effectively produce a directory of mutual customers identified between a specific Data Provider's Agency Database and DCF's CARE System (**Person Directory**). The Person Directory for a Data Provider will comprise only the unique identifier assigned to the individual by the Data Provider (**Agency ID**) and the paired unique identifier assigned to the individual by DCF (**CARE ID**), and no other personal information.

3.4 The Person Directory for a Data Provider will enable Schedule 1 Data to be shared directly from that Data Provider's Agency Database to the DCF's 360VoC Data Hub. The transferred data will then be accessible to authorised users within DCF via CARE, based on role-based access permissions. Transferred data is only accessible by authorised users within DCF and DCDD, as specified in the Data Access Agreements.

3.5 The MDM technology will be operated and maintained by DCDD, which is the digital services provider for the NT Government and currently manages each of the Data Providers' and DCF's business applications, data warehouses and operating systems.

4. Information flows

4.1 The information flows through the MDM technology, and controls on the data matching and data linkage process, are set out in the following diagram and described in detail below.



Agency Database

4.2 Each Data Provider has its own operational system, that it uses to hold personal information and data about individuals to whom it provides services, defined below as the **Agency Database**. The Agency Identity Data is held in the Agency Database.

4.3 Each Data Provider collects personal information from individuals (including the Agency Identity Data) for the primary purpose of the performance of their own functions or activities, including to provide relevant, timely and essential services to the NT public (each in the field of the relevant Data Provider).

4.4 Like the other Data Providers, DCF has its own source system, that it uses to hold personal information and data about individuals to whom it provides services (**CARE System**).

4.5 The CARE Identity Data is collected by DCF for the purpose of providing child protection services to Children of Attention and Children in Care in the NT.

4.6 The Agency Database and CARE Systems are all NT government ICT systems that are managed and supported by DCDD, as the central NT Government ICT agency.

Enterprise software with MDM functionality

4.7 The NT Government currently holds an enterprise licence for software with MDM functionality (**Software**). Permissions for access will be managed within the Software by DCDD (on instructions from each Data Provider and DCF).

4.8 Each Data Provider, and DCF, will each have their own secure dataspace.

4.9 Each Data Provider will use an Application Programming Interface (**API**) to transfer the Agency Identity Data from their Agency Database into that Data Provider's individual dataspace within the Software. As such, each Data Provider will remain the owner of its data and will control what data is in their own dataspace (including to exclude any data that cannot be shared under Secrecy Laws or can otherwise be excluded pursuant to Part 5.1 of the CPC Act).

4.10 Each Data Provider will also be able to control what is done to its Agency Identity Data the whole time it is hosted in the Software, including to remove it from the Software. Specifically:

(a) all data in the Software will be view only;

(b) the Agency Database remains the single source of truth for the data; and

(c) as such, any changes to the data can only be done through the Agency Database.

For example, if an Agency (as data owner) noticed the address is incorrect for an individual, the update would need to be made in the Agency Database, which would then programmatically be updated in the Software.

4.11 There is no comingling of the Agency Identity Data belonging to each of the Data Providers.

4.12 DCF will also use an API to transfer its CARE Identity Data from the CARE System to the Software and have the ability to filter/exclude data as necessary to comply with secrecy laws.

4.13 DCDD will have access to these discrete agency data repositories within the Software, as a service provider. DCDD will manage the environment from a technical perspective and will have responsibility for the security of the Agency Identity Data and CARE Identity Data held in the discrete agency data repositories. DCDD cannot edit any of a Data Provider's underlying data – data can only be changed within the Agency Database.

Data matching

4.14 Within the Software, the data matching function will be applied to a Data Provider's Agency Identity Data and DCF's CARE Identity Data on a one-to-one basis. This will identify:

(a) Agency Identity Data that has a confirmed match with CARE Identity Data (which in other words, is the data of a Child of Attention, a Child in Care or a Close Connection); and

(b) Agency Identity Data that has no confirmed match with CARE Identity Data (which in other words, is the data of any other NT resident that is not a Child of Attention, Child in Care or Close Connection).

4.15 There will be occasions where there is a partial/unconfirmed match, where the relevant Agency Identity Data and/or CARE Identity Data will need to be reviewed by the Data Provider and/or DCF authorised personnel, to manually verify whether the individual is or is not a match (in a manner that mirrors the existing manual processes).

Person Directories

4.16 Where a match is confirmed between the Agency Identity Data and the CARE Identity Data:

(a) the Software will create a file or database view of the matched data (i.e. creates a "Matched Group");

(b) each match gets a Group ID; and

(c) the Software will then transfer the matched IDs only to the 360VoC Solution (i.e. Agency ID and CARE ID as a matched pair).

4.17 Each Data Provider's dataspace will have its own Person Directory – i.e. one per Data Provider, where the CARE ID and Agency ID is matched.

4.18 There is no co-mingling or cross matching between a CARE ID and multiple Agency IDs.

4.19 The Person Directory for each Data Provider will trigger the sharing of data relating to a matched individual (Child of Attention/Child in Care/Close Connection) pursuant to the Data Access Agreement, as follows:

(a) the matched IDs will be transferred from the Software to the 360VoC Solution; and

(b) the matched IDs will be used to trigger the transfer of Schedule 1 Data from the Agency Database to the 360VoC Data Hub (being the data prescribed under the Data Access Agreement).

Controls on the data matching and data linkage process

4.20 As described above, to mitigate the risks associated with data matching/linkage to the greatest extent possible, the Software has been designed to ensure that there is no co-mingling of Agency Identity Data or Agency IDs, at any point within the process.

4.21 Specifically:

(a) each Data Provider has its own discrete database to transfer and standardise its Agency Identity Data;

(b) each Data Provider has its own discrete database to perform the matching function against the CARE Identity Data on a one to one basis;

(c) each Data Provider will retain control over its own Agency Identity Data within the Software (by determining the role-based access permissions which DCDD will implement);

(d) each Data Provider can only view its own Agency Identity Data (except in limited circumstances, where authorised personnel from that Data Provider can review CARE Identity Data, for the purpose of manually verifying an unconfirmed/partial match of an individual);

(e) DCF can only view its own CARE Identity Data (except in limited circumstances, where authorised DCF personnel can review Agency Identity Data, for the purpose of verifying an unconfirmed/partial match of an individual); and

(f) each of the Person Directories established from the matching process, will hold the paired CARE ID and Agency ID for a matched individual; It will not involve any co-mingling of Agency IDs, nor contain any broader Agency Identity Data or CARE Identity Data about the matched individual.

4.22 Additionally, the Software will only be accessible to a limited number of personnel from the Data Providers, DCDD and DCF, and will be subject to further specific access controls/roles and auditing functions.

4.23 The Software provides security controls, auditing and traceability to the matching process (and ensures that non-matched individuals' personal information is not disclosed to DCF personnel or transferred into CARE).

4.24 At all times, each Data Provider will remain the owner of the Agency Identity Data (and DCF the owner of the CARE Identity Data) and changes to this data can only be made by that agency itself, through its Agency Database. At all other stages of the process, the Agency Identity Data will be view-only – meaning the Agency Database from which the data originates, remains the single source of truth.

4.25 DCF and DCDD will take all reasonable steps to:

(a) ensure that the automated transfer of personal information about an individual from a Data Provider's Agency Database to the 360VoC Data Hub ceases as soon as that individual ceases to be a Child of Attention, Child in Care or Close Connection;

(b) without limiting (a), ensure that the Person Directories are regularly updated, so that the Agency ID and CARE ID of an individual who is no longer a Child of Attention, Child in Care or Close Connection is unpaired and/or removed;

(c) conduct regular reviews of the data held in the MDM environment (at least annually) to ensure that no unnecessary information is being transferred by or retained in the MDM; and

(d) certify in writing, by a senior officer of DCDD, that a review has been conducted and of the outcome of the review.

5. Public sector organisations covered by the Code

5.1 This Code applies to the following public sector organisations:

(a) Department of Children and Families (**DCF**);

(b) Department of Corporate and Digital Development (**DCDD**); and

(c) the following public sector organisations, together and where applicable individually, **Data Providers**:

(i) Department of Health

(ii) Department of Education and Training

(iii) Attorney-General's Department

(iv) NT Police

(v) Department of Housing, Local Government and Community Development

(vi) Department of Corrections

6. Information covered by the Code

6.1 This Code applies to the following information:

(a) full name;

(b) aliases;

(c) date of birth (actual, or approximate if not known);

(d) gender (identified), sex (biological)

(e) residential address;

(f) Agency ID and other government identifiers assigned to individuals by a Data Provider;

(g) date of death (actual, or approximate if not known).

6.2 The intention of this Code is to permit the collection, use and disclosure of such information for the following purposes:

(a) to accurately identify a Child of Attention, Child in Care or Close Connection on a Data Provider's Agency Database;

(b) to match and pair the Agency ID and the CARE ID for that individual, through the use of MDM technology and manual verification (where required);

(c) to create a Person Directory for each Data Provider, of paired CARE IDs and Agency IDs; and

(d) to facilitate the transfer of personal information about that individual from a Data Provider to DCF for child safety and wellbeing purposes, in strict compliance with the Data Access Agreements and Part 5.1 of the CPC Act; and

(e) to continue to test, refine and improve the data matching capability within the MDM environment over time.

7. Modification of IPPs

7.1 The application of the IPPs set out in Schedule 2 to the Information Act to the public sector organisations identified in section 5, is modified as follows:

7.2 IPP 1 is modified as follows:

(a) The collection of personal information by DCF for child safety and wellbeing purposes is a lawful purpose that is related to DCF's functions and activities. DCF will only collect the personal information of a Child of Attention, a Child in Care or a Close Connections, which can be lawfully collected under the Data Access Agreements and Part 5.1 of the CPC Act .

(b) The primary purpose of collection of personal information by the Data Providers remains unchanged, and where such collection is necessary for one of its own functions and activities it is lawful. The Data Providers will not collect any new or additional personal information for the purposes of the Project.

(c) The Data Providers are not required to notify individuals, that their personal information will be used and disclosed by the Data Provider, for the purposes covered by this Code.

(d) To the extent that the following activities constitute collection of personal information under IPP 1, DCDD is authorised to collect CARE Identity Data and Agency Identity Data for the following purposes:

(i) to match and pair the Agency ID and the CARE ID for that individual, through the use of MDM technology and manual verification (where required);

(ii) to create a Person Directory for each Data Provider, of paired CARE IDs and Agency IDs; and

(iii) to manage and oversee the transfer of personal information about that individual from the Data Providers to DCF for child welfare and safety purposes, in strict compliance with the Data Access Agreements and Part 5.1 of the CPC Act;

(iv) managing, refining and improving the ongoing data matching and data linkage processes;

(v) otherwise monitoring, operating and managing the MDM technology, including by:

(A) providing technical support and carrying out maintenance, updates, new releases and improvements as reasonably required from time to time.

(B) establishing, maintaining and modifying the permissions/roles/access controls, in accordance with the Data Providers' and/or DCF's instructions;

(C) establishing, maintaining and modifying the matching rules used in the MDM, in accordance with the Data Providers' and/or DCF's instructions;

(D) resolving unconfirmed/partial matches, in accordance with the Data Providers' and/or DCF's instructions.

(e) DCDD is not required to notify individuals, that their Agency Identity Data or CARE Identity Data will be used and disclosed by DCDD for the purposes covered by this Code.

7.3 IPP 2 is modified as follows:

(a) DCF can use, and disclose to each Data Provider and DCDD, CARE Identity Data without an individual's consent, where reasonably necessary for one of the purposes specified in paragraph 6.2.

(b) Each Data Provider is authorised to use, and disclose to DCF and DCDD, Agency Identity Data without an individual's consent, where reasonably necessary for one of the purposes specified in paragraph 6.2.

(c) DCDD is authorised to use and disclose CARE Identity Data and Agency Identity Data, without an individual's consent, where reasonably necessary for one of the purposes specified in paragraph 7.2(d).

7.4 IPP 7 is modified as follows:

(a) DCF is authorised to disclose CARE IDs to each Data Provider and DCDD, and each Data Provider and DCDD are authorised to use CARE IDs, where reasonably necessary for one of the purposes specified in paragraph 6.2.

(a) Each Data Provider is authorised to disclose Agency IDs to DCF and DCDD, and DCF and DCDD are authorised to use Agency IDs, where reasonably necessary for one of the purposes specified in paragraph 6.2.

(b) DCDD is authorised to use and disclose Agency IDs and CARE IDs without an individual's consent, where reasonably necessary for one of the purposes specified in paragraph 7.2(d).

7.5 IPP 10 is modified as follows:

(a) This section applies to the extent that Agency Identity Data disclosed by a Data Provider is deemed to be 'sensitive information' within the meaning of section 4 of the Information Act. Specifically:

(i) the Agency Identity Data does not include any types of personal information that would typically be considered sensitive in nature; however

(ii) the Agency Identity Data held by some Data Providers could be 'sensitive information' due to the nature of their interactions with individuals, for instance the Department of Health (which may be considered to comprise "personal information connected with the provision of a health service") or the Attorney-General's Department (where Agency Identity Data may disclose information about the existence of a criminal record).

(b) The Data Providers are authorised to disclose Agency Identity Data to DCF, without an individual's consent, where reasonably necessary for one of the purposes specified in paragraph 6.2.

(c) DCF is authorised to collect Agency Identity Data directly from the Data Providers, without an individual's consent, where reasonably necessary for one of the purposes specified in paragraph 6.2.

(c) DCDD is authorised to collect Agency Identity Data directly from the Data Providers, without an individual's consent, where reasonably necessary for one of the purposes specified in paragraph 7.2(d).

8. Publication of information, breaches and complaints

8.1 DCF will make available on its website:

(a) a copy of the approved Code;

(b) information about the Project;

(c) information about how to make an enquiry or complaint about a breach or possible breach of this Code or the IPPs in relation to the aspects of the Project covered by this Code; and

(d) contact details for making an enquiry or complaint.

8.2 A public sector organisation identified in section 5 that becomes aware of a breach or possible breach of this Code or the IPPs in relation to the aspects of the Project covered by this Code, or a complaint of that nature, will notify each other public sector organisation to which this Code applies.

8.3 The public sector organisations identified in section 5 will co-operate to appropriately address any notified breach or complaint.

9. Duration and Review

9.1 The Code will continue for five (5) years from the commencement date of the first Data Access Agreement but may be:

(a) extended by the Commissioner (under section 77 of the Information Act); or

(b) terminated by the Commissioner by giving at least three months' written notice to DCF,

subject to the outcome of the review required in clause 9.2.

9.2 DCDD and DCF will review the operation of this Code and will report to the Information Commissioner on the outcome of that review, within three (3) years from the commencement date of the first Data Access Agreement.

9.3 The report to the Information Commissioner will include:

(a) information about action taken under the Code; and

(b) information about the steps that the parties to this Code have taken to ensure compliance with the Code.

10. Interpretation/Glossary

10.1 In this Code:

360VoC Application means the data application which will display Transferred Data sourced from the 360VoC Data Hub, in a read only format, via link in CARE.

360VoC Data Hub means the data hub within the 360VoC Solution, created and managed by DCDD that receives and stores Transferred Data about a Child or Close Connection, and includes any updated, modified or replacement version of that data hub that may be adopted by the Data Recipient from time to time, provided that version continues to meet the requirements of the Information Act and this Agreement.

360VoC Solution means the overall software system used to facilitate the sharing of data between the Data Provider and Data Recipient under this Agreement, which includes the 360VoC Data Hub and 360VoC Application but does not include the MDM.

Agency has the meaning given in the *Interpretation Act 1978*.

Agency Identity Data means the types of personal information specified in section 6.1, as contained in an Agency Database.

Agency ID means the unique identifier assigned to an individual by a Data Provider, as specified in section 3.3.

Agency Database means the Data Providers' agency based software database that contains (amongst other things) the Agency ID Data and Schedule 1 Data.

API means an Application Programming Interface, being a set of programming codes enabling data to be transferred between systems.

CARE Identity Data means the types of personal information described in section 6.1, as contained in the CARE system.

CARE ID means the unique identifier associated with an individual, as specified in section 3.3.

CARE means the existing database software system used by DCF.

CCIS means the Community Care Information System previously used by DCF.

Child (or Children) means a person under the age of 18 years (or where a child's age cannot be proven, DCF reasonably believes the child to be under 18 years), who is a Child in Care or Child of Attention.

Child of Attention has the meaning given in section 2.7(a)(i).

Child in Care has the meaning given in section 2.7(a)(ii).

Close Connection has the meaning given in section 2.7(a)(iii).

Code means this privacy code of practice.

CPC Act means the *Care and Protection of Children Act 2007* (NT).

Data Access Agreements means the agreements to be entered into between DCF and each Data Provider, in accordance with the CPC Act, as described in section 2.12.

Data Providers has the meaning given in section 5.1(c).

DCDD means the Department of Corporate and Digital Development.

DCF means the Department of Children and Families, formerly known as the Department of Territory Families, Housing and Communities.

Information Act means the *Information Act 2002* (NT).

IPP means the information privacy principles as set out in Schedule 2 of the Information Act.

MDM means master data management technology which will apply predefined matching rules to identify a match between a Child or Close Connection in the 360VoC Solution and an individual on the Agency's Database, and link the Schedule 1 Data.

Person Believed Responsible means, where an allegation of harm towards a Child has been investigated and harm, or the risk of harm, to the Child has been substantiated by DCF in accordance with the CPC Act, the person believed responsible for causing the harm and/or the risk of harm to the Child (whether by an act or omission).

Person Directory means the directory of mutual customers identified from the Data Providers' Agency Database and DCF's CARE System, as further described in section 3.3.

Project means the 360VoC Project, as described in section 2.6.

Royal Commission means the *2016-2017 Royal Commission into the Protection and Detention of Children in the Northern Territory*.

Schedule 1 Data means the types of data permitted to be shared under the Data Access Agreements and CPC Act, as further described in section 2.14.

Secrecy Laws means:

(a) a secrecy or confidentiality provision in any applicable law which prohibits or precludes disclosure of certain information; or

(b) a confidentiality, suppression or secrecy order issued by a court, tribunal or commission.

Software means the software with MDM functionality for which the NT Government holds an enterprise licence.