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

Data Protection Notice

CASP Person Making a Disclosure (PMD)

How we protect and manage your personal data

www.tusla.ie

1. What is a Data Protection Notice?

The Child and Family Agency, Tusla ('we' 'our' 'us') strongly believes in protecting the confidentiality and security of your personal data. This document is referred to as our 'CASP Data Protection Notice" or throughout this document "Data Protection Notice" and describes how we use the personal data that we collect and receive about you.

A Person Making a Disclosure (PMD) is defined in CASP a person – either a child or an adult – who has made a disclosure of child abuse.

All references to 'you' in this document are intended to refer to a PMD or the parent of a PMD (if the PMD is a child). References to parent include a child's legal guardian and in the case of a child in care may include Tusla.

This Data Protection Notice contains some terms which you may need help understanding. The most commonly used terms are listed in the Glossary at the end of our Data Protection Notice.

2. Who We Are

The Child and Family Agency, Tusla, is a statutory body established under the Child and Family Agency Act 2013. Tusla is required under section 3 of the Child Care Act 1991 (as amended) to promote the welfare of both identified and identifiable children in its area who are not receiving adequate care and protection. This requires Tusla to take all reasonable steps to investigate a notification, referral or disclosure of child abuse before sharing information with third parties to safeguard children from risk while ensuring that the person the subject of abuse allegations (PSAA) which is defined in CASP as a person – either a child or an adult – who has had allegations of child abuse made against them, is afforded fair procedures.

The Child Abuse Substantiation Procedure (CASP) is the process and steps involved in Tusla's assessment of disclosures of child abuse, where Tusla may need to inform a relevant third party of a potential risk to children. Examples of relevant third parties include parents, family members, employers and community organisations.

We are the **Controller** of your personal data as we decide what information to collect about you and what we will use it for in order to discharge our statutory responsibilities in relation to CASP.

3. How to Contact Us for Help

If you want help with our Data Protection Notice or have questions about it, please contact the Child and Family Agency's Data Protection Officer whose contact details are below:

Telephone:	+353 1 771 8500
Email:	datacontroller@tusla.ie
Post:	Tusla, Brunel Building, Heuston South Quarter, St John's Road W, Kilmainham, Dublin, Ireland

If you are unhappy about any aspect of the way we collect, share or use your personal data, we would like you to tell us. You can contact us using the details above. You can make a data subject rights request using our **Data Subject Rights Request Portal**

If you are not happy with our response, you have a right to complain to the

Data Protection Commission
21 Fitzwilliam Square South
Dublin 2
D02 RD28
Ireland
www.dataprotection.ie
https://forms.dataprotection.ie/contact

4. Your Rights

We have set out a summary of your rights regarding your personal data below. This section explains your rights in relation to your personal data in detail. The various rights are not absolute and are subject to certain exceptions or qualifications.

Your Right	This may include:
The right to be informed	You have the right to be provided with clear, transparent and easily understandable information about how we use your personal data and your rights. This is why we're providing you with the information in this Data Protection Notice.
The right of access	You have the right to obtain access to your **personal data** (if we're **processing** it), and other certain information (similar to that provided in this Privacy Notice). This is so you're aware and can check that we're using your **personal data** in accordance with data protection law. **What can you request access to?** You have the right to: – receive confirmation from us that your **personal data** is being processed; – receive confirmation from us about the type of information we hold about you, why we use it, what we use it for and information about your privacy rights (all of this is included in this Data Protection Notice); and – access to your information. You can request copies of paper and electronic records (including recorded calls, where applicable) about you that we hold, share or use. To deal with your request, we can request proof of identity and enough personal data to enable us to locate the personal data you request. **When will access not be provided?** We can only provide you with your information, not personal data about another person. Also, where access would adversely affect another person's rights, we are not required to provide this. Due to legal privilege, we may not be able to show you everything that we learned in connection with a claim or legal proceeding. Please clearly set out in your access request the personal data that you're requesting. If this is not clear, we may come back to you to ask for further personal data by way of clarification.

Your Right	This may include:
The right to rectification	You're entitled to have your personal data corrected if it's inaccurate or incomplete. **Correcting your Information** You have the right to obtain from us without undue delay the correction of inaccurate personal data concerning you. If you tell us that the personal data we hold on you is incorrect, we will review it and if we agree with you, we will correct our records. If we do not agree with you, we will let you know. If you wish, you can tell us in writing that you believe our records still to be incorrect and we will include your statement when we give your personal data to anyone outside the Child and Family Agency. You can contact us using the details in the section at the beginning of the Data Protection Notice headed **'How to Contact Us for Help'**. You may also have the right to have incomplete personal data completed, including by means of providing a supplementary statement. Whether or not this is appropriate in any particular case depending on the purposes for which your personal data is being processed. We need to notify any third parties with whom we have shared your personal data that you've made a rectification request. We will take reasonable steps to do this, but if it is not possible or may involve disproportionate effort we may not be able to do this or ensure they rectify the personal data they hold. **How You Can See and Correct Your Information** Generally, we will let you see the personal data that we hold about you, or take steps to correct any inaccurate information, if you ask us in writing. Due to legal privilege, we may not be able to show you everything that we learned in connection with a claim or legal proceedings.

Your Right	This may include:
The right to erasure	This is also known as 'the right to be forgotten' and enables you to request the deletion or removal of your personal data where there's no compelling reason for us to keep using it. This is not an absolute right to erasure. We may have a right or obligation to retain the information, such as where we are under a legal obligation to do so or have another valid legal reason to retain it. **When can you request erasure?** Subject to the section below you have a right to have your personal data erased, and to prevent processing, where: - the personal data is no longer necessary for the purpose it was originally collected/processed; - we have been processing your personal data in breach of data protection laws; or - the personal data has to be erased in order to comply with a legal obligation **When can we refuse erasure requests?** The right to erasure does not apply where your information is processed for certain specified reasons, including for the exercise or defence of legal claims or to allow us to administer and manage our employment relationship. **Do we have to tell other recipients of your personal data about erasure requests?** Where we have provided the personal data you want to be erased to third parties, we need to inform them about your erasure request, so they can erase the personal data in question. We will take reasonable steps to do this, but this may not always be possible or may involve disproportionate effort. It may also be that the recipient is not required/able to erase your personal data because one of the exemptions above applies.

Your Right	This may include:
The right to restrict processing	In certain situations, you have the right to 'block' or suppress further use of your information. When processing is restricted, we can still store your information, but may not use it further. When is restriction available? You have the right to restrict the processing of your personal data: – where you disagree with the accuracy of the information, we need to restrict the processing until we have verified the accuracy of the information; – when processing is unlawful and you oppose erasure and request restriction instead; – if we no longer need the personal data but you need this to establish, exercise or defend a legal claim; or – where you have objected to the processing in the circumstances detailed in paragraph (a) of Objecting to processing below, and we are considering whether those interests should take priority. **Do we have to tell other recipients of your personal data about the restriction?** Where we have disclosed your relevant personal data to third parties, we need to inform them about the restriction on the processing of your information, so that they don't continue to process this. We will take reasonable steps to do this, but this may not always be possible or may involve disproportionate effort. We'll also let you know if we decide to lift a restriction on processing.
The right to object	You have the right to object to certain types of processing of your personal data. If you object to the processing of your personal data in relation to CASP we will review your objection in the context of the personal data we process about you. If we consider that we can demonstrate compelling legitimate grounds for the processing which may override your individual objection we may continue to process your personal data despite your objection. If we feel we cannot demonstrate compelling legitimate grounds for the processing, we will stop processing your personal data. We will continue to process your personal data where it is necessary for research and statistical purposes carried out in the public interest as the right to object does not apply in this instance.

Further information and advice about your rights can be obtained from the Data Protection Commission, 21 Fitzwilliam Square South, Dublin 2, D02 RD28, Ireland, or on its website at **www.dataprotection.ie.**

You are entitled to receive your personal data free of charge except where we may charge a reasonable fee to cover our administrative costs of providing the personal data for manifestly unfounded or excessive/repeated requests, or further copies of the same information.

Alternatively, we may be entitled to refuse to act on the request. Please consider your request responsibly before submitting it. We will respond as soon as we can. Generally, this will be within one month from when we receive your request but, if the request is going to take longer to deal with, we will let you know. In order to exercise any of the rights described below please contact us using the details in the section at the beginning of the Data Protection Notice headed **'How to Contact Us for Help'**

5. What personal data do we process?

Description	This may include
Identification Information	First name(s), maiden name and surname, age, date and place of birth, gender, marital status, number of dependents, language of communication, nationality, citizenship.
Physical Characteristics and Location Information	Contact Details, Address, Physical Description
Family, Lifestyle and Social Circumstances Information	Information relating to family, lifestyle and social circumstances, family and other household members, housing and travel
Criminal Convictions	Information relating to criminal convictions, offences or alleged offences
Special categories of information	Information classified by law as **"special categories of personal data"** including information about health, medical records, sexual history or sex life, racial and/or ethnic origin, religion and religious beliefs

6. How do we collect this personal data?

We collect and process personal data relating to disclosures of child abuse and offences against children from you directly, from mandated persons and from other sources including members of the public who are not mandated persons (non-mandated persons).

The Children First Act 2015 (the 2015 Act) requires certain specified categories of persons, known as "mandated persons", to report child protection concerns to Tusla using a mandated report form. This applies where the person knows, believes or has reasonable grounds to suspect that a child is being harmed, has been harmed or is at risk of being harmed, or where the child makes such a disclosure.

A notification, referral or disclosure of child abuse may come from outside of Tusla from the following parties which initiates the standard child protection and welfare process:

- A referral from a mandated person
- A referral from a non-mandated person
- A notification from An Garda Síochána
- A disclosure from a PMD (child)
- A disclosure made on behalf of a PMD by a parent/guardian or other party (child)
- A retrospective disclosure from a PMD (adult)
- A disclosure made on behalf of a PMD by another individual (adult)

An internal referral may arise from a child protection and welfare case being processed in Tusla.

After the initial notification, referral or disclosure, Tusla may collect more personal data from:

- You or a person representing you who may provide further data on request or of your own initiative;
- The PSAA who may provide further data on request or of his or her own initiative
- An Garda Síochána, the Health Services Executive, medical practitioners;
- Tusla Child Protection and Welfare sources;
- Third parties identified by either you or the PSAA as witnesses.

7. How will we use your personal data?

We may use the information we have about you for the following purposes:

Why We Use Your Personal Data:	What this means:
Notifying Relevant Third Parties	Tusla must consider if there is an immediate risk to children, and we take immediate and appropriate action to protect any child in this situation. This may involve notifying relevant third parties about child protection concerns during the substantiation assessment if an immediate serious risk is identified without informing the PSAA beforehand. Tusla will notify relevant third parties and at the end of the substantiation assessment if there is a founded outcome and a risk to children has been identified and after a review that confirms a founded outcome and, in both cases, the PSAA will be informed beforehand. Tusla will also notify relevant third parties in the case of an unfounded outcome if they have already been informed of the allegations, for example where they were informed due to a concern that a child may be at immediate and serious risk of harm.
Notifying An Garda Síochána (AGS)	Where Tusla suspects that a crime has been committed and a child has been wilfully neglected or physically or sexually abused, it will formally notify An Gardaí Síochána without delay as it has a legal obligation to do so.
National Vetting Bureau Specified Information Notification	Under sections 19, (1) & (2) National Vetting Bureau (Children and Vulnerable Persons) Act 2012] where Tusla has a bona fide concern that a person may harm a child or put a child at risk of harm, Tusla must initiate a specified information notification to the Garda National Vetting Bureau (GNVB). Prior to a specified information notification being made, the PSAA (and/or their parents if the PSAA is a child) must be informed of the fact of that concern and of Tusla's intention to notify the GNVB of it. Such a notification has no impact on the conduct or outcome of a substantiation assessment.
Obtaining Mandated Assistance from a Mandated Person	Tusla may disclose information about a child protection concern with a mandated person in order for that mandated person to assist Tusla with such information and assistance as it may reasonably require.

Why We Use Your Personal Data:	What this means:
Screening	All referrals of child abuse received by Tusla will be subject to a screening and CASP preliminary enquiry process to determine if there is a basis for a substantiation assessment and safety planning for an identified and/or yet to be identified child(ren). When screening a referral, the CASP Social Worker must consider the following: a) does the information in the referral meet the Children First threshold of reasonable grounds for concern and definition of child abuse? and b) are they satisfied that the referral information is not a fake or a hoax? and c) does the information in the referral fall within the category of cases as outlined in Section 3.2 Criteria for applying the CASP to allegations of child abuse? The screening stage is also used to make decisions on any immediate protective action that may be required in relation to identified and/or yet to be identified children.
Preliminary Enquiries	The CASP Social Worker will contact you, outlining the process and informing you of your rights, liaise with AGS as appropriate and identify prospective witnesses and will determine before progressing to Stage 1 whether: (i) There are ongoing grounds for concern; and (ii) The disclosure warrants further investigation
Stage 1 of the Substantiation Assessment	The CASP Social Worker will engage in the interview process with you and identified witnesses, carry out checks for reliability and accuracy of the information gathered and will determine before progressing to Stage 2 whether: (i) There are ongoing grounds for concern; and (ii) The allegation warrants further investigation.
Stage 2 of the Substantiation Assessment	The CASP Social Worker will engage in the interview process with the PSAA and identified witnesses, carry out checks for reliability and accuracy of the information gathered including, if appropriate, facilitating questions from the PSAA to you before reaching a conclusion.

Why We Use Your Personal Data:	What this means:
Provisional and Final Conclusion	The CASP Social Worker can reach either of the following conclusions: – Founded Outcome: The outcome of a substantiation assessment where it is established on the balance of probabilities that child abuse has occurred. – Unfounded Outcome: The outcome of a substantiation assessment where it is not established on the balance of probabilities that child abuse has occurred The CASP Social Worker will inform the PSAA (and/or their parents if the PSAA is a child) of the provisional conclusion and provide them with 21 days in which to respond with any observations or new information. The final conclusion is reached once any representation or additional information provided by the PSAA in response to the Provisional Conclusion, has been considered and assessed. The Social Worker will inform the PSAA (and/or their parents if the PSAA is a child) of the final conclusion and inform the PSAA that if he or she wants a review, he or she must ask for the review within 14 days of receipt of the final conclusion and that if the PSAA does not ask for a review, the final conclusion of founded will stand.
CASP Review	If a Founded outcome has been reached and if the PSAA is not satisfied with the Founded outcome her or she can ask that it is looked at by another group of people known as the CASP Review Panel.
Statistical Analysis and Research	Statistics from CASP will be compiled and may be shared with researchers. Please note that when we provide these statistics to researchers for analysis and research we take out all personal data from this information so that you are not identified or identifiable from this information either on its own or when combined with any other information.

8. Why are we allowed to process your personal data?

We only use your information for the reasons set out above in Section 7 '**What will my personal data be used for?**' We are permitted to do so under the General Data Protection Regulation (GDPR) generally because

- the processing is necessary for the performance of tasks carried out in the public interest or in the exercise of official authority vested in us;

- the processing of your **personal data** is necessary for compliance with a legal obligation to which we are subject;

AND in the case of **"special categories of personal data"**, also because the processing is necessary for the purposes of provision of medical care, treatment or social services, management of health or social care systems and services.

9. How long do we keep your personal data?

We will keep your information for no longer than is necessary for the purposes for which the information is collected. Our data retention policies comply with all applicable laws and privacy legislation to which we are subject. They set out how long we are allowed to retain different types of data we hold and are reviewed on a regular basis.

Our retention periods take into account legal obligation(s) under applicable law to retain data for a certain period of time, statute of limitations under applicable law and guidelines issued by relevant data protection authorities and other relevant regulatory authorities.

10. How we keep your personal data safe and secure

The security and confidentiality of your personal data is extremely important to us. Your information is stored securely in IT systems administered by Tusla. Tusla has technical, administrative, and physical security measures in place to protect your personal data from unauthorised access and improper use; secure our IT systems and safeguard the information; and ensure we can restore your data in situations where the data is corrupted or lost in a disaster recovery situation.

Where appropriate, we use encryption or other security measures which we deem appropriate to protect your personal data. We also review our security procedures periodically to consider appropriate new technology and updated methods.

Despite our reasonable efforts, no security measure is ever perfect or impenetrable.

11. How we keep your personal data safe and secure

We store your data on a cloud infrastructure provided by our third party service provider. This data sharing arrangement with the provider is governed by a service agreement that requires the provider to implement and maintain appropriate technical and organizational measures to protect your **personal data** and to maintain its confidentiality and security. The provider is required to abide by the requirements of data protection law regarding the collection, use, transfer, retention, and other processing of your **personal data**. The provider may transfer the data to a third country for purposes of providing this hosting service and is required to undertake such transfers subject to appropriate safeguards as **model clauses** described in Article 46 of the GDPR and such transfers and safeguards will be documented according to Article 30(2) of the GDPR.

We share personal data only to the extent that this sharing is strictly necessary to comply with the requirements of fair procedures (to allow the PSAA to respond to the allegations made), to conduct a substantiation investigation and to comply with our legal obligation to report crimes and suspected crimes with:

Recipient	What We Will Share
PSAA	Your name, age, geographical area, the fact that you are a PMD and, if required for fair procedures, ethnicity, proof of identity, date of birth, profession. The special categories or other sensitive personal data in respect of you and which may include health, criminal convictions, gender, age, allegations of abuse, disabilities issues (relevant in relation to interactions with you), literacy issues (relevant in relation to interactions with you), history of any abuse you suffered, relationship history, mental health, addictions, event details (which may include hobbies, religion, culturally sensitive issues), current and future risks identified in respect of you, sexual orientation, sexual activity, sexual history, sexual preference.
Witness	Your name, age and geographical area and the fact that you are a PMD
An Garda Síochána	Your name, age, address and the fact that you are a PMD. The special categories or other sensitive personal data in respect of you and which may include health, criminal convictions, gender, age, allegations of abuse, disabilities issues (relevant in relation to interaction with you), literacy issues (relevant in relation to interaction with you), history of any abuse you suffered, relationship history, mental health, addictions, event details (which may include hobbies, religion, culturally sensitive issues), current and future risks identified in respect of you, sexual orientation, sexual activity, sexual history, sexual preference.
CASP Review Panel Members	Your name, age, geographical area and the fact that you are a PMD. The special categories or other sensitive personal data in respect of you and which may include health, criminal convictions, gender, age, allegations of abuse, disabilities issues (relevant in relation to interaction with you), literacy issues (relevant in relation to interaction with the you), history of any abuse you suffered, relationship history, mental health, addictions, event details (which may include hobbies, religion, culturally sensitive issues), current and future risks identified in respect of you, sexual orientation, sexual activity, sexual history, sexual preference.

Glossary

Personal data is any personal information relating to an individual who can be identified, directly or indirectly, by reference to that information.

The **Controller** is the person or organisation which decides the purposes and means of the processing of personal data either on its own or with others.

Processing means any operation or set of operations which is performed on personal data such as collection, recording, organisation, structuring, storage, alteration, retrieval, consultation, use, disclosure, erasure or destruction.

Special categories of personal data are types of personal data which might show a person's race, ethnicity, political opinions, religious or philosophical beliefs, trade union membership, sex life or sexual orientation, details about their health and any genetic or biometric data.

Model clauses are standard contractual clauses which have been approved by the European Commission as providing adequate safeguards to enable personal data to be transferred outside the European Economic Area.

Personal Data Breach means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed.