Master Data Management and Code of Practice Fact Sheet

Background

Having the right information at the right time helps us make good decisions about children and their families.

We're reforming our child protection case management systems to achieve better outcomes for children, families and communities.

These reforms will automate access to information about children we know may be at risk of harm and their Close Connections - information that is currently available to us through manual processes. These changes will improve responses and streamline the process for sharing information we currently obtain during child protection inquiries and investigations.

These changes will improve responses and streamline the process for sharing information the Department of Children and Families (DCF) can already obtain during child protection inquiries and investigations.

Child safety is everyone's business, and a strong whole-of-government approach to information sharing and collaboration will help ensure the safety of children.

We're proactively working to create safer, stronger communities with the highest priority of keeping children safe while ensuring connection to family, identity and culture.

These reforms recognise that when DCF is entrusted with the parental responsibility, or daily care and control of a child, we need access to the same information that any parent has, to make decisions about their wellbeing.

Master Data Management (MDM) system

The MDM system will be used to facilitate interagency data sharing from the following Participating Agencies:

- Department of Health
- Department of Education and Training
- Attorney-General's Department
- Northern Territory (NT) Police Force
- Department of Housing, Local Government and Community Development
- Department of Corrections.

The MDM will be used for data matching purposes to ensure that the Participating Agencies can only share data with DCF that relates to a child in care or at the attention of DCF, and their identified Close Connections – and not broader members of the public.

Master Data Management and Code of Practice Fact Sheet

A Close Connection is a person who is linked or related to a child in care, or at the attention of DCF, because they are:

- a sibling, a parent or a current or prospective legal guardian or carer
- another family member of the child (including as understood under the Aboriginal kinship system) identified as relevant to the safety and wellbeing of the child
- a household member at any premises where the child normally resides, or
- the person believed to be responsible for harm to the child.

Using basic identity data, MDM technology will verify and match the identity of individuals between a Participating Agency's source system and DCF's case management system (CARE) to create a mutual customer register called a Person Directory.

Basic identity data is limited to a person's name (including aliases), date of birth, date of death, gender, sex at birth, address, relationships and system identifiers assigned by the Participating Agency (e.g. student numbers, health record numbers).

There will be no direct sharing of identity data or other personal information between Participating Agencies. Each Participating Agency's identity data will be directly matched against CARE identity data.

The data matching will trigger the sharing of agreed data from Participating Agencies to DCF, in compliance with the Data Access Agreements. If the MDM cannot make a verified data match, information will not be transferred to 360 Degree View of a Child (360VoC).

Use of the MDM will remove the need for Participating Agencies to manually match individuals in its source system, against individuals in DCF's CARE system. To do this manually is an extremely labour, time and resource intensive process and risks causing errors or delays that could impede a child's safety.

The MDM will be operated and maintained by the Department of Corporate and Digital Development (DCDD), the digital services provider for the NT Government that currently manages each of the Participating Agencies' and DCF's business applications, data warehouses and operating systems.

The data stored in the MDM will not be used for any purpose other than identity matching, and access to the data for other purposes is prohibited. To ensure the MDM is used solely for its intended purpose, its use will be governed by a Code of Practice.

Master Data Management and Code of Practice Fact Sheet

Code of Practice

Use of the MDM technology is governed by a Code of Practice between DCF, DCDD and other Participating Agencies, approved by the Information Commissioner.

This Code of Practice outlines what specific types of data DCF and the Participating Agencies can collect, use and disclose, for data matching purposes associated with the MDM and 360VoC Project, and the extent to, and manner in which, any Information Privacy Principles are applicable to the 360VoC Project.

The Code of Practice took effect on 15 November 2024, the date the notice of approval was published in the NT Government Gazette, and will continue for an initial period of five (5) years. Overall compliance with the Code of Practice, and all reviews or amendments of the Code of Practice, will be overseen by the Office of the Information Commissioner and published on their website.

View approved Code of Practice here.

Legislation

A Code of Practice may be drafted under Part 5, Division 3 of the *Information Act 2002* (NT), where public sector organisations seek to modify specific aspects of the Information Privacy Principles. A Code of Practice can only be implemented with the approval of the Information Commissioner.

DCF, DCDD and the Participating Agencies will be bound by the terms of this Code of Practice.

Security

The MDM is a 'back end' technology, and its data will only be accessible to a limited number of personnel from DCDD and DCF, as well as a restricted number of Data Stewards from each Participating Agency that will have access to the extent that manual identity matching may need to occur. It will be subject to further specific access controls/roles and auditing functions.

As with all NT Government ICT systems, those providing technical support (DCDD) will have access to the database in which the data will be stored. Those individuals are subject to extra security clearances.

Data will be securely transferred to, and stored in, the MDM software. The MDM software will provide security controls, auditing and traceability to the data matching process.

Timing

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.