

Data Access Agreement

Agreement Under Part 5.1 of the *Care and Protection of Children Act 2007*

Department of Territory Families, Housing and
Communities (**Data Recipient**)

Department of Education (**Data Provider**)

Department of Corporate and Digital Development
(**Digital Services Manager**)

Data Access Agreement

Agreement Under Part 5.1 of the *Care and Protection of Children Act 2007*

Details	4
Parties	4
Background	4
Part 1 – Definitions	5
1. Defined terms & interpretation	5
1.1 Defined terms	5
Part 2 – Purpose of Agreement	7
2. Object and underlying principle	7
3. Sharing of information	7
4. Role of the Digital Services Manager	8
5. Sharing of Schedule 1 Data	9
5.1 Transferred Data	9
5.2 CARE Data	9
5.3 Responsibility for Transferred Data	9
Part 3 – Specific requirements of the Act	10
6. Section 227 of the Act	10
6.1 Requirements of section 227	10
6.2 Detailed description of the data (s.227(i)(a))	10
6.3 How the Transferred Data will be accessed, used, interpreted, linked and secured (s.227(1)(b))	10
6.4 Categories of users and access conditions (s.227(1)(c))	12
6.5 Restrictions on access, use and interpretation of the Transferred Data (s.227(1)(d))	13
6.6 Data Provider no longer owns the Schedule 1 Data (s.227(1)(e))	13
6.7 What happens if a party breaches the Agreement (s.227(1)(f))	13
6.8 The period for which the Agreement is in force (s.227(1)(g))	14
6.9 How the Agreement may be terminated (s.227(1)(h))	14
6.10 Review of Agreement (s.227(3))	14
Part 4 – Ancillary provisions	14
7. Education and training	14
8. Governance, transparency and oversight	15
8.2 Freedom of Information requests	15
9. Changes to Schedule 1 Data	15
9.1 Expanded or new information	15
9.2 Variation	15
9.3 Rejection of request	15
9.4 Variation	16
10. Change to Authorised Users and CARE Data Users	16
10.1 Removal or creation of Authorised Users and CARE Data Users	16

10.2	Variation	16
10.3	Rejection of request	16
10.4	Variation	16
11.	What happens if there is a Data Breach	16
12.	Privacy complaints procedure	18
13.	Dispute resolution	18
14.	Notices	18
15.	General provisions	19
15.1	Variation	19
15.2	Information-sharing obligations outside of this Agreement	19
	Schedule 1 – Description of the Schedule 1 Data	20
	Schedule 2 – Authorised Users, CARE Data Users, DSM Users and Permitted Purposes	26
	Signing page	28

Details

Date

Parties

Name	Department of Territory Families, Housing and Communities
Short form name	Data Recipient

Name	Department of Education
Short form name	Data Provider

Name	Department of Corporate and Digital Development
Short form name	Digital Services Manager

Background

- A. The Data Recipient is the Agency that administers the Act. In 2021, the Act was amended to improve Northern Territory Government coordination and information sharing for child safety and wellbeing purposes by introducing a new statutory framework to remove barriers that impeded the sharing of government data between government agencies.
- B. The statutory framework enables the CEO of the Data Recipient to enter into data access agreements with CEOs of other Agencies.
- C. The Digital Services Manager manages the Northern Territory Government's digital environment and supports all Northern Territory Government agencies' software systems through the delivery of digital services including core ICT infrastructure and support services and data centre services.
- D. The Agency Database is an Agency business system that is supported by the Digital Services Manager.
- E. The Data Provider agrees to share the Schedule 1 Data with the Data Recipient, and the Data Recipient agrees to use and access the Schedule 1 Data for the Permitted Purpose, on the terms of this agreement.
- F. The Data Provider and the Data Recipient each agree to the Digital Services Manager facilitating the transfer of Schedule 1 Data from the Agency Database to the 360VoC Data Hub and CARE on the terms of this agreement.

Part 1 – Definitions

1. Defined terms & interpretation

1.1 Defined terms

In this Agreement:

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 the Digital Services Manager 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 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.

Act means the *Care and Protection of Children Act 2007*.

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

Agency Database means the Data Provider's agency based software database that contains the Schedule 1 Data.

Agreement means this data access agreement and includes all schedules and attachments (if any) to this Agreement.

Authorised Officer means any individual who is an 'authorised officer' as defined in the Act.

Authorised User means:

- (a) an Authorised Officer; or
- (b) at any time, any individual who is employed by the Data Recipient or the Digital Services Manager under the *Public Sector Employment and Management Act 1993*; or
- (c) a contractor engaged by the Digital Services Manager, under a service contract with the Digital Services Manager, to provide services relating to the development and operation of the MDM and 360VoC Solution,

and who in each case, meets the requirements of this Agreement and holds a position specified in Schedule 2 as amended from time to time in accordance with clause 10.

Business Day means a weekday other than a public holiday in the Northern Territory.

CARE means the existing database software system used by the Data Recipient.

CARE Data means the Schedule 1 Data described in Schedule 1 as Data that may be transferred by the Digital Services Manager from the Agency Database directly into CARE.

CARE Data User means, at any time, any individual employed under the *Public Sector Employment and Management Act 1993* by the Data Recipient who has been approved by the CEO of the Data Recipient to access the CARE Data for the Permitted Purpose.

CEO of a party means the Chief Executive Officer of that party.

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

Child in Care has the meaning in Schedule 1.

Child of Attention has the meaning in Schedule 1.

Close Connection means a linked or related person to a Child that is:

- (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 the Child habitually resides; or
- (d) a Person Believed Responsible.

Commencement Date means the date on which this Agreement takes effect pursuant to section 229(2) of the Act.

Committee means the Children and Families Standing Committee, comprising of representatives of various agencies, the objective of which is aimed at improving outcomes for children and families across the Northern Territory or any replacement or successor committee from time to time.

Data has the meaning given to it in section 225(1) of the Act.

Data Provider means:

- (a) the Agency described as the 'Data Provider' on page 4 of this Agreement that provides Data to the Data Recipient under this Agreement for the purpose of the Act; and
- (b) any other Agency that is, from time to time after the Commencement Date, responsible for an area or activity of government that was previously the Data Provider's responsibility and now has possession or custody of the Schedule 1 Data and is subject to a data access agreement under Part 5.1 of the Act.

Data Recipient means:

- (a) the Agency described as the 'Data Recipient' on page 4 of this Agreement that receives the Data from the Data Provider under this Agreement for the purpose of the Act; and
- (b) any other Agency that is, from time to time after the Commencement Date, responsible for administering the Act.

Data Steward means, for the purposes of clause 6.3(e):

- (a) in relation to the Digital Services Manager, an individual employed or contracted by the Digital Services Manager who holds, or acts in, the position described in item 4 of Schedule 2; and
- (b) in relation to the Data Recipient or the Data Provider, an individual employed by the Data Recipient or the Data Provider (as applicable) who has been approved by the CEO of the Data Recipient or the CEO of the Data Provider (as applicable) to access the MDM for the purpose of manual verification of an unconfirmed/partial match of an individual, as requested by the Digital Services Manager, in accordance with clause 6.3(e).

DSM User means at any time, any individual employed by the Digital Services Manager who has been approved by the CEO of the Digital Services Manager to collect and use Schedule 1 Data (or an agreed subset of it) for the Permitted Purpose.

Go Live Date has the meaning given in clause 4(d).

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.

Permitted Purpose means the purpose specified in Schedule 2 for which the Transferred Data may be used by Authorised Users, CARE Data Users and DSM Users (as the case may be).

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 the Data Recipient in accordance with the Act, the person believed responsible for causing the harm and/or the risk of harm to the Child (whether by an act or omission).

Personal Information has the meaning given in applicable Privacy Laws from time to time, and includes any information or opinion in any form, whether recorded or not, about an identified individual or an individual who is reasonably identifiable.

Pre-Production Testing means the first stage testing of the MDM and 360VoC Solution for compliance with this Agreement, to be undertaken during the Testing Period.

Privacy Laws means all applicable laws relating to data security and the protection of Personal Information in force from time to time, including the *Information Act 2002 (Information Act)* and *Information Privacy Principles*, and any codes or guidelines approved under that act.

Production Testing means the second stage testing of the MDM and 360VoC Solution for compliance with this Agreement, which testing will take place in a live environment such as that in which the software system will be required to operate on a day to day basis, to be undertaken during the Testing Period.

Schedule 1 Data means the Data held by the Agency in relation to a Child or Close Connection, that falls within the data categories and descriptions set out in the Schedule 1 or any other data categories and descriptions as agreed by the parties under clause 9, but does not include:

- (a) information that is covered by a secrecy provision or confidentiality provision that precludes disclosure; or
- (b) information that is subject to a confidentiality, suppression or secrecy order issued by a court, tribunal or commission.

Term means the period of time specified in clause 6.8.

Testing Period means a period of 60 days from the Commencement Date (or such longer period notified by the Digital Services Manager).

Transferred Data means the Schedule 1 Data of a Child or Close Connection that has been transferred by the Digital Services Manager from the Agency Database to the 360VoC Data Hub, to CARE or to the MDM, and can be accessed by:

- (a) Authorised Users in the 360VoC Application (and, where expressly stated in Schedule 2, the 360VoC Data Hub);
 - (b) CARE Data Users in CARE; and
 - (c) DSM Users in the 360VoC Solution and MDM,
- (in each case, respectively).

wellbeing of a child has the meaning set out in section 14 of the Act.

WWC Clearance means a clearance notice issued under the Act that is in force.

Part 2 – Purpose of Agreement

2. Object and underlying principle

The parties:

- (a) agree that they have entered into this Agreement for the purpose of Part 5.1 of the Act; and
- (b) acknowledge the object of Part 5.1 of the Act is to ensure the safety and wellbeing of children, by enabling the CEO of the Data Recipient to have timely access to information about children by virtue of having entered into this Agreement.

3. Sharing of information

- (a) The parties acknowledge and agree that for the purpose of section 226(2) of the Act, the sharing of the Schedule 1 Data:
 - (i) is reasonably necessary to achieve the objects of the Act; and

- (ii) is likely to enable the Data Recipient to detect, investigate, manage or otherwise respond to matters related to the safety and wellbeing of children; and
 - (iii) is likely to substantially contribute to the Data Recipient's capacity to improve outcomes for child safety and wellbeing, including by improving the efficiency with which information can be accessed to guide decisions and actions regarding child safety and wellbeing.
- (b) The parties acknowledge that the sharing of data under this Agreement consists of the transfer of Schedule 1 Data by the Digital Services Manager from the Agency Database to the 360VoC Data Hub or CARE without notification to or further authorisation by the Data Provider.
 - (c) Notwithstanding any other provision of this Agreement, the Data Provider may refuse to provide certain Schedule 1 Data on the basis outlined in section 232 of the Act.
 - (d) The Digital Services Manager must ensure that the technical solution referred to in clause 4(b) enables the Data Provider to:
 - (i) exercise its rights under, and in compliance with, section 232 of the Act;
 - (ii) identify information that is covered by a secrecy provision or confidentiality provision that precludes disclosure; and
 - (iii) identify information that is subject to a confidentiality, suppression or secrecy order issued by a court, tribunal or commission.
 - (e) The Digital Services Manager must ensure that the technical solution enables the transfer of Schedule 1 Data to occur in a manner which will not compromise the Data Provider's rights under section 232 of the Act and is compliant with this Agreement.

4. Role of the Digital Services Manager

- (a) The parties acknowledge that the Digital Services Manager is the agency that manages the Northern Territory Government's digital environment and supports all Northern Territory Government agencies through the delivery of digital services including core ICT infrastructure and support services and data centre services.
- (b) The Digital Services Manager is responsible for establishing a technical solution to enable the transfer of data as contemplated by clause 3(b).
- (c) The Digital Services Manager is responsible for:
 - (i) undertaking all the activities necessary for the Pre-Production Testing stage and the Production Testing stage during the Testing Period; and
 - (ii) the Transferred Data prior to the Go Live Date.
- (d) Once the Production Testing has been successfully completed, the Digital Services Manager will give notice to the Data Recipient and the Data Provider of the date that the Transferred Data will be made available to Authorised Users (**Go Live Date**).
- (e) The Digital Services Manager agrees to:
 - (i) undertake the Pre-Production Testing and Production Testing during the Testing Period, at all times in compliance with applicable law;
 - (ii) monitor, manage and operate the linkage of data as described in clause 6.3(e), at all times in compliance with applicable law;
 - (iii) manage the Data in accordance with the Privacy Laws and to the extent that same are not inconsistent with the Privacy Laws, its usual security and privacy practices and procedures; and
 - (iv) assist the parties in relation to technical matters that may arise under this Agreement in connection with the Schedule 1 Data and Transferred Data.

5. Sharing of Schedule 1 Data

5.1 Transferred Data

If the Data Recipient:

- (a) wishes to access the Schedule 1 Data about:
 - (i) a Child; or
 - (ii) any Close Connection to the extent that the relevant Schedule 1 Data is identified as Schedule 1 Data applicable to a Close Connection; and
- (b) intends to use that Schedule 1 Data for a Permitted Purpose,
then:
 - (c) by entering into this Agreement, the Data Provider authorises the transfer, provided the Data Recipient is compliant with this Agreement;
 - (d) the Data Recipient may initiate the transfer by the Digital Services Manager of that Schedule 1 Data from the Agency Database to the 360VoC Data Hub;
 - (e) once that Schedule 1 Data is transferred to the 360VoC Data Hub, that Schedule 1 Data becomes Transferred Data for the purpose of this Agreement; and
 - (f) the Transferred Data held in the 360VoC Data Hub will be displayed to Authorised Users in the 360VoC Application on and from the Go Live Date.

5.2 CARE Data

If the Data Recipient:

- (a) requires urgent and immediate access to CARE Data about a Child; and
- (b) intends to use that CARE Data for a Permitted Purpose,
then:
 - (c) the Data Recipient may initiate the transfer by the Digital Services Manager of that CARE Data from the Agency Database to CARE;
 - (d) by entering into this Agreement, the Data Provider authorises that transfer, provided the Data Recipient remains compliant with this Agreement;
 - (e) once that Schedule 1 Data is transferred to CARE, that Schedule 1 Data becomes Transferred Data for the purpose of this Agreement; and
 - (f) the Transferred Data held in CARE will be displayed to CARE Data Users in CARE on and from the Go Live Date.

5.3 Responsibility for Transferred Data

The Data Recipient acknowledges and agrees:

- (a) it will have possession or custody of the Transferred Data, and will 'own' Transferred Data for the purpose of section 225 of the Act, on and from the Go Live Date;
- (b) the Data Provider gives no warranty as to the accuracy or completeness of the Transferred Data;
- (c) the Data Provider will have no access to, or control over, or knowledge of the Transferred Data (other than to the extent it is set out in Schedule 1);
- (d) the Transferred Data is the responsibility of the Data Recipient on and from the Go Live Date; and
- (e) except to the extent the Act is inconsistent with another law of the Territory, acknowledges that it must deal with the Transferred Data in the manner required by the Privacy Laws.

Part 3 – Specific requirements of the Act

6. Section 227 of the Act

6.1 Requirements of section 227

- (a) The parties acknowledge that section 227 of the Act requires this Agreement to include certain information.
- (b) This clause 6 contains the information required by section 227 of the Act.

6.2 Detailed description of the data (s.227(i)(a))

- (a) Subject to this clause 6.2, the Data Provider will make available to the Digital Services Manager for transfer to the Data Recipient in accordance with the terms of this Agreement and subject to the Act, the Schedule 1 Data, which as at the Commencement Date is the information set out in Schedule 1.
- (b) The Data Recipient may only initiate a transfer of Schedule 1 Data to the 360VoC Data Hub for a Child if Part 1 of Schedule 1 indicates that the Schedule 1 Data can be transferred in respect of a Child.
- (c) The Data Recipient may only initiate a transfer of Schedule 1 Data to the 360VoC Data Hub in respect of a Close Connection if Part 2 of Schedule 1 indicates that the Schedule 1 Data can be transferred in respect to a Close Connection.
- (d) The Data Recipient may only initiate a transfer of Schedule 1 Data to CARE for a Child if Part 1 of Schedule 1 indicates that the Schedule 1 Data can be transferred to CARE in respect of a Child.
- (e) The parties acknowledge that not all of the Schedule 1 Data, as at the Commencement Date, will be available in the Agency Database to enable it to be transferred to the 360VoC Data Hub or CARE in the manner contemplated by clause 3(b). As particular Schedule 1 Data becomes available in the Agency Database, the Data Provider will cooperate with the Data Recipient to make that Schedule 1 Data available in the Agency Database as soon as practicable after the Commencement Date.

6.3 How the Transferred Data will be accessed, used, interpreted, linked and secured (s.227(1)(b))

Access to, and use of, Transferred Data

- (a) The Data Recipient may allow an Authorised User and CARE Data User (as applicable) to access and use the Transferred Data for the Permitted Purpose.
- (b) Subject to clause 6.3(e)(x), the Data Recipient must (and must ensure the Authorised Users and CARE Data Users) comply with all applicable laws in respect of the use of the Transferred Data and must not:
 - (i) use Transferred Data in a manner which causes the Data Provider to contravene any applicable law;
 - (ii) use Transferred Data other than for the Permitted Purpose; and
 - (iii) provide Transferred Data to any third party unless expressly permitted by this Agreement or required or permitted by law.

Interpretation of Transferred Data

- (c) The Data Recipient acknowledges and agrees that it will ensure that each Authorised User and CARE Data User interprets the Transferred Data in accordance with the Permitted Purpose.

- (d) The Digital Services Manager acknowledges and agrees that it will ensure that each DSM User interprets the Transferred Data for the purposes set out in clause 6.3(e).

How Schedule 1 Data will be linked

- (e) The Schedule 1 Data will be linked in the following manner:
- (i) The Digital Services Manager will utilise MDM to link the Schedule 1 Data.
 - (ii) Software with MDM functionality will apply predefined matching rules to identify and match a given individual across the Agency Database and the 360VoC Solution. These matching rules will analyse and compare the basic identity information (being the individual's first name, family name, alternative first and family names, date of birth, gender (identified), sex (biological) contact details, date of death and the Data Provider's and Data Recipient's identifiers) of customers in the Agency Database (**Agency Identity Data**), against the basic identity information of a Child and Close Connections in CARE (**CARE Identity Data**), to determine if an individual on the Agency Database is a Child or Close Connection in CARE.
 - (iii) The Data Provider can only view its own Agency Identity Data (except in limited circumstances, where a Data Steward of the Data Provider can review CARE Identity Data, for the purpose of manually verifying an unconfirmed/partial match of an individual).
 - (iv) The Data Recipient can only view the CARE Identity Data (except in limited circumstances, where a Data Steward of the Data Recipient can review Agency Identity Data, for the purpose of verifying an unconfirmed/partial match of an individual).
 - (v) Where a direct match is identified through this automated process, a common identifier will be assigned to the individual (being a Child or Close Connection), programmatically linking the relevant individual between the Agency Database and CARE.
 - (vi) Where a partial or suspected match is identified by those predefined matching rules:
 - (A) a Data Steward (Digital Services Manager) will manually review the Agency Identity Data and CARE Identity Data, to determine whether there is any match between the individual in the Agency Database and any Child or Close Connection;
 - (B) Data Stewards of the Data Recipient and Data Provider may be requested to manually review the Agency Identity Data and CARE Identity Data, to determine whether the partial or suspected match can be validated;
 - (vii) Where a direct match is identified through this manual process, the Data Steward (Digital Services Manager) will then manually assign a common identifier to the matched Data, programmatically linking the relevant individual between that Agency Database and CARE.
 - (viii) Where there is a match (either automatically or manually), the common identifier will link the Schedule 1 Data for that individual with the relevant Child or Close Connection in the 360VoC Data Hub, and enable the relevant Schedule 1 Data to be transferred in accordance with clause 5.1.
 - (ix) Where no match is identified, either automatically (by the predefined matching rules) or manually (by a Data Steward), then the Agency Identity Data cannot be linked. This ensures that no Personal Information will be transferred to the 360VoC Solution in respect of an individual that is neither a Child nor Close Connection.
 - (x) The Digital Services Manager must (and must ensure DSM Users) comply with all applicable laws in respect of the collection and/or use of Schedule 1 Data (or a subset of it) for the purposes set out in this subclause (e).

How Transferred Data will be secured

- (f) The Data Recipient must:
 - (i) subject to clause 6.3(f)(iii), secure the Transferred Data in the same manner, and to the same extent, as it secures other confidential, personal and sensitive data within its control from time to time;
 - (ii) maintain, enforce and continuously improve its safety and security procedures and safeguards against the unauthorised use, disclosure, destruction, loss or alteration of Transferred Data; and
 - (iii) if the Data Recipient proposes to secure the Transferred Data in a manner different to that contemplated in clause 6.3(f)(i), establish and update from time to time protocols and guidelines in relation to such security arrangements, provided it is no less secure.
- (g) The Digital Services Manager must secure the Agency Identity Data and CARE Identity Data in the MDM in the same manner, and to the same extent, as it secures other Data within its control from time to time and in accordance with applicable laws.

6.4 Categories of users and access conditions (s.227(1)(c))

- (a) The following categories of individuals may access the Transferred Data for the Permitted Purpose:
 - (i) an individual who holds, or acts in, the position of CEO of the Data Recipient;
 - (ii) an individual who is an Authorised User, CARE Data User or DSM User and meets each of the following criteria:
 - (A) the individual has provided the Data Recipient (if required by the Data Recipient) with a current valid WWC Clearance and agrees to maintain the validity of the WWC Clearance;
 - (B) if required by the Data Recipient, the individual has provided the Data Recipient with an exemption granted by the CEO under section 187(5) of the Act and on expiry of that exemption, provides the Data Recipient with a current valid WWC Clearance and agrees to maintain the validity of the WWC Clearance;
 - (C) the individual has completed the required training in clause 7 and has confirmed in writing they are aware of their legal obligations when accessing Transferred Data; and
 - (D) the individual has provided the Data Recipient with a satisfactory national police check obtained from the SAFE NT website and where necessary or if required by the Data Recipient, from the Australian Federal Police or if the individual resides outside of Australia, from the equivalent police authority in the individual's country of residence, and agrees to provide the Data Recipient with an updated national police check or equivalent police authority (if applicable), if required to do so.
- (b) The conditions of an individual described in clause 6.4(a)(ii) maintaining access to the Transferred Data are that the individual must:
 - (i) maintain the validity of the WWC Clearance (if required by the Data Recipient);
 - (ii) at all times comply with their legal obligations when accessing Transferred Data;
 - (iii) maintain a satisfactory record for the purpose of offending that would appear on a national police check or equivalent police authority from the individual's country of residence (if applicable); and
 - (iv) at all times comply with the terms of this Agreement.

6.5 Restrictions on access, use and interpretation of the Transferred Data (s.227(1)(d))

- (a) An Authorised User, CARE Data User and DSM User must only access, use and (where their role requires them to do so) interpret Transferred Data in accordance with:
 - (i) this Agreement;
 - (ii) all applicable laws, including the Act and Privacy Laws; and
 - (iii) to the extent that they are consistent with the laws referred to in clause 6.5(a)(ii), all applicable Northern Territory Government policies and guidelines.
- (b) No person, including Authorised Users, may access the Transferred Data at any time unless they meet the criteria set out in clause 6.4(a) and are compliant with the conditions set out in clause 6.4(b).
- (c) The Data Recipient will, at least twice in each calendar year, conduct an audit of Authorised Users' compliance with this Agreement and report the extent and level of compliance to the Committee together with steps that it will take to address any non-compliance and timeframes within which the non-compliance will be addressed.

6.6 Data Provider no longer owns the Schedule 1 Data (s.227(1)(e))

If the Data Provider no longer owns the Schedule 1 Data (for example, as a result of machinery of government changes with the Data Provider no longer having administrative responsibility for the Schedule 1 Data), it will notify the Data Recipient immediately that it does not own the Schedule 1 Data and cannot provide the Schedule 1 Data in accordance with this Agreement. If only part of the Schedule 1 Data is no longer owned by the Data Provider, then this Agreement shall be deemed to be varied to delete that part of the Schedule 1 Data from Schedule 1.

6.7 What happens if a party breaches the Agreement (s.227(1)(f))

- (a) If a party (**Breaching Party**) becomes aware that it has not, or that there are reasonable grounds to suspect that it has not, complied with any of its obligations under this Agreement, the Breaching Party must notify the other parties (**Non-Breaching Parties**) as soon as practicable after becoming aware. The Breaching Party's notice must give details of the relevant breach, including which obligation has been breached and how it was breached.
- (b) If a party (**Non-Breaching Party**) becomes aware that another party (**Breaching Party**) has not, or that there are reasonable grounds to suspect that the Breaching Party has not, complied with any of its obligations under this Agreement, the Non-Breaching Party must notify the Breaching Party within 2 Business Days after becoming aware. The Non-Breaching Party's notice must give details of the relevant breach, including which obligation has been breached and how it was breached.
- (c) After a notice is given under clause 6.7(a) or 6.7(b), the parties will cooperate to agree on any steps that should be taken to:
 - (i) rectify the breach, to the extent that it is capable of being rectified;
 - (ii) mitigate the impact of the breach, including any risk of the breach causing serious harm to any individual; and
 - (iii) mitigate the risk of any similar breach occurring in the future,**(Remediation Steps).**
- (d) The parties will cooperate to:
 - (i) take any action in relation to the relevant breach that is necessary to comply with:
 - (A) the requirements of any applicable laws, having regard to the nature of the breach; and
 - (B) to the extent that they are consistent with the laws referred to in clause 6.7(d)(i)(A), any applicable government policies or guidelines; and

- (ii) otherwise seek to remedy the relevant breach and mitigate the impact of that breach, including by implementing any agreed Remediation Steps to the extent that they are consistent with the actions required by clause 6.7(d)(i)(A).

6.8 The period for which the Agreement is in force (s.227(1)(g))

This Agreement will commence on the Commencement Date and continue for a period of 5 years unless terminated earlier in accordance with this Agreement.

6.9 How the Agreement may be terminated (s.227(1)(h))

- (a) The parties acknowledge and agree that this Agreement has been entered into in accordance with the Act and to ensure the safety and wellbeing of children in the Northern Territory, and that the purpose of, and the continued operation of, the Agreement is fundamental to upholding the principles of the Act.
- (b) Notwithstanding the parties' acknowledgement outlined in clause 6.9(a), a party may terminate this Agreement if:
 - (i) (acting reasonably) a change in circumstances or Agency or Territory policy or direction requires;
 - (ii) a dispute remains unresolved after following the process in clause 13(a) to 13(d); or
 - (iii) there is a Serious Data Breach,

provided that the party must notify the other party, and the parties must first make their respective CEOs reasonably available to meet to discuss the Agreement during the period of 10 Business Days after that notice is given. After expiration of those 10 Business Days, unless the parties agree otherwise in writing, either party may terminate this Agreement immediately by notice to the other party.

6.10 Review of Agreement (s.227(3))

- (a) The parties agree to review this Agreement to ensure the sharing of Schedule 1 Data continues to meet the criteria specified in section 226(2) of the Act on the third anniversary of the Commencement Date (**Review**) (and thereafter at least once every five years) and each Review will:
 - (i) be carried out by the parties following consultation with the Committee and will take in to account the view of the Information Commissioner (NT);
 - (ii) consider any improvements or upgrades that may be required to be made to either parties' software systems and consider who is responsible for payments of the costs if upgrades and improvements are needed;
 - (iii) consider the impact (if any) of the broader data sharing arrangements (for example, data sharing with the Commonwealth); and
 - (iv) consider what information (if any) needs to be made available to the public.
- (b) If, following the Review, a party intends to terminate this Agreement, that party must first follow the process set out in clause 6.9.
- (c) On expiry or early termination of this Agreement, the Data Recipient must deal with the Transferred Data in accordance with the Data Recipient's retention protocols and applicable laws.

Part 4 – Ancillary provisions

7. Education and training

The Data Recipient must establish, maintain and continuously improve, education and training of Authorised Users and the CARE Data Users with respect to:

- (a) privacy and confidentiality of the Data and prevention and management of breaches;
- (b) how the Data may be accessed, used, interpreted, linked and secured;
- (c) unauthorised use and misuse of Data;
- (d) how to deal with the Data when it is no longer needed;
- (e) compliance with this Agreement; and.
- (f) the consequences of non-compliance such as criminal and civil liability, disciplinary action, Independent Commissioner Against Corruption investigation, and the like.

8. Governance, transparency and oversight

- (a) The Data Recipient and the Data Provider agree that the Committee will monitor the progress of the obligations performed under this Agreement.
- (b) The Data Recipient and the Data Provider agree that the Committee will consider various matters raised following the process in clause 13 and include such things as:
 - (i) the privacy and confidentiality of the Transferred Data and prevention and management of breaches in accordance with this Agreement;
 - (ii) whether the arrangement is operating as intended and achieving its objectives;
 - (iii) how the Transferred Data is being accessed, used, interpreted, linked and secured;
 - (iv) whether there has been any unauthorised use or misuse of the Transferred Data;
 - (v) resolving any dispute notified to the Committee by the parties under clause 13(e); and
 - (vi) ongoing compliance with this Agreement.

8.2 Freedom of Information requests

In relation to the Transferred Data, the Data Recipient will be responsible for dealing with freedom of information requests in accordance with the Information Act.

9. Changes to Schedule 1 Data

9.1 Expanded or new information

The Data Recipient may request a change be made to the Schedule 1 Data set out in Schedule 1 by way of expansion on current information required or new information to be included at Schedule 1.

9.2 Variation

If the Data Recipient makes a request under clause 9.1, and the Data Provider provides its written consent to the expanded or new information, then subject to clause 9.4 the expanded or new information will be taken to be Schedule 1 Data for the purpose of this Agreement.

9.3 Rejection of request

- (a) If the Data Recipient makes a request under clause 9.1, and the Data Provider does not provide its written consent to the request, this Agreement continues unchanged. Such a rejection does not prevent the Data Recipient from submitting another request under clause 9.1.
- (b) If the Data Provider does not provide its written consent to the request, either party may refer the matter to dispute resolution under clause 13.

9.4 Variation

Notwithstanding the provisions of this clause 9, the parties must comply with the Act.

10. Change to Authorised Users and CARE Data Users

10.1 Removal or creation of Authorised Users and CARE Data Users

The Data Recipient may request in writing the removal of existing positions, or the creation of new positions, of Authorised Users and CARE Data Users as set out in Schedule 2. The Data Provider may seek additional information as it requires to consider the request. Provided the Data Provider has received the information it requires to consider the request, the Data Provider will not unreasonably refuse the request and if it does refuse the request, it will provide reasons for doing so.

10.2 Variation

If the Data Recipient makes a request under clause 10.1, and the Data Provider provides its written consent to the request, then subject to clause 10.4, the positions will be taken to be added to or removed from (as the case may be) the list of Authorised Users or CARE Data Users (as the case may be) set out in Schedule 2 for the purpose of this Agreement.

10.3 Rejection of request

- (a) If the Data Recipient makes a request under clause 10.1, and the Data Provider does not provide its written consent to the request, this Agreement continues unchanged. Such a rejection does not prevent the Data Recipient from submitting another request under clause 10.1.
- (b) If the Data Provider does not provide its written consent to the request, either party may refer the matter to dispute resolution under clause 13.

10.4 Variation

Notwithstanding the provisions of this clause 10, the parties must comply with the Act.

11. What happens if there is a Data Breach

- (a) The parties acknowledge that a Data Breach has the potential to significantly impact the Northern Territory Government's reputation and create a financial liability for the one or more of the parties.
- (b) This clause 11 applies if the Data Recipient becomes aware, or reasonably suspects, that:
 - (i) there has been unauthorised access to, or unauthorised disclosure of, any Transferred Data; or
 - (ii) Transferred Data has been lost in circumstances where unauthorised access to, or unauthorised disclosure of, that data may occur,(a **Data Breach**).
- (c) In the event of a Data Breach, the Data Recipient must:
 - (i) take all reasonable action to contain the Data Breach;
 - (ii) maintain a centralised log of all Data Breaches;
 - (iii) notify the Data Provider of the Data Breach:
 - (A) immediately (verbally) in the event of a "**Serious Data Breach**", being a Data Breach that:
 - (I) is likely to cause serious harm to any individual; or

- (II) has resulted in a significant unauthorised access or disclosure of personal information (such as a cyberattack); or
 - (III) is otherwise designated by applicable Northern Territory Government policies and procedures as requiring immediate notification to the Data Provider,

with such notification being given in writing no later than 2 Business Days after becoming aware of the Data Breach; and
 - (B) in any other case – in writing as soon as practicable after that time;
- (iv) undertake an expeditious and thorough investigation of the Data Breach, in compliance with any applicable Northern Territory Government policies or guidelines including any relevant policies or guidelines issued by the Office of the Information Commissioner (NT) and any applicable Privacy Laws;
- (v) if a Serious Data Breach has occurred:
 - (A) immediately take any other action that is necessary to prevent the threat of or likelihood of serious harm from occurring (including reporting to appropriate authorities);
 - (B) as soon as reasonably practicable after becoming aware of the Serious Data Breach, notify affected persons (in compliance with any applicable Northern Territory Government policies or guidelines);
 - (C) comply with the requirements of any applicable laws, including Privacy Laws; and
 - (D) to the extent that they are consistent with the laws referred to in clause 11(c)(iv), comply with any applicable Northern Territory Government policies or guidelines including any relevant policies or guidelines issued by the Office of the Information Commissioner (NT) or the Data Recipient, including as to the notification to affected individuals; and
- (vi) without limiting the Data Recipient's obligations under clause 11(c)(iv):
 - (A) immediately take all reasonable action, at the Data Recipient's cost and/or the Digital Services Manager's cost (as the case may be), to contain and remedy the Serious Data Breach and take appropriate remedial action to mitigate or prevent any serious harm, or further misuse or breach;
 - (B) promptly provide the Data Provider, the Committee and the Information Commissioner (NT) with a statement setting out:
 - (I) a description of the Serious Data Breach;
 - (II) the kind or kinds of information concerned; and
 - (III) recommendations on the steps that the Data Recipient will take in response to the Serious Data Breach; and
 - (IV) outlining the steps taken or proposed to be taken to notify affected persons,

and copies of any report or such other documentation relevant to the investigation as the Data Provider, the Committee or the Information Commissioner (NT) might reasonably request.
- (d) The Data Recipient acknowledges and agrees:
 - (i) the Transferred Data is not within the Data Provider's possession or control;
 - (ii) the Data Provider is not and will not be responsible for a Data Breach; and
 - (iii) the Data Recipient will bear all responsibility and liability of dealing with a Data Breach, including any claim, demand, charge, interest, loss, penalty, cost and expense (including reasonable legal fees), including those incurred by the Data

Provider, and will consult with the Data Provider appropriately in dealing with the consequences of a Data Breach.

12. Privacy complaints procedure

- (a) The Data Recipient must comply with its procedures when:
 - (i) handling inquiries about the privacy of Transferred Data;
 - (ii) taking, investigating and making a decision about complaints about the interference with the privacy of an individual; and
 - (iii) providing for reporting to the Information Commissioner (NT).
- (b) Complaints made to the Data Provider or the Digital Services Manager with respect to Transferred Data will be promptly referred to the Data Recipient to be dealt with in accordance with its procedure.
- (c) The Data Recipient must keep a register of the complaints received and, if requested by the Data Provider, provide a copy of the register to the Data Provider.

13. Dispute resolution

- (a) If a dispute arises under this Agreement, the parties must use its reasonable efforts to resolve the dispute.
- (b) If the parties cannot resolve a dispute, either party may deliver a written notice to the other party (**Notice of Dispute**) which states that it is a Notice of Dispute under this clause 13 and provide details of the dispute.
- (c) Within 5 Business Days (or such longer period as agreed in writing by the parties) of delivery of a Notice of Dispute, representatives of the parties who have authority to resolve the dispute must meet in good faith and attempt to resolve the dispute.
- (d) If the dispute is not resolved within 10 Business Days of the delivery of the Notice of Dispute (or within such longer period as agreed by the parties), then the dispute will be referred to each party's CEO who must meet in good faith and attempt to resolve the dispute within a further 10 Business Days, or other period agreed in writing between the parties.
- (e) If the dispute is not resolved in accordance with this clause 13, the parties may notify the Committee and request the Committee consider and resolve the dispute or a party may terminate the Agreement.
- (f) Despite the existence of a dispute, the parties must continue to perform their obligations under this Agreement.

14. Notices

- (a) A notice under this Agreement must be:
 - (i) in writing;
 - (ii) given by the CEO of the notifying party; and
 - (iii) sent to the CEO of the receiving party.
- (b) A notice received after 4.30 pm, or on a day that is not a Business Day, is deemed to be given on the next Business Day. Otherwise, a notice is deemed to be given upon delivery to the address of the receiving party's CEO (if delivered by post or by hand) or upon actual receipt by the receiving party's CEO (if transmitted electronically).

15. General provisions

15.1 Variation

An amendment of this Agreement is binding only if it is:

- (a) agreed in writing and signed by the parties; and
- (b) made in accordance with section 231 of the Act.

15.2 Information-sharing obligations outside of this Agreement

- (a) Nothing in this Agreement affects any Other Information-Sharing Obligation that may apply to either party from time to time, whether arising under:
 - (i) the Act;
 - (ii) the *Information Act 2002* (NT);
 - (iii) the *Domestic and Family Violence Act 2007* (NT); or
 - (iv) any other applicable laws.
- (b) In this clause 15.2, '**Other Information-Sharing Obligation**' means any duty or other legal obligation relating to the sharing of data or information, excluding any such duty or obligation that arises under the terms of this Agreement.

Schedule 1 – Description of the Schedule 1 Data

INTRODUCTION

The Chief Executive Officer of the Department of Territory Families, Housing and Communities as the Data Recipient (CEO), in addition to the general responsibility for promoting and safeguarding the safety and wellbeing of Children, has a particular interest in Data relating to the following:

A Child of Attention

- a child for whom information has been received which raises a concern about the child's safety and wellbeing; and
- a child whom the CEO believes on reasonable grounds might be in need of protection.

These children are referred to in the tables below as a '**Child**' (as defined in clause 1.1). The CEO has the power to make enquiries about a Child of Attention to inform the CEO's decision as to whether any further action should be taken to safeguard the safety and wellbeing of the Child.

A Child in Care

- a child in the CEO's care, whether under a temporary placement arrangement or provisional protection; or
- a child 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 Northern Territory.

These children are referred to in the tables below as a '**Child**' (as defined in clause 1.1). The CEO has an interest in these Children as if the CEO was their parent, and has a range of obligations in relation to these Children, such as developing care plans, providing appropriate living arrangements, and monitoring the Child's wellbeing. Therefore, it is important to the work of the CEO, and Authorised Users in the office of the Data Recipient, to have access to a variety of information that would ordinarily be available to the Child's parent, including education related information.

This will allow the CEO to have a holistic view of a Child and their circumstances to assist in identifying family and social support, as well as evaluating risks to safety and wellbeing.

The CEO delegates powers under the *Care and Protection of Children Act 2007* to a range of officers within the Agency, including Authorised Users specified in Schedule 2 of this Agreement. These Authorised Users include, among others, Child Protection Practitioners and Case Support Workers who work with Children and their families and carers, and Child Intake Case Managers who investigate notifications of potential harm to Children of Attention or Children in Care. When exercising the delegated powers, these Authorised Users require access to data in CARE and the 360VoC Application.

The tables below set out the Data Categories, with illustrative examples of the Data type that the Department of Education as the Data Provider will make available to the Data Recipient through the 360VoC Solution. The tables also include an explanation as to why the Data is likely to enable the Data Recipient to detect, investigate, manage or otherwise respond to matters relating to the safety and wellbeing of Children.

DATA REPOSITORIES		
Repository Name	Purpose	Who can access the data
360VoC Data Hub	The 360VoC Data Hub is a secured central repository for Data of the nature described in the tables below and is the data hub within the 360VoC Solution, that receives and stores Data about a Child or Close Connection provided by the Data Provider in a 'read only' format.	The Data is accessible only to DSM Users and the reporting and analytics worker under the Data Access Agreement
360VoC Application	The 360VoC Application is a secured central repository for Data that displays Data sourced from the 360VoC Data Hub, in a 'read only' format, via link in CARE.	The Data is accessible only to Authorised Users under the Data Access Agreement.
CARE	This is the consolidated system utilised by the Data Recipient for child protection, youth justice and adoptions case management.	The Data is accessible only by CARE Data Users under the Data Access Agreement

PART 1. DATA RELATING TO CHILD OF ATTENTION AND CHILD IN CARE

All Data in Part 1 relating to a Child will transfer into the 360VoC Data Hub and will be accessible to Authorised Users via the 360VoC Application as a 'read only' reflection of what appears in the Agency Database of the Data Provider.

Index	Data Categories	Description	Why is the data required by the CEO?
1.1	Person	<p>Identifying information for a Child.</p> <p><u>Illustrative Examples</u></p> <ul style="list-style-type: none"> • Given Name • Middle Name • Family Name (Surname) • Gender (identified) • Sex (biological) • Date of Birth • Alias Names • Address • System Identifiers • Relationships 	<p>Data on the Child stored by the Data Recipient, will be matched against the Data held in the Data Provider's Agency Database. Examples of how the Data will be used by the Data Recipient is explained in each information category.</p>

Index	Data Categories	Description	Why is the data required by the CEO?
		<ul style="list-style-type: none"> • Contacts 	
1.2	Current School/s	<p>This section provides information on the government school/s where a Child is currently enrolled.</p> <p>Note: Students may be enrolled in more than one school, for example at a special education school and another government school, or a remote high school and a distance education school.</p> <p><u>Illustrative Examples</u></p> <ul style="list-style-type: none"> • School details including school name, location, contact details, principals name etc • Date of last attendance, and status of enrolment (active/not active) • Current year level • Date of enrolment • Parent/caregiver details 	<p>The CEO requires details of the school/s where the Child is currently enrolled.</p> <p>This will assist in understanding:</p> <ul style="list-style-type: none"> • whether the Child is regularly being sighted by persons who have ability to identify concerns for the Child's safety and wellbeing • to support identification of the location of the Child to inform risk assessment and plan an investigation • where the Child is currently studying • when the Child last attended this school • what year level the Child is in • the Child's current engagement with the school to assist with potential communications with them. <p>Note: Specific contacts at the school for the Child will be recorded elsewhere in CARE.</p>
1.3	Enrolment History	<p>Provides a summary of enrolments at NT government school/s for a Child, and the period that they were enrolled, e.g. from 2015 to 2018.</p> <p><u>Illustrative Examples</u></p> <ul style="list-style-type: none"> • School details including school name, location, contact details, principals name etc • Entry (Enrolment) Date • Departure Date • Enrolment status (Active, non-active, no longer enrolled) 	<p>The CEO requires details regarding the Child's enrolment history.</p> <p>This will assist in understanding:</p> <ul style="list-style-type: none"> • the Child's consistency and commitment towards education • where the Child has been enrolled over certain time periods • a comparison to other information about the Child's history and context.
1.4	Attendance history	<p>Provides a summary of the annual attendance data at NT government schools for a Child.</p> <p><u>Illustrative Examples</u></p> <ul style="list-style-type: none"> • School name • Year (the calendar school year) 	<p>The CEO requires details regarding a Child's attendance history by school and year.</p> <p>This will assist in understanding:</p> <ul style="list-style-type: none"> • changes in the Child's mobility and caregiver arrangements

Index	Data Categories	Description	Why is the data required by the CEO?
		<ul style="list-style-type: none"> Days attended/school days enrolled 	<ul style="list-style-type: none"> parent/caregiver capacity to support their Child attain a reasonable level of education to provide for their long term wellbeing the Child's consistency and commitment towards education where the Child has been engaged and disengaged with different schools over certain time periods a comparison to other information about the Child's history and context.
1.5	Recent attendance	<p>Attendance records from NT government schools where a Child, is/was enrolled.</p> <p>Note: Enrolment and attendance records from non-government schools, and schools outside the NT are excluded.</p> <p><u>Illustrative Examples</u></p> <ul style="list-style-type: none"> Days attended/School days on offer Un-notified absence Notified unacceptable absence Other notified absence 	<p>The CEO requires details regarding a Child's recent attendance at school.</p> <p>This will assist in understanding:</p> <ul style="list-style-type: none"> parent/carer support for the Child to attain an education to support their immediate and long term wellbeing and development the Child's consistency and commitment towards education how the Child's engagement in schooling is tracking recently.
1.6	Suspensions and history	<p>Provides the suspension history across NT government schools for a Child.</p> <p>Note: It does not include suspension history from non-government schools or schools outside the NT.</p> <p><u>Illustrative Examples</u></p> <ul style="list-style-type: none"> Incident date refers to the date of the incident that led to the suspension. Start date refers to the first date of the suspension period. Length is the number of school days for the suspension period, excluding weekends. 	<p>The CEO requires details regarding the suspension history of a Child.</p> <p>This will assist in:</p> <ul style="list-style-type: none"> understanding the Child's behaviour at school understanding the number of suspensions or different types/reasons for suspension the Child has received understanding concerning and/or complex behaviours of the Child at school understanding requirements to maintain the Child's engagement with education understanding a comparison of other information about the Child

Index	Data Categories	Description	Why is the data required by the CEO?
		<ul style="list-style-type: none"> Reason is a category of behaviour type which led to the suspension and limited to: e.g. assault, dangerous act etc. The main reason is identified by the school for each suspension. Subtype provides further detail as to the behaviour that led to the suspension. The main subtype is identified by the school for each suspension. 	<ul style="list-style-type: none"> assessing the wellbeing of the Child and identifying triggers or events that may impact on the Child's wellbeing understanding how a Child's trauma history may be contributing to behaviours that lead to suspension assessing the safety of a Child not attending school for an extended period of time support carers to make alternate care arrangements for a Child so they can continue to meet their employment commitments.
1.7	Educational Adjustments for disability	<p>Provides a history of recorded educational adjustment for disability across NT government schools, for a Child. Includes details on whether a formal disability diagnosis has been reported by the Child's parent/guardian/caregiver to the school.</p> <p><u>Illustrative Examples</u></p> <ul style="list-style-type: none"> Physical e.g. loss of a part of the body, cerebral palsy, diabetes, rheumatic heart disease Cognitive e.g. intellectual disability, specific learning disorder in reading, language disorder Social/emotional e.g. Autism, ADHD, Anxiety disorder Sensory e.g. vision or hearing impairment Level of adjustment made by the school for learning Formal diagnosis reported to school by parent 	<p>The CEO requires details regarding the Child's disability data including the level of adjustment.</p> <p>This will assist in understanding:</p> <ul style="list-style-type: none"> the best way to provide support and care the adjustments the Child receives at school to support their learning whether the Child has a disability that requires support outside of school assess vulnerability that may affect the safety and wellbeing of a Child.

*** Guidance Notes on interpreting Schedule 1:**

Schedule 1 Data

- "Schedule 1 Data" is defined to mean the Data held by the Agency in relation to a Child or Close Connection, that falls within the *Data Categories* and *Descriptions* set out in this Schedule 1.
- The '*Data Categories*' are set out in the second column, and the '*Descriptions*' are set out in the third column, of this Schedule 1.

- These two columns comprise 'Schedule 1 Data' and are agreed by the parties at the time of signing this Agreement. Any change to these two columns can only occur in accordance with clause 9 and the requirements of the Act.
- The '*illustrative examples*' set out in the third column do not form part of the definition of 'Schedule 1 Data'. They are only examples of the types of data that may be held by the Agency from time to time, that fall within the Data Categories and Descriptions set out in the second and third columns.
- The '*illustrative examples*' may therefore change from time to time subject to data quality, availability, changes in Agency systems and by agreement of the parties. If the parties agree that the '*illustrative examples*' fall within the existing Data Categories and Descriptions, it will form part of the "Schedule 1 Data" and a formal variation will not be required.

Ability to refuse to provide data

- Notwithstanding the Data Categories and Descriptions set out in this Schedule:
- "Schedule 1 Data" is defined to expressly *exclude* information that is covered by a secrecy provision or confidentiality provision that precludes disclosure, or information that is subject to a confidentiality, secrecy or suppression order issued by a court, tribunal or commission.
- Additionally, the Data Provider can refuse to provide any Schedule 1 Data for the reasons set out in section 232 of the Act.
- Section 3(d) and (e) of this Agreement requires the Digital Services Manager to ensure that the technical solution enables the Data Provider to exercise its rights under section 232 of the Act and identify information that must be excluded due to confidentiality or secrecy laws or orders.

Schedule 2 – Authorised Users, CARE Data Users, DSM Users and Permitted Purposes

Permitted Purpose for Authorised Users

Item	Authorised Users positions	Permitted Purposes
1.	CEO of the Data Recipient	Any purpose consistent with s 227(2) of the Act.
2.	Aboriginal community worker Aboriginal practice advisor Adoptions practitioner Case support worker Central intake worker Child protection manager Child protection practitioner Child protection student on placement Child protection team leader Child protection youth worker Clinical services worker Complaints officer Families and children’s enquiries and support worker Information release officer Legal administrative officer Legal director Legal manager Legal support officer Placements officer Practice leader Remote family worker	<p>To enable the person to detect, investigate, manage or otherwise respond to matters related to the safety and wellbeing of a Child.</p> <p>To enable the person to consider and respond to any freedom of information requests in accordance with the Information Act.</p> <p>To enable the person to consider and respond to any court orders, warrants, notices to produce and complaints in accordance with all applicable laws.</p> <p>To enable the person to consider and respond to any internal and external audit requirements.</p>
3.	Reporting and analytics worker	To contribute to the Data Recipient’s capacity to improve outcomes for child safety and wellbeing, including by undertaking research on the Transferred Data and improving the efficiency with which information can be accessed to guide decisions and actions regarding child safety and wellbeing, and compiling and analysing reports from the 360VoC Application and the 360VoC Data Hub.
4.	Data Steward (Digital Services Manager)	To ensure the system is operating such that other Authorised Users and where applicable CARE Data Users are able to access, use, interpret or link the Transferred Data for a Permitted Purpose. Without limiting the preceding sentence, this purpose includes the performance of any activities contemplated by clause 6.3(e) and clause 4(c) and (d) plus

Item	Authorised Users positions	Permitted Purposes
		support, carry out maintenance, updates, new releases and improvements as reasonably required.
5.	Authorised Officer	Any purpose consistent with s 227(2) of the Act.
6.	Any other position or role which, in the opinion of the Data Recipient's CEO, requires the relevant individual to access, use, interpret or link the Transferred Data for a purpose consistent with s 227(2) of the Act.	In relation to a position or role described in this item 6, such purposes as are approved by the Data Recipient's CEO for that position or role.

Permitted Purpose for CARE Data Users

Item	CARE Data Users positions	Permitted Purposes
1.	CARE Data Users	All of the purposes listed in Item 2 of the table above.

Permitted Purpose for DSM Users

Item	DSM Users positions	Permitted Purposes
1.	DSM Users	<p>For the purpose of monitoring, operating and managing the MDM technology or tool, pursuant to clause 6.3(e), plus to support, carry out maintenance, updates, new releases and improvements as reasonably required.</p> <p>For the purpose of ongoing monitoring, operating and managing the 360VoC Solution, pursuant to clause 4, including to support, carry out maintenance, updates, new releases and improvements as reasonably required.</p> <p>For the purpose of undertaking all activities necessary for the Pre-Production Testing and Production Testing during the Testing Period.</p> <p>For the purpose of compiling and producing reports from the 360VoC Application and 360VoC Data Hub for the relevant Authorised Users.</p>

Signing page

EXECUTED as an agreement.

Signed for and on behalf of the **Department of Territory Families, Housing and Communities** in the presence of



Signature of witness



Emma White – Chief Executive Officer

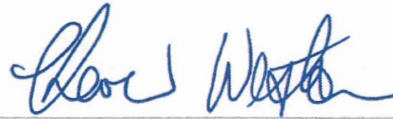
Karolina Iliou

Name of witness (print)

Signed for and on behalf of the **Department of Education** in the presence of



Signature of witness



Karen Weston – Chief Executive Officer

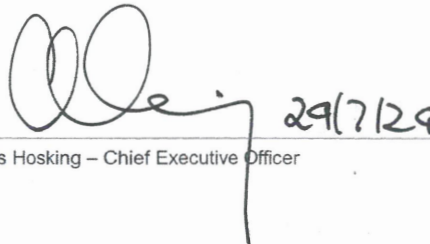
Ashlea Compain

Name of witness (print)

Signed for and behalf of **Department of Corporate and Digital Development** in the presence of



Signature of witness



Chris Hosking – Chief Executive Officer

LYDIA SZCZYGLOWSKI

Name of witness (print)

I, , Minister for Territory Families approve this Agreement pursuant to section 229(4) of the *Care and Protection of Children Act 2007* (NT).

29 July 2024