

Child Safeguarding Statement: Social Media and Digital Images Guidance for Staff Working with Children and Young People, including Online Safety

.....

**Children
First**

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



Tusla Child Safeguarding Statement – Social Media and Digital Images Guidance for Staff Working with Children and Young People, including Online Safety

Document Reference Number	
Revision Number	3
Approval Date	TBC
Next Revision Date	TBC
Document Developed By	Tusla Children First Information and Advice Service
Document Approved By	National Policy Oversight Committee - NPOC
Responsibility for Implementation	All Staff
Responsibility for Review and Audit	Children First Steering Committee– Children First Lead – Tusla CFIAS CSS Working Group

Introduction

This guidance is developed in line with The Children First Act 2015, The *'Children First – National Guidance for the Protection and Welfare of Children'* (published under s.6, Children First Act 2015) and Tusla Child Safeguarding: A Guide for Policy Procedure and Practice and Guidance on Developing a Child Safeguarding Statement.

The Children First Act 2015 - Section 11 requires organisations that are providers of relevant services to prepare a Child Safeguarding Statement. This is a written statement that specifies the service being provided and the principles and procedures to be observed in order to ensure, as far as practicable, that a child availing of the service is safe from harm. Tusla is required to have a Child Safeguarding Statement, as a relevant service, under the Act and includes a written assessment of the risk and, in that regard, specifies the procedures that are in place to manage any risk identified, as well as reference to the six specified procedures required by the Children First Act 2015. The following Guidance has been developed under five categories to support relevant services with regards to managing the risk of harm identified in the course of carrying out a risk assessment as a part requirement of the Child Safeguarding Statement.

This document contains additional guidance to support Tusla's Child Safeguarding Statement (CSS). All service managers, line managers and staff are responsible for familiarising themselves with the contents of this document. When carrying out the assessment of risk of harm to a child while availing of their specific services (as required by the Children First Act 2015, Tusla's CSS and accompanying Tusla guidance on carrying out the related risk assessment), service managers must consider the guidance as provided in this document.

Purpose

The purpose of this guidance is to assist Tusla staff in managing risks identified in the CSS risk assessment, thus meeting our legislative requirements as per the Children First Act 2015

You will find a general glossary, scope, legislation and related guidance on revision and references consistent with Tusla's Procedure for Developing Policies, Procedures, Protocols and Guidelines. The guidance provided within this document may be relevant to the service you are providing and should be used to manage the risk identified in your service's risk assessment.

Scope

Heads of service: this guidance is generic and may require further consideration to reflect local area practices.

Managers: All managers are responsible for bringing this document to the attention of staff for whom they have responsibility. Managers are responsible for monitoring implementation of this guidance.

All Staff: This guidance applies to all Tusla staff members. All staff members are responsible for familiarising themselves with the terms of this guidance and for adhering to them.

Legislation and Other Related Policies

Addendum to Children First: National Guidance for the Protection and Welfare of Children - Online Safety

Child Care Act 1991

Children First Act 2015

Children First: National Guidance for the Protection and Welfare of Children 2017

Criminal Justice (Withholding of Information on Offences Against children and Vulnerable Persons) Act 2012

Equal Status Acts (2000-2018)

National Vetting Bureau Acts 2012-2016

Protected Disclosures Act 2014

Tusla Child Protection and Welfare Practice Handbook 2

Tusla Child Safeguarding Statement and all related specified procedures

Tusla Child Sexual Exploitation Procedure 2021

Tusla Data Protection and Privacy Policy 2021

Glossary of terms

Child – As defined by the Child Care Act 1991.

Child Safeguarding – ensuring safe practice and appropriate responses by staff and volunteers to concerns about the safety or welfare of children, including online concerns,

should these arise. Child safeguarding is about protecting the child from harm, promoting their welfare and in doing so creating an environment which enables children and young people to grow, develop and achieve their full potential.

Child Safeguarding Guide – Tusla Children First – Child Safeguarding: A

Guide to Policy, Procedure and Practice.

Child Safeguarding Statement – defined in the Children First Act 2015, this is a statement, including a written assessment of risk of harm to children and the measures that will be taken to manage any identified risks.

Children First – This is an overarching term that refers to responsibilities under Children First: National Guidance for the Protection and Welfare of Children (DCYA, 2017, published under s.6 of the Children First Act 2015) and/or Children First Act, 2015.

Information and communications technology (ICT): Although there is no single, universal definition of ICT, the term is generally accepted to mean all devices, networking components, applications and systems that combined allow people and organizations (i.e., businesses, non-profit agencies, governments and criminal enterprises) to interact in the digital world. Devices encompassed by the term ICT include mobile phones, laptops, computers, tablets, etc.

Parents – All references to parents includes legal guardians and caregivers.

Provider – as defined in the Children First Act 2015, 'means, in relation to a relevant service, a person-

- (a) who provides a relevant service, and
- (b) who, in respect of the provision of such relevant service—
 - (i) employs (whether under contract of employment or otherwise) one or more than one other person to undertake any work or activity that constitutes a relevant service,
 - (ii) enters into a contract for services with one or more than one other person for the provision by the person of a relevant service, or
 - (iii) permits one or more than one other person (whether or not for commercial or other consideration and whether or not as part of a course of education or training, including an internship scheme) to undertake any work or activity, on behalf of the person, that constitutes a relevant service;"

Relevant service – as defined in the Children First Act 2015, 'means any work or activity specified in Schedule 1 [of that Act]'.

Staff – All references in this policy to 'staff' should be interpreted as meaning all staff, whether they are in a paid or unpaid capacity.

Social Media: The Merriam-Webster Dictionary defines social media as "forms of electronic communication (such as websites for social networking and

microblogging) through which users create online communities to share information, ideas, personal messages, and other content (such as videos)". Any website that enables users to interact is considered a Social Media site, including social networking sites such as Facebook, Instagram and Twitter.

Tusla – the Child and Family Agency, is the lead, statutory organisation for safeguarding children in Ireland.

Review and Audit

The monitoring, audit and revision of all policies, procedures and guidelines contained in this document will be undertaken when the Tusla Child Safeguarding Statement is reviewed unless a practice issue or change in legislation or policy guidance requires an earlier review.

This Tusla Child Safeguarding Statement Additional Guidance to Manage Risk of Harm, will be reviewed 24 months after adoption and every 24 months thereafter. It should be reviewed earlier if there is a material change to legislation and policy/procedure, or if there is an incident relating to matters covered in this guidance. All Directorates, Heads of Services and managers must ensure that all staff comply with this guidance where appropriate.

A National PPPG Catalogue will be maintained by the Director of Policy and be published on the Tusla Website. All approved PPPGs will be listed as well as the scheduled year of review.

References and Useful Resources

- Always Children First: Child Safeguarding Awareness Training for Organisations
- Appropriate use of social networking tools, guidelines for youth work staff and volunteers (Youth Work Ireland 2009)
- Child Care Act 1991
- Child Protection and Welfare Allegations against Tusla Staff Policy and Procedure (Tusla 2019)
- Tusla Child Safeguarding Statement – Additional Guidance to Manage Risk of Harm
- Child Protection and Welfare Practice Handbook 2 (Tusla 2018)
- Child Safeguarding: A Guide for Policy, Procedure and Practice (2nd ed) (Tusla 2019)
- Child Sexual Exploitation Procedure (CSE) (Tusla 2020)
- Children First Act 2015

- Children First: National Guidance for the Protection and Welfare of Children (DCYA 2017)
- Criminal Justice (Withholding of Information on Offences Against children and Vulnerable Persons) Act 2012
- Cyberbullying in Schools: Guidance and Resources for Management (Department of Education and Skills 2013)
- Information and Communications Technology (ICT) Acceptable Use Policy.
- Information and Communications Technology Acceptable Usage Policy (Tusla March 2021)
- Let's Beat Bullying (NYCI 2007)
- Lone Working Policy (HSE 2017)
- Merriam Webster Dictionary
- Procedure for Developing Policies, Procedures, Protocols and Guidelines
- Protected Disclosures Act 2014
- Safe Driving for Work Policy (HSE 2018)
- Staff Procedure for Reporting Child Protection and Welfare Concerns (Tusla 2019)

Tell Us: Tusla Comments and Complaints Policy (Tusla 2021)

Tusla Disciplinary Procedure

Tusla Privacy Policy

Tusla Social Media Procedure

United Nations Convention on the Rights of the Child (1989)

www.tusla.ie

Revision History

Version 3 drafted 30-05-24.

Overview

The purpose of the Tusla Child Safeguarding Statement Guidance: Social Media and Digital Images Guidance for Staff Working with Children and Young People, including Online Safety, is to provide guidance and direction to Tusla staff regarding the safe and responsible use and storage of social media and digital images when working with children/young people. All staff need to be clear on their roles and responsibilities in relation to the use of this guidance while working with children/young people. Having a Social Media and Digital Images Guidance for staff working with children and young people, including online safety, in place will help staff focus on supporting children and

young people's rights and remain child-centred in their everyday work. Additionally, The Department of Children and Youth Affairs (now DCEDIY) published an Addendum on Online Safety to the Children First: National Guidance for the Protection and Welfare of Children in January 2019. This guidance takes into account guidance provided in

- the Addendum.
- Child Protection and Welfare Practice Handbook 2
- Tusla Child Safeguarding: A Guide for Policy, Procedure and Practice

Purpose

The purpose of this guidance is as follows:

- To give staff guidance and direction regarding the safe and responsible use of social media and digital images in relation to children and young people under 18 years of age.

Guidance

Staff Responsibilities¹

All Tusla staff should only use Tusla phones and ICT equipment to communicate with children/young people, in the context of their work and only where necessary.

Mobile Phone

Staff should not use their personal mobile phone or personal social media account to communicate with children/young people. This includes phone calls, text messages, e-mail or web-based communications e.g. "X" formally known as Twitter/WhatsApp./Instagram/Facebook/TikTok/YouTube/Snapchat etc

Guidance on the use of social media and digital Images.

- All digital and social media communications with young people should be with the consent of the child, parent, carer, staff members and line manager. Texting, telephoning, e-mails to children/young people should be with parental knowledge/consent (where appropriate).
- Some staff may use texting or text advice services where children/young people may be involved in a one-to-one texting exchange with a worker, given the nature or type of service. However, good practice guidelines should be in place which protect children/young people, the worker and Tusla.

¹ This document must be read in conjunction with Tusla's [Information Technology Acceptable Usage Policy](#), [Acceptable Use of Information and ICT Assets](#), [Policy on Record Management and Retention](#), [Child Sexual Exploitation Procedure \(CSE\)](#), <http://www.tusla.ie/about/twitter-policy>.

- Staff must not participate in the viewing or exchange of inappropriate images or obscene materials with young service users.
- Misuse of ICT or social media could result in the need for additional supervision, retraining, counselling and in some situations could result in disciplinary procedures being invoked.
- In the event that a member of staff receives or comes across images of child abuse or concerning data, this should be reported to your line manager following Tusla's Staff Procedure for Reporting Child Protection and Welfare Concerns.
- Staff who use social media sites as part of their work or for work related purposes should do so only with the agreement of their Line Manager.
- All contact with children and young people through social media sites should be recorded alongside other communications and work with children/young people.
- If using any form of social media maintain a work profile which is separate from any personal profiles.
- Any misuse of social media should be reported to your line manager as soon as possible. You must also report any inappropriate comments on Social Media by another member of staff.
- Staff must not use their personal social media profile or personal devices to communicate with, or to take or share images of, children and young people with whom they work.
- Staff must not accept 'friend' or 'network' requests from children/young people with whom they work.
- Staff must not share their personal contact details with children/young people with whom they work.

Digital Images;

- Staff must not use their own personal equipment to take images. Decision must be made in consultation with line manager
- Parental Consent or legal guardians where appropriate, must be sought to take and/or store images.
- Parents/legal guardians, where appropriate or legal guardians, should be informed about why photos are being taken and/or stored.
- Consent from child/young person to be photographed must be obtained.

- All children/young people must be appropriately dressed when images are taken.
- All staff must comply with Tulsa's data retention policies

Publishing Images

- Identifying details of children/young people such as full name, e-mail address, home address, telephone number, etc. should not be published with photos.
- Do not provide additional information that can assist someone to locate children/young people.
- Permission should be sought from children/young person and parent and legal guardian (as appropriate).
- If using an outside photographer, ensure you have complete contact details of photographer used. Clearly outline that all images will remain the property of Tulsa and cannot be used or sold for any other purpose.

E-Mails

- Staff must only use their work e-mail account for communication with children /young people as agreed with Line manager.
- Do not send messages which are discriminatory, harassing, negative, or threatening and which could cause offence to the child/young people.
- Do not email private messages to children/young people.
- Tone in email should be professional when communicating with children/young people.

Computer use by children and young people

You must ensure the following:

- Appropriate supervision of children/young people's use of the Internet, including time and place;
- Young people themselves are made aware of the ICT usage policy and that the history will be checked, as appropriate;
- Where appropriate, that you discuss risky and safe behaviour around ICT usage, with child/young person (e.g. privacy settings, not using profile photos, not using own name etc.);
- An appropriate level of monitoring should take place and informing the child/young person how you are monitoring their usage;
- Any concerns about a child's online safety must be recorded and

reported to your line manager following reporting procedures for any child protection and welfare concerns;

- Develop an ICT code of behaviour with children and young people;
- Policies and procedures for online safety are communicated to parents /guardians.