TUSLA
An Ghníomhaireacht um Leanaí agus an Teaghlach
Child and Family Agency

Child Abuse Substantiation Procedure (CASP) (Excluding CASP Review)
Data Protection Impact Assessment

Stage 2 FINAL

[Public]

1. Introduction

The relevant service or area has completed the Stage 1 Impact Assessment Template and the relevant Information Owner has attested to the factual accuracy of all information contained in this template in order to proceed to the next stage which is a review by the DPU of all information contained within this template in order to identification and assess any data protection and privacy risks relating to this processing activity in order to recommend proposed solutions or safeguards to mitigate the risks identified and assessed during this stage.

Guidance for the DPU Unit:

Review the Stage 1 (and Stage 1a if relevant) Impact Assessment Template and using the Data Protection Impact Assessment Risk Taxonomy at Appendix 1 to this template identify all relevant data protection risks identifying the risk category from the taxonomy and providing a detailed description of the risk for the Information Owner. Read the risk definitions on the taxonomy carefully as these will help you to describe the risk as it applies to this processing accurately for the Information Owner so that he or she can understand the risk and decide whether to agree to the proposed safeguard or risk accept.

Using the Data Protection Impact Assessment Risk Probability and Impact Grid at Appendix 2 to this template assess both the probability and impact of this risk occurring before you recommend any safeguards and calculate the inherent risk rating of this risk and complete this template.

Stage 2 Template

Subject/title of DPIA	CASP (excluding CASP REVIEW)
Information Owner in Tusla Responsible for Signing Off on this DPIA, that is, responsible for implementation any actions to remediate any risks identified in this DPIA and for confirming the factual accuracy of all content in this DPIA	Eilidh McNab, Interim Services Director, Dublin North East

1: Identification and Assessment of Risks and Proposed Safeguards (Measures to Address Risk)

Risk URN	*Risk Category*	*Probability*	*Impact*	*Inherent Risk Rating*	*Residual Risk Rating*	*Target Date of Implementation*
CASP001	*Accountability*	*Probable*	*Severe*	*High*	*Low*	*Before CASP goes live*

There is a risk that if employees do not have sufficient guidance on key elements of data processing as they relate to CASP this may result in a failure to adequately demonstrate and evidence compliance will result in a breach of the Accountability Principle and that failure to comply with the GDPR may result in investigation, administrative fines, prosecution, or other sanctions.

<u>The CASP document</u>

The DPO has reviewed CASP and notes that much work has been done to incorporate the feedback from the DPO in previous iterations of this DPIA and the important consultation workshops and focus groups with key stakeholders including but not limited to, victims' rights groups.

CASP contains appropriate references to data protection and useful guidance on, for example, when to consult the CASP Data Protection Guidance and how and where to record key information and in particular contains the following section which is very important from a data protection accountability perspective:

"Section 9.0:*'The recording and management of information as part of CASP'*

9.1 Introduction

The CASP Data Protection Guidance provides detailed information on Tusla's data protection obligations to, and the data protection rights of service users to whom CASP may apply. The CASP Data Protection Guidance should always be referred to for help in applying data protection obligations in the context of CASP.

9.2 Sharing information with a PSAA

Where the assessment moves to stage 2, fair procedures require that the PSAA is informed of allegations made against them and provided with all relevant information and documentation gathered by the CASP social worker. This information must be provided in accordance with the procedure, even if the PSAA does not request it. If there is information contained within the relevant documentation gathered by the CASP social worker which is not relevant and relates to people other than the PMD or the PSAA, that information should be redacted on the grounds of data protection.

9.3 Information, documentation, and reports from other professionals

Before seeking reports from other professionals, the CASP social worker should advise the reports' authors of Tusla's requirement to share all relevant information and documentation with the PSAA (and their parents if the PSAA is a child). It is important that the authors are aware of this before providing a report to Tusla. This is because, once they receive the documentation, the CASP social worker is obliged to disclose relevant information and documentation to the PSAA should the assessment move to stage 2.

If reports or documents have been given to the CASP social worker that were not requested by them, these reports will have to be disclosed to the PSAA (and their parents if the PSAA is a child) if they are relevant to the assessment. Therefore, it is important that the authors of such reports are informed of the requirements and given the opportunity to raise any objections or request any data restrictions in advance of providing the reports.

9.4 Record Keeping

A record in the PMD's name and the PSAA's name is to be opened when the referral is received. These records are used to hold the details of:

- *disclosures and allegations,*

- *names and circumstances of the PMD and the PSAA,*
- *decisions made during the first stage of the substantiation assessment.*

A case record should also be created in the name of each identified child who is believed to be at risk of harm, including any child who is in the direct care of the PSAA.

Whether the PMD takes part in the substantiation assessment or not, details of an allegation and the actions taken must be carefully recorded in all circumstances. This includes where a disclosure does not reach the threshold to move to stage 1 of a substantiation assessment.

If action has been taken to inform a relevant third party of child protection concerns, the details and reasons for the action must be clearly recorded on any identified child's record and the record of the PSAA.

Details of any agreements and decisions regarding the substantiation assessment should be carefully recorded in records of the PMD and the PSAA.

Documents and handwritten notes must be scanned and saved onto Tusla Case Management System (TCMS), and the originals securely shredded.

When the case is closed, the PMD and the PSAA (if the assessment has moved to stage 2), will be informed in writing of the case closure and their rights under data protection, which should be recorded on the case record.

Details of a Review, the people involved, the correspondence and reports produced must be recorded and kept on the case record on TCMS."

CASP Standard Forms and Templates

The DPO has also reviewed CASP and provided comments on the text and provided comments on all CASP Standard Forms and Templates which are being built into TCMS, (the Tusla Case Management System, the case management system which allows users to digitally manage and record their activities relating to a CASP substantiation assessment and CASP Review).

CASP Data Protection Guidance

The DPO has drafted the CASP Data Protection Guidance to be used by all staff involved in CASP and which is to be read together with CASP and which sets out how the data protection principles apply to CASP.

CASP TCMS Standard Operating Procedures

The DPO is of the view that while CASP sets out important principles, framework and guidance and key factors to be taken into account when operating the CASP process and contains good guidance on record and information management at section 9 and is supplemented by the standard letter and correspondence templates to be built into TCMS, staff would benefit from having Standard Operating Procedures which set out step by step instructions to be followed at each crucial step in the CASP process when using TCMS for CASP and which would reduce the risk of any inconsistent application of the CASP process particularly as it relates to key data processing activities.

For example, staff would benefit from having detailed instruction on (this list is not exhaustive and is offered here by way of example for assistance only):

- How to open a case record;
- What is to be included in a case record;
- What is to be included in the PSAA person record;
- What is not to be included in the PSAA person record;
- What is to be included in the PMD person record;
- What is not to be included in the PMD person record;
- How information is to be collected from the PMD and witnesses, for example, what data collection forms and templates are to be used, how are notes from interviews to be recorded and where, what happens to hard copy notes;

- How to generate correspondence, what templates to use for each correspondence type, where draft and final correspondence is to be stored, how correspondence is to be transmitted, how evidence of correspondence is to be retained;
- Who carries out each individual task and where approvals are required, who provides these approvals, where are they recorded, what happens if approval is not provided;
- Where on the case records key decisions in relation to the investigation are to be recorded;
- How relevant material is to be transmitted to the PSAA, how it is to be prepared, who is responsible for carrying out redactions, who is responsible for ensuring that it is transmitted securely
- How communications with both the PMD and the PSAA are to be recorded and where;
- Timelines and sequencing of all of the key activities relating to all stages of CASP.

Recommended Safeguards:

1. The DPO recommends that all feedback comments on the CASP text (CASP Document Suggested Changes) and the CASP Standard Forms and Templates (CASP Standard Letters and Templates Suggested Changes) be implemented.

2. The DPO recommends that CASP TCMS Standard Operating Procedures (SOP) be drafted to support the implementation of the CASP so that all staff are clear at all stages of the process what their role is, who performs what steps, the order of those steps and any escalation points in the process. The benefits of developing and implementing a CASP TCMS SOP are that it would:
    a. Reduce individual employee training time as a written set of guidelines helps ensure that all new hires or new users of the CASP process get the same training, on the same topics and responsibilities, in the same amount of time;
    b. Maintain consistency in relation to the application of the CASP and uniformity in communication;
    c. Reduce errors and avoids risk of guesswork in day-to-day operations and help ensure that all staff understand the processes associated with their particular roles and responsibilities within CASP;
    d. Provide a clear view of the leadership structure and governance model for CASP, particularly important where there are necessarily a number of stages of review and approval as we are mandating in our recommended safeguards in relation to data accuracy, data minimisation and integrity and confidentiality
    e. Transfer work easily, when resources move on or even in cases where they are on leave etc.

3. The DPO recommends that all staff operating the CASP process receive detailed training on both the CASP Data Protection Guidance and the CASP TCMS SOP.

Risk URN	*Risk Category*	*Probability*	*Impact*	*Inherent Risk Rating*	*Residual Risk Rating*	*Target Date of Implementation*
CASP002	*Fairness and Transparency*	*Probable*	*Severe*	*High*	*Low*	*Before CASP go live*

Risk Description:

If CASP data subjects do not receive a comprehensive and clearly communicated data protection notice at the appropriate stages of data processing and employees do not have sufficient guidance on how to provide transparency and information to the data subject in the context of the CASP process, there is a risk that Tusla might be using personal data in any way that is not expected by an individual and which he or she does not know about it which would result in processing that is unfair and will be a breach of data protection legislation.

It is important that all data subjects involved in the CASP process understand what their personal data is being used for and how they can exercise their rights in relation to their personal data.

The DPU has drafted the CASP Data Protection Guidance which contains guidance in sections on lawfulness, fairness and transparency and the requirement to provide information by way of relevant Data Protection Notice to CASP data subjects i.e. the PMD, the PSAA and other individuals involved in the CASP process.

The DPU has drafted Data Protection Notices for PMDs and PSAAs which meets the transparency and fairness requirements of the GDPR and related requirements and a general data protection notice for the CASP process which addresses other data subjects involved in the process including, but not limited to, witnesses, persons to whom allegations of abuse are disclosed, mandated persons, other alleged victims or identified children at risk.

The DPU has also reviewed CASP and notes the requirements throughout CASP to provide and explain the relevant CASP Data Protection Notice at various points in the process in addition to the timetable at section 7 which also mandates the provision of the relevant CASP Data Protection Notices to PMDs, PSAAs and witnesses.

In addition to the above the DPU has reviewed the CASP Standard Forms and Templates which are to be built into TCMS and which are templates which address all correspondence requirements for CASP and which contain standard wording referring to the CASP Data Protection Notice being enclosed.

Recommended Safeguard:
The DPO recommends that the relevant CASP Data Protection Notices be provided to the relevant data subjects at first contact when engaging in the CASP process (detailed instructions are set out in the revised CASP Data Protection Guidance) and as set out in CASP and the CASP Standard Forms and Templates referred to above and the CASP Data Protection Guidance which states that these notices must be provided to the relevant individuals in printed hard copy (if and) when meeting in person, PDF version attached to relevant correspondence transmitted by secure email and printed hard copy enclosed with relevant correspondence by registered post.

Risk URN	*Risk Category*	*Probability*	*Impact*	*Inherent Risk Rating*	*Residual Risk Rating*	*Target Date of Implementation*
CASP003	*Data Accuracy*	*Probable*	*Severe*	*High*	*Low*	*Before CASP go live*

Risk Description:
If Tusla does not ensure that all personal data processed is accurate and, where necessary, kept up to date and that every reasonable step is taken to ensure that personal data that are inaccurate are erased or rectified without delay, there is a significant risk that breaches of personal data and other data protection breaches will occur particularly as procedures for ensuring the accuracy of personal data within the CASP process and a four-eye or second review of documentation and records relating to CASP do not appear to be embedded in the CASP process.

The DPU has drafted the CASP Data Protection Guidance which contains a section on data accuracy including detailed guidance and instructions on when and how to perform a second review (four-eye review) of documentation in CASP.

The DPU has reviewed CASP and notes that it provides the following guidance in relation to the requirement to complete a second review or four eye review before any decision to disclose relevant information and documentation to a PSAA as follows:

"14.6 If it is decided to move to stage 2
The PSAA (and their parents if the PSAA is a child) is entitled to receive all relevant information and documentation gathered up to that point of the assessment. Information is said to be relevant if it discloses a fact or facts(s) which either supports or undermines the disclosure made by the PMD.
The CASP social worker should obtain a second review from their line manager (a four-eye review) of all the information the CASP social worker is considering disclosing to the PSAA. This should happen before any decision is made to move the assessment to stage 2.

Recommended Safeguard:
The DPO recommends that the CASP TCMS SOP incorporate the second review and data accuracy guidance contained in the revised CASP Data Protection Guidance and in particular that the requirement that a four eye or second review of documentation and records be conducted and recorded at the following points in the CASP process:

- Opening a Case Record on TCMS;
- Opening a Person Record for a PSAA on NCCIS;
- Opening a Person Record for a PMD on NCCIS;
- All correspondence with the PMD;
- All correspondence with the PSAA;
- All correspondence with witnesses and third parties;
- Notifications to Relevant Third Parties.

Risk URN	*Risk Category*	*Probability*	*Impact*	*Inherent Risk Rating*	*Residual Risk Rating*	*Target Date of Implementation*
CASP004	*Integrity, Availability and Confidentiality*	*Probable*	*Severe*	*High*	*Low*	*Before CASP Go Live*

Risk Description:
There is a risk that the personal data processed for CASP is processed in a manner that might result in any of the following:

- Accidental or unlawful destruction, loss, alteration, unauthorised disclosure of or access to personal data
- Unjustifiable or unauthorised access, transfer, sharing or publishing of data (this is a particular concern in relation to the CASP process as a significant personal data breach occurred in the past where personal data relating to Complainants was disclosed to a relevant third party in a safeguarding letter who published the letter on social media)
- Lost or stolen data or destruction and alteration of data
- The data is disseminated more than necessary and beyond the control of the data subject
- Inappropriate disclosure of personal data internally within Tusla due to a lack of appropriate controls being in place i.e. breach of least privilege and 'need to know' principles
- The data is modified in such a way that the processing operations have been or could be misused.
- Breach of data held electronically by “hackers”

This risk will manifest itself in CASP if the data lifecycle is not defined and managed rendering it is impossible to say with any certainty that data management and information security controls applied to the processing are adequate and risk appropriate given the nature, context and scope of the processing and in particular given the high-risk nature of the processing of personal data under CASP.

Further risk arises if third parties with whom personal data is shared by Tusla in order to undertake certain activities on behalf of Tusla in relation to CASP, are not risk assessed and managed correctly to ensure that appropriate data sharing agreements and governance are in place with these third parties so that the personal data they process is safeguarded, secured and processed correctly. For the avoidance of any doubt this does not include any disclosures or notifications to relevant third parties required under CASP and refers instead to any repeated sharing of the same data sets with entities outside of Tusla such as a third party engaged on behalf of Tusla to complete any part of the CASP process.

Further risk arises in the potential for the personal data disclosed as part of CASP to be misused for purposes other than that for which they were disclosed (as was the case with a significant breach which formed the basis

for the IN-19-12-8 inquiry). It is the nature of CASP that certain personal data is required to be disclosed to individuals who are subject to the procedure - for example, for fair procedure, the PSAA receives all 'relevant information and documentation' which was relied upon in the substantiation assessment but this information and documentation may contain the personal data, sensitive personal data and special categories of personal data of the PMD and possibly other individuals and relevant third parties will be notified for the purposes of safeguarding where a child is at risk which may disclose certain personal data of the PSAA. In this regard, the DPU has reviewed the CASP Standard Forms and Templates and is pleased to note that:

- warnings are included in any letters to PSAAs on his or her obligations in relation to any personal data that is disclosed to him or her and the sanctions that will be pursued by Tusla in the event of misuse of this data; and
- warnings are included in any notification letters to relevant third parties on their obligations in relation to any personal data that is disclosed to them and the sanctions that will be pursued by Tusla in the event of misuse of this data

The DPU has drafted CASP Data Protection Guidance which contains a section on Integrity and Confidentiality.

Recommended Safeguards:

1. The DPO recommends that a Data Management Plan for CASP be developed and implemented (and I note one is underway) which defines the data lifecycle, data management, governance and security controls to be applied to the data for the duration of its lifecycle and the relevant roles and responsibilities for each activity at each stage of the lifecycle.
2. The DPO recommends that all proposed third party data sharing with external third parties engaged by Tusla are identified and comply with the requirements of the Third Party Data Protection and Privacy Risk Management Policy and Standard Operating Procedures. The Third Party Data Sharing Initiation Form must be completed in respect of each third party engaged by Tusla and, at a minimum, a data sharing agreement entered into between Tusla and each third party. Each data sharing agreement will be drafted by the DPU based on the information provided in the completed form and will be executed by the Information Owner with the relevant third party.

Risk URN	*Risk Category*	*Probability*	*Impact*	*Inherent Risk Rating*	*Residual Risk Rating*	*Target Date of Implementation*
CASP005	*Data Minimisation*	*Probable*	*Severe*	*High*	*Low*	*Before CASP go live*

Risk Description:

There is a risk of unjustifiable or excessive collection, processing or sharing of personal data if Tusla does not ensure that we only collect, process or share the minimum amount of information we need for the purpose of our processing or sharing i.e. that the personal data are adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed or shared. The DPU has a concern in particular that Tusla may not be able to demonstrate that all steps have been taken to minimise the amount of personal data to be shared with the PSAA in order to afford fair procedures and protect the data protection rights and the right of privacy and other fundamental rights of the PMD.

The DPO has drafted CASP Data Protection Guidance which contains a section on data minimization requirements for all staff operating the CASP process and which contains detailed instructions on what personal data to redact and what personal data to disclose in order to balance the rights of fair procedure of the PSAA with the data protection rights and right to privacy of the PMD and other data subjects.

The DPO is pleased to note that section 11 of CASP sets out guidance on the requirement for CASP social workers to have a reasonable basis for requesting information from the PMD based on the CASP social worker's interactions with the PMD. The purpose of this is to prevent excessive collection of non-relevant information during the interview process. Guidance in Section 11 sets out that it may not be necessary or appropriate to look for certain types of sensitive information and the CASP social worker must be aware of this during their engagement with the PMD. Section 11 also provides that when collecting information from the PMD the CASP social worker must make the PMD aware that if the assessment moves to stage 2, any information that the

PMD has furnished will be given to the PSAA (and their parents if the PSAA is a child) if it is relevant to the assessment.

The DPO is also pleased to note that before any decision to disclose 'relevant information and documentation' to a PSAA for the purposes of fair procedures is made, that the CASP Social Worker must obtain a second review of all material he or she proposes to disclose from his or her line manager as follows:
"14.6 If it is decided to move to stage 2
The PSAA (and their parents if the PSAA is a child) is entitled to receive all relevant information and documentation gathered up to that point of the assessment. Information is said to be relevant if it discloses a fact or facts(s) which either supports or undermines the disclosure made by the PMD.
The CASP social worker should obtain a second review from their line manager (a four-eye review) of all the information the CASP social worker is considering disclosing to the PSAA. This should happen before any decision is made to move the assessment to stage 2."

The DPO is further pleased to note having reviewed the CASP Standard Forms and Templates that the initial data protection notification to the PSAA contains no personal data of the PMD and that data pseudonymization measures are in place (replacing real identifiers with [PSAA NCCIS Identifier] and [PMD NCCIS Identifier] and communicating the real identifiers by separate standalone correspondence) to ensure that only the minimum amount of personal data is contained in correspondence and to reduce the risk of a personal data breach should the correspondence be intercepted or transmitted to the wrong recipient.

Address information on letters is automatically mailed merge from the address on TCMS which helps to prevent copy and paste errors or other mistakes when entering addresses on letters. There is, however, an outstanding risk on TCMS standard forms and templates that the mail merge does not pull into the TCMS templates all required personal identifiers from NCCIS but pulls into TCMS instead only the name and address of the recipient and the name of the sender. All dynamic text in the body of each of the TCMS letters which constitutes either personal data in the form of the name of the PMD, PSAA or other and the corresponding NCCIS identifier (e.g. PMD NCCIS Identifier and PSAA NCCIS Identifier) is not pulled or automatically populated from NCCIS on any standard form and template on TCMS and must instead be manually entered by the user each time and for each instance of such dynamic text. This significantly increases the risk of a personal data breach arising as a result of the incorrect name or identifier being manually entered by a user in correspondence.

The DPO has been informed that TCMS will 'force' and record a second review (4-eye) review of all documentation issued from TCMS and that when correspondence is created, the creator (user A) can select an approver (user B) to perform the second review of that correspondence. User B must then accept the task of performing the second review and it is only when this task has been marked as 'complete' on TCMS by User B can User A issue the correspondence. Notwithstanding the data accuracy measures in place in TCMS as referred to above, given the high risk nature of all correspondence relating to CASP, a residual risk remains that personal data breaches may arise from incorrect personal data being manually entered by a user on a template. Tusla has an obligation to seek to mitigate this risk to the fullest extent possible and it is the view of the DPO that this risk will not be mitigated to the fullest extent possible until this outstanding issue on TCMS is remediated.

Recommended Safeguard:

1. The DPO recommends that the outstanding issue on TCMS i.e. that the mail merge does not pull all required personal identifiers from NCCIs but only populates the name and address of the recipient and the name of the sender requiring users to manually input the PMD and PSAA names and NCCIS Identifiers into the body of the relevant template correspondence, be rectified as soon as possible, so that all required personal data can be pulled from NCCIS to populate the relevant TCMS template.
2. The DPO recommends that a quality assurance review be incorporated into the standard Child Protection and Welfare QA audits whereby a selection of CASP substantiation assessment files is reviewed each month to ensure that only material relevant to the substantiation assessment was disclosed to the PSAA in each file and any material disclosed which should not have been disclosed is:
   (a) Reported as a personal data breach and managed in accordance with Tusla's personal data breach procedures; and
   (b) Used as a worked example (anonymised) for process improvement, training and feedback to all CASP staff on how to share personal data safely during the CASP process

3. The DPO recommends that a quality assurance review be incorporated into the standard Child Protection and Welfare QA audits whereby a selection of CASP files is reviewed each month to ensure that where relevant third parties have been notified of child protection concerns that the notification letters do not contain any personal data identifying the PMD and only the minimum required personal data relating to the PSAA in order to ensure a child at risk is protected and any personal data disclosed which should not have been disclosed is:
   (c) Reported as a personal data breach and managed in accordance with Tusla's personal data breach procedures; and
   (d) Used as a worked example (anonymised) for process improvement, training and feedback to all CASP staff on how to share personal data safely during the CASP process

Risk URN	*Risk Category*	*Probability*	*Impact*	*Inherent Risk Rating*	*Residual Risk Rating*	*Target Date of Implementation*
CM006	*Storage Limitation*	*Probable*	*Severe*	*High*	*Low*	*Before CASP go live*

Risk Description:

There is a risk that personal data may be kept longer than required because Tusla does not ensure that personal data are kept in a form which permits identification of data subjects for no longer than is necessary for the purpose(s) of the processing. The DPO notes that while an in perpetuity timeframe applies to certain child care records and personal data, these records and personal data are limited to registers and case records created under Statutory Instruments (SIs) concerning fostering[1] and placement with relatives[2] are required to be held in perpetuity as set out in the table at Appendix 3 and does not apply to all personal data processed as part of CASP and would be concerned, therefore, by any attempt to apply a blanket in perpetuity timeframe to all CASP records and personal data.

The DPO notes the judgement of Barr J in *MQ* v *Gleeson* [1998] 4 IR 85 who stated, in relation to the rights of Tusla to record and disseminate information as to alleged abuse and Tusla's duty arising therefrom to the alleged abuser, the following: "*Arising out of its obligation to investigate allegations of child abuse made to it or of which it becomes aware, [Tusla] is entitled to keep records of such allegations, whether substantiated or not, and, indeed, has an obligation so to do in the interest of professional competence. The only exception which I perceive in that regard would be where on investigation an allegation is found to be positively false. In such circumstances it would be unfair to record the identity of the innocent alleged abuser, although the fact that the Complainant had made a false allegation might itself have subsequent relevance in regard to that person.*" The DPO has a concern in relation to how unfounded allegations are processed by Tusla and notes that, pursuant to section 9 of CASP, regardless of whether the final conclusion is that an allegation is 'founded' or 'unfounded' copies of all documentation, together with details of the allegations and the record of the substantiation assessment and decisions, must be included in the PSAA record.

The DPO has drafted the CASP Data Protection Guidance which contains detailed guidance on steps staff must take to comply with storage limitation requirements.

Recommended Safeguards:

The DPO notes that significant work is being undertaken in a review of the Records Management Policy and that a new policy is in development along with Records Management Best Practice Guidance, a revised Record Retention Schedule and an implementation plan to give operational effect to these documents in addition to the establishment of a Records Management Office as a new corporate function in Tusla.

The DPO recommends that:

- all retention periods for any personal data processed under CASP be reviewed to ensure that data is retained for only the minimum duration necessary to meet retention requirements as determined by legal obligations and service needs and that the retention period is objectively linked to the purpose for processing of that data
- retention periods for personal data relating to unfounded allegations must take into account the judgment of Barr J in *MQ v Gleeson* referred to above and consideration should be given as to

[1] SI 260/1995, regulations 13 and 14
[2] SI 261/1995, regulations 12 and 13

whether, on final conclusion that an allegation is unfounded and taking into account any period for review, the PSAA's entire record should be anonymised in those instances where an allegation is found to be positively false.

- the retention schedule items are sufficiently granular to assure necessity and proportionality in relation to retention
- personal data relating to children in care records and registers which must be held in perpetuity be distinguished from all other personal data related to CASP which is not required to be held in perpetuity for purposes of applying the correct retention periods to that data
- there are sufficient safeguards to retain records securely when they are no longer active but must be retained
- there is distinct access control for inactive retained records and long-term archive
- that controls are implemented to provide for the secure deletion and destruction of data once retention periods have expired i.e. that personal data is put beyond use
- that controls are implemented for regular review of personal data held in relation to CASP for compliance with retention timeframes

Risk URN	*Risk Category*	*Probability*	*Impact*	*Inherent Risk Rating*	*Residual Risk Rating*	*Target Date of Implementation*
CASP007	*Preventing Data Subjects from Exercising Control over Their Personal Data*	*Probable*	*Severe*	*High*	*Low*	*Before CASP go live*

Risk Description:

There is a risk of preventing data subjects from exercising control over their personal data if Tusla employees are not aware of how to uphold the rights and freedoms of data subjects as they apply to CASP, are not able to explain these rights to data subjects as required and data subjects are not aware of their rights, how they may assert them, and how restrictions may apply to these rights in relation to CASP. A further risk arises if all personal data relating to CASP cannot be readily located, isolated, retrieved, amended and deleted as required to facilitate data subject rights.

The DPO has drafted the CASP Data Protection Guidance which contains sections on lawfulness, fairness and transparency, and data subject rights management and contains important information on data subject rights, how this information is to be communicated to data subjects through the relevant Data Protection Notice and how these rights can be facilitated

Recommended Safeguards:

1. The DPO recommends that TCMS be reviewed and enhanced if required with data subject rights management features i.e. the ability to locate, isolate, retrieve, restrict, amend, delete data as required in order to facilitate data subject rights for PMDs, PSAAs and all other data subjects whose personal data is processed as part of CASP.
2. The DPO recommends that all personal data relating to CASP be classified, indexed and archived in compliance with the Records Management Policy and Best Practice Guidance to ensure that it is capable of location and retrieval as required to facilitate the exercise of data subject rights as required.

Risk URN	*Risk Category*	*Probability*	*Impact*	*Inherent Risk Rating*	*Residual Risk Rating*	*Target Date of Implementation*
CASP008	*Harm to the Data Subject*	*Probable*	*Severe*	*High*	*Low*	*Before CASP go live*

Risk Description:

There is a risk that processing and in particular, unauthorised disclosure or inappropriate access to, personal data, may result in psychological bodily harm, loss of liberty or freedom of movement of a data subject where for example his or her location or whereabouts is revealed to someone which might put them in danger. The DPU is particularly concerned with any disclosure which results in revealing the identity or location of the PMD to the PSAA without appropriate safeguards in place or indeed the PSAA to relevant third parties again without appropriate safeguards in place.

The DPO has reviewed CASP with the above risk in mind and is pleased to note the following:

1. Before any decision to disclose relevant information and documentation to the PSAA is made, the relevant information and documentation is provided to the PMD who is given an opportunity to review and raise any objection to the disclosure which the CASP Social Worker must take into account;
2. Steps have been taken to minimise the disclosure of personal data in correspondence through the use of pseudonymisation in the CASP Standard Forms and Templates:
3. Before any decision to disclose 'relevant information and documentation' to a PSAA for the purposes of fair procedures is made, that the CASP Social Worker must obtain a second review of all material he or she proposes to disclose from his or her line manager;

4. Warnings are included in any letters to PSAAs on his or her obligations in relation to any personal data that is disclosed to him or her and the sanctions that will be pursued by Tusla in the event of misuse of this data; and
5. Warnings are included in any notification letters to relevant third parties on their obligations in relation to any personal data that is disclosed to them and the sanctions that will be pursued by Tusla in the event of misuse of this data
6. Provision is made in CASP for situations where it is established that a PMD or a witness is afraid to come forward because of fear of reprisal should the PSAA become aware that they have made a disclosure of abuse and agreement should be sought from the PMD or the witness to contact An Garda Síochána with a view to establishing an APMD safety plan to secure their protection;
7. A child PMD or PSAA may be accompanied by a parent or other responsible adult in any interviews pertaining to the substantiation assessment
8. An Adult PMD may be accompanied by a support person in any interview pertaining to the substantiation assessment.
9. A PSAA may be accompanied by a support person in any interview pertaining to the substantiation assessment.
10. Reference to the term 'stress-testing or cross-examination' has been removed from CASP and instead the CASP Social Worker is required to perform a 'reliability and accuracy check' of allegations;
11. Provision is made in CASP for where a PMD (and/or their parents if the PMD is a child) has requested anonymity from Tusla or advised Tusla that they do not want contact with An Garda Síochána, Tusla is still obliged to notify An Garda Síochána where it suspects that a crime has been committed or a child has been wilfully neglected or physically or sexually abused. However, Tusla will inform An Garda Síochána of the PMD's requests for anonymity and wish not to be contacted by An Garda Síochána.
12. Guidance is provided in CASP about the requirement for CASP social workers to have a reasonable basis for requesting information from the PMD based on the CASP social worker's interactions with the PMD to prevent excessive collection of non-relevant information during the interview process..
13. CASP provides that at the CASP Preliminary Enquiries stage the CASP Social Worker when engaging with the PMD must advise the PMD that:
    a) they are not obliged to engage with Tusla regarding a substantiation assessment.
    b) if they choose not to engage their information will not, in the normal course of events, be released to the PSAA; except in circumstances where Tusla must act to protect a child and so has to engage with a PSAA. In these circumstances, in line with Tusla's statutory duties and function and fair procedures obligations, Tusla will be obliged to share information with the PSAA relevant to the allegations made.
    c) they can bring a support person with them to the formal interview and any subsequent meetings, explain that if they choose to bring a support person, fair procedures require the PSAA (and/or their parents if the PSAA is a child) to know of this however the support person's name would not be disclosed to the PSAA;
    d) they do not have to provide detail or information about their disclosure at this meeting.
    e) If required, the PMD should be provided with a reasonable amount of time to decide if they wish to provide details of their disclosure. If the PMD does not require any extra time to make their decision the CASP Social Worker should seek to establish the main facts of what is being disclosed.
14. CASP provides that due consideration should be given to any potential harm for a PMD of the release of any relevant information and documentation to a PSAA, mindful of the fact that relevant information can only be withheld from PSAA in stage 2 in extremely limited circumstances. This consideration should take the form of a discussion with the PMD.
15. Provision is made in CASP for ensuring that the PMD has the opportunity to access appropriate support with an instruction that the PMD should be signposted towards local, regional and/or National therapeutic services that may be of assistance to the PMD.
16. CASP provides in relation to the actions at the end of Stage 1:
    a) The PMD (or parents of a child PMD) should be given the opportunity to raise objections to the sharing of their information
    b) Consideration should be given to any potential harm for a PMD of the release of any relevant information and documentation to a PSAA (and/or their parents if the PSAA is a child).

Relevant information can only be withheld from PSAA in stage 2 in extremely limited circumstances where there is a clear and continuing risk of harm to an identified person.

c) In exceptional cases, where there is a concern that there is a serious risk of harm posed to a PMD by the release of information to the PSAA (and/or their parents if the PSAA is a child), Tusla will consider such risk with a view to determining if it is appropriate to disclose relevant information and documentation to a PSAA.

d) Given the nature of issues involved, such a withholding could only be justified in the most extreme of cases and where the information is withheld to the least extent possible.

e) In such circumstances any decision to withhold relevant information and documentation would have to be kept constantly under review and be reactive to any information that suggests that any initial perception of risk of serious harm is no longer accurate.

17. Guidance is provided at section 17 of CASP for those instances where the PSAA asks to have questions put to a PMD or a witness;
18. Contained within the guidance provided at section 18.2 of CASP on "**Factors to consider in reaching a founded or unfounded finding"** is:
"18.2.1 The need to be trauma aware
The CASP social worker should be aware of the range of a person's possible responses to physical, emotional, sexual abuse and neglect. People who have experienced abuse can present with certain signs of trauma which the CASP social worker must consider in their assessment of the allegation.
The CASP social worker should consider if there is a pattern, or history of behaviours and presentations that may be linked to a person's experience of abuse and or neglect. Whilst these presentations and behaviours may indicate that the PMD experienced abuse, these factors alone, would not be sufficient to reach a founded outcome."

Recommended Safeguard:

1. While the DPO is mindful of the requirements relating to fair procedures, the DPO has a particular concern with the disclosure of location data or contact details of the PMD to the PSAA as a significant breach in the past where this information was disclosed to a PSAA resulted in sustained harassment of the PMD by the PSAA and the requirement for Tusla to work with local authorities to rehouse the PMD. The DPO recommends, therefore, that the PMD's contact details are never disclosed to the PSAA and, has included detailed instructions on steps to be followed when considering the disclosure of the PMD's address in the CASP Data Protection Guidance as follows:
"PMD's Address - Redact - Rationale
May not be required for fair procedures and potential for significant risk of harm to PMD if this information is disclosed. If the particular circumstances of a substantiation assessment are such that the CASP Social Worker considers it is necessary to disclose this information in order for the PSAA to properly respond to an allegation, the CASP Social Worker must (as set out in CASP) provide the information proposed to be disclosed to the PMD and afford the PMD the opportunity to object to the disclosure. If the PMD objects to this information being disclosed to the PSAA, the CASP Social Worker must refer the matter to a CASP Lead for decision who in turn may consult with Tusla Office of Legal Services as required. If the PMD raises objections on the grounds of concern for his or her safety, the CASP Social Worker should seek permission from the PMD to engage with AGS with a view to AGS establishing an APMD safety plan for his or her protection."

2. The DPO recommends that all training relating to CASP reinforce these requirements and the important of protecting the identity and location of the PMD, the PSAA and other data subjects to the fullest extent possible and ensuring that only the minimum information required to be disclosed in order to ensure fair procedures and to complete a substantiation assessment is disclosed. We have included detailed guidance on data minimisation and redaction in the revised CASP Data Protection Guidance for this purpose.

Observations:
The DPO during the course of completing this DPIA has a number of observations which we consider though not data protection risks per se would be remiss of us not to document in this DPIA as it may helpful for Tusla senior management to take these observations into account before CASP goes live.

Tusla's Legal Basis for Processing under section 3 of the Child Care Act 1991

In order for Tusla to process any personal data of its Service Users and other data, Tusla must have a statutory basis for processing that personal data. This means that Tusla's statutory obligations must permit or require the processing of personal data. Much, if not most, of Tusla's processing is grounded on section 3 of the Child Care Act 1991 i.e. Tusla asserts that section 3 permits and requires the processing of personal data in order for Tusla to carry out its functions under section 3 and in relation to CASP.

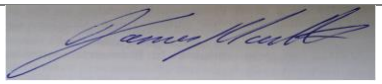
The DPO is of the view that any apparent uncertainty as to Tusla's obligations are under section 3 may undermine Tusla's position regarding section 3 and its ability to assert a lawful basis for processing of personal data relating to section 3. This coupled with the fact that obligations, which either emerge or are clarified by case law, are onerous for Tusla and have far reaching implications for parties to the CASP process, namely PMDs and PSAAs, are not accompanied by supporting statutory powers, is not satisfactory for any party involved in the CASP process. It is important that Tusla has certainty when asserting a lawful basis for processing under data protection legislation as this is the point of departure for both Tusla as data controller to comprehend its data protection obligations and for data subjects to assert their individual rights.

Because Tusla places so much reliance on section 3 it would be helpful for Tusla if the boundaries of section 3 were clearly set out and that any legal obligations imposed by section 3 on Tusla were accompanied by clear legal powers to carry out these legal obligations so that when Tusla asserts section 3 as a statutory basis for processing this basis will not be subject to challenge and no ambiguity remains as to the extent of the requirements or permissions set out under section 3.

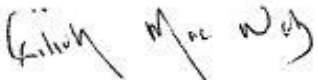
Furthermore, given the significant concerns raised by various stakeholders in relation to section 3 (as set out in the Stage 1 template) it would be prudent for Tusla senior management to consider that the implementation of CASP might result in a loss of social trust in Tusla particularly if the views of data subjects and other relevant stakeholders are not taken into account before CASP is implemented, if PMDs are deterred from engaging with Tusla because of their experience throughout the CASP process or if prospective PMDs s are deterred because of their perceptions of CASP.

It might be helpful, therefore, for Tusla senior management to continue to engage with the Department of Children, Equality, Disability, Integration and Youth (DCEDIY) to lobby for legislative change which would codify the requirements to undertake investigations pursuant to section 3 and which would arm the investigating body undertaking such investigations with the powers to conduct them in a manner which would ensure the state's compliance with the ECHR, reduce the risk of legal challenge to any decisions arising from the CASP process and importantly transpose the requirements of the EU Victims Directive to the CASP process in order to provide appropriate supports to PMDs throughout the process. It may also be helpful for Tusla senior management and the DCEDIY to consider carefully whether, in fact, Tusla is best placed to conduct these investigations given the statutory role of Tusla in child protection and welfare in the state and the requirement for such investigations to be conducted impartially and by investigators who are suitably qualified to discharge fair procedures and balance the rights of the PSAA and the PMD.

Data Protection Officer Approval

I agree with the risks identified above along with the assessment of these risks and approve the proposed safeguards to mitigate these risks or propose the following amendments (state whether approved in full or approved subject to amendments)	Approved in full.
DPO's Signature	
Date of Approval	11 March 2022

Information Owner Acceptance

I agree with proposed safeguards to mitigate these risks or propose the following amendments (state whether approved in full or approved subject to amendments)	Approved in full.
Information Owner's Signature	
Date of Agreement	14th March 2022

Appendix 1 - Data Protection Impact Assessment Risk Taxonomy	
Risk Category	**Risk Definition**
Lawful Processing Risk	There is a risk that Tusla has not identified a lawful reason for processing personal data and that Tusla does not have a statutory function or legal duty which allows Tusla to process and collect this personal data. There is a risk that the purpose for collecting and using the personal data is not supported by a legal power or duty (for example, Tusla may be required or permitted to collect personal data of Service Users because it needs this data to provide services to service users) or that the personal data collected is not necessary and proportionate for the purpose and that Tusla cannot assert a lawful basis for this processing under GDPR or that the lawful basis asserted is incorrect rendering the processing unlawful and illegal.
Fairness and Transparency Risk	1. There is a risk that Tusla might be using personal data in any way that is not expected by an individual and which he or she does not know about it which would result in processing that is unfair and will be a breach of data protection legislation and includes inappropriate use or misuse of data including: • use of data beyond individuals' reasonable expectations • unusual use of data beyond societal norms • where any reasonable individual in this context would object 2. There is a risk that Tusla does not process personal data in a way that is transparent to Service Users and other data subjects. Tusla has a standard overarching privacy notice which explains how we use information generally. If this does not cover new uses of information set out in this process, Tusla will need to give data subjects a new privacy notice and if information is not provided we may not meet transparency requirements.
Purpose Limitation Risk	There is a risk that personal data are not collected for specified, explicit and legitimate purpose and not further processed in an incompatible manner and that "Function creep" occurs, where a purpose for which the personal data was obtained is gradually widened or blurred and the data is used for a purpose other than those planned.
Data Minimisation Risk	There is a risk of unjustifiable or excessive collection, processing or sharing of personal data if Tusla does not ensure that we only collect, process or share the minimum amount of information we need for the purpose of our processing or sharing i.e. that the personal data are adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed or shared. Merging of datasets may result in a data controller having far more information about individuals than anticipated by the individuals. "
Data Accuracy Risk	There is a risk of use or storage of inaccurate or outdated data if Tusla does not ensure that all personal data that we process is accurate and, where necessary, kept up to date and that every reasonable step is taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay. Personal data are inaccurate if they are incorrect or misleading as to any matter of fact.
Storage Limitation Risk	1. There is a risk that personal data may be kept longer than required in the absence of appropriate policies because Tusla does not ensure that personal data are kept in a form which permits identification of data

	subjects for no longer than is necessary for the purpose(s) of the processing. 2. There is a risk that retention criteria applied to the personal data failed to take into account fulfilling any legal/statutory retention requirements or identifying business or service needs for retention from experience. 3. There is a risk that after the retention period has expired and Tusla is no longer allowed to keep the data it does not delete the data securely or put deleted data beyond use.
Integrity Availability and Confidentiality Risk	1. There is a risk that failure to ensure adequate arrangements are in place in relation to the sharing of personal data whether with other controllers, processors or as part of a joint controllership arrangement will result in a risk to the integrity and confidentiality of that data. 2. There is a risk that the data is processed in a manner that does not ensure appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures ('integrity and confidentiality') which may result in any of the following: • Accidental or unlawful destruction, loss, alteration, unauthorised disclosure of or access to personal data • The data is seen by an unauthorised person. • Unjustifiable or unauthorised access, transfer, sharing or publishing of data • Lost or stolen data or destruction and alteration of data The data is copied and saved to another location. • The data is disseminated more than necessary and beyond the control of the data subject. • Inappropriate disclosure of personal data internally within Tusla due to a lack of appropriate controls being in place i.e. breach of least privilege and 'need to know' principles. • The data is modified in such a way that the processing operations have been or could be misused. • Breach of data held electronically by "hackers" • Information released in anonymised form might lead to disclosure of personal data if anonymisation techniques chosen turn out not to be effective. • Accidental loss of electronic equipment by personnel may lead to risk of disclosure of personal information to third parties. • Loss of confidentiality of personal data protected by professional secrecy or duty of confidentiality (Tusla owes this duty to its Service Users) in most instances • Merging of datasets may inadvertently allow individuals to be identified from anonymised data.
Accountability Risk	There is a risk of failure to adequately demonstrate and evidence compliance will result in a breach of the Accountability Principle. There is a risk of failure to comply with the GDPR which may result in investigation, administrative fines, prosecution, or other sanctions. There is a risk that failure to live up to stakeholder expectations regarding privacy and personal data are likely to cause reputational risk and that any harm caused to individuals by reason of mishandling of personal data may lead to claims for compensation.
Risk to the Right to Privacy	There is a risk that Tusla fails to comply with section 3 of the European Convention on Human Rights Act 2003 and does not perform its functions in a manner compatible with the State's obligations under the Convention provisions and that the processing is not 'necessary' and constitutes an unacceptable intrusion into private life or an unjustifiable interference with the right to privacy which Tusla cannot objectively defend.

Risk to the Right to a Fair Trial and Fair Procedures	There is a risk that Tusla fails to comply with section 3 of the European Convention on Human Rights Act 2003 and does not perform its functions in a manner compatible with the State's obligations under the Convention provisions and that the processing interferes with or undermines an individual's right to a fair trial or fair procedures which Tusla cannot objectively defend.
Risk to Right to Freedom of Expression or Association	There is a risk that Tusla fails to comply with section 3 of the European Convention on Human Rights Act 2003 and does not perform its functions in a manner compatible with the State's obligations under the Convention provisions resulting in detriment arising from monitoring or exposure of identity, characteristics, activity, associations or opinions or a chilling effect on freedom of speech, association which Tusla cannot objectively defend.
Risk of Discrimination or Damage to Reputation	Where personal data are processed which reveal racial or ethnic origin, political opinions, religion or philosophical beliefs, trade union membership, and the processing of genetic data, data concerning health or data concerning sex life or criminal convictions and offences or related security measures and such data is compromised or processed unfairly. Where personal aspects are evaluated, in particular analysing or predicting aspects concerning performance at work, economic situation, health, personal preferences or interests, reliability or behaviour, location or movements, in order to create or use personal profiles which if created unfairly may lead to discrimination or any other significant economic or social disadvantage;
Risk of Identity Theft, Fraud or Financial Loss	There is a risk that unauthorised disclosure or inappropriate access to personal data may result in identity theft or fraud to the data subject which might result in financial loss to the data subject.
Risk of Preventing Data Subjects from Exercising Control over their personal data	There is a risk of preventing data subjects from exercising control over their personal data where personal aspects are evaluated, in particular analysing or predicting aspects concerning performance at work, economic situation, health, personal preferences or interests, reliability or behaviour, location or movements, in order to create or use personal profiles which if created unfairly may lead to loss of autonomy or inappropriate curtailing of personal choice. There is a risk of preventing data subjects from exercising control over their personal data where data may be transferred to countries with inadequate data protection regimes. There is a risk of preventing data subjects from exercising control over their personal data if processes are not in place to ensure that files and personal data can be retrieved quickly to comply with access and other data subject rights requests.
Risk of Psychological Harm	There is a risk that processing, and in particular, unauthorised disclosure or inappropriate access to, personal data, may result in personal, family, workplace or social fear, embarrassment, apprehension or anxiety.
Risk of Physical Harm	There is a risk that processing and in particular, unauthorised disclosure or inappropriate access to, personal data, may result in bodily harm, loss of liberty or freedom of movement of a data subject where for example his or her location or whereabouts is revealed to someone which might put them in danger.
Risk of Societal Harm	There is a risk that the processing may cause societal harm due to a loss of social trust in Tusla and/or damage to democratic institutions, for example excessive state or police power.

Appendix 2 - Data Protection Impact Assessment Risk Probability and Impact Grid

Probability Impact Grid (PIG) and Risk Scoring Criteria

PROBABILITY					
Greater than to 90% chance of occurance. r	90%	Probable	Medium	High	High
Up to 50% chance of occurrence	50%	Possible	Low	Medium	High
Up to 10% chance of occurance.	10%	Remote	Low	Low	Medium
			Minimal	Significant	Severe
		Service User	Contains no sensitive data but a minor amount of personal data of limited number of Service Users in very limited geographical areas that if disclosed inappropriately would not cause harm to Service Users or other individuals.	Contains moderate amount of sensitive personal data that if disclosed in appropriately would cause some harm to Service Users; geographical location limited; quantities limited;	Where personal data of vulnerable natural persons, in particular of children, are processed; or where processing involves a large amount of personal data and affects a large number of data subjects any unauthorised disclosure of such data would cause significant harm to data subjects
		Regulatory	No breach of GDPR but breaches an internal policy	Breach of GDPR but no breach of GDPR principles	Breaches a principle of the GDPR
		Reputational	Minor damage to Tusla's reputation that may result in minor disruption to operations Isolated adverse media coverage with limited consequential effects	Limited damage to Tusla's reputation that may result in moderate disruption of operations Service User satisfaction and/or confidence is moderately impaired Negative media coverage that has a moderate impact on reputation	Tusla's reputation is significantly damaged that results in extremely significant disruption of operations May lead to significant impairment of High profile and/or long term negative media coverage that has a sustained impact on reputation
				IMPACT	

Appendix 3 – Table of Requirements Case Records and Registers

Statutory Instrument	Prescribed Contents of Case Record	Prescribed Contents of Register
S.I. No. 260/1995 - Child Care (Placement of Children in Foster Care) Regulations, 1995	(2) A case record of a foster child shall include such of the following documents as are available to the health board— (a) medical and social reports on the child, including background information on the child's family, (b) a copy of any court order relating to the child or of parental consent to the child's admission to the care of the board, as appropriate, (c) the birth certificate of the child, (d) a copy of the contract between the board and the foster parents, (e) a copy of the plan for the care and upbringing of the child prepared by the board under article 11 of these Regulations, f) reports on the child's progress at school, where applicable, (g) a note of every visit to the child and the foster parents in accordance with article 17 of these Regulations, (h) a note of every review of the child's case pursuant to article 18, 19 or 20 of these Regulations, together with particulars of any action taken as a result of such review, and (i) a note of every significant event affecting the child.	(2) An entry in the register with respect to a foster child shall include such of the following particulars as are available to the health board— (a) the name, sex and date of birth of the child, (b) the names and address of the parents of the child, (c) the names and address of the foster parents with whom the child has been placed, (d) the date of placement, and (e) where the child ceases to be placed with those foster parents, the date on which the placement ceased.
S.I. No. 261/1995 - Child Care (Placement of Children With Relatives) Regulations, 1995	(2) A case record of a child placed with relatives shall include such of the following documents as are available to the health board— (a) medical and social reports on the child, including background information on the child's family, (b) a copy of any court order relating to the child or of parental consent to the child's admission to the care of the board, as appropriate, (c) the birth certificate of the child, (d) a copy of the contract between the board and the relatives, (e) a copy of the plan for the care and upbringing of the child prepared by the board under article 11 of these Regulations,	An entry in the register with respect to a child placed with relatives shall include such of the following particulars as are available to the health board— (a) the name, sex and date of birth of the child, (b) the names and address of the parents of the child, (c) the names and address of the relatives with whom the child has been placed, (d) the date of placement, and (e) where the child ceases to be placed with those relatives, the date on which the placement ceased. (3) Every change in the particulars entered in the register with respect to

Statutory Instrument	Prescribed Contents of Case Record	Prescribed Contents of Register
	(f) reports on the child's progress at school, where applicable (g) a note of every visit to the child and the relatives in accordance with article 17 of these Regulations (h) a note of every review of the child's case pursuant to article 18, 19 or 20 of these Regulations, together with particulars of any action taken as a result of such review, and (i) a note of every significant event affecting the child.	a child placed with relatives shall be recorded in the register.