

I2 Safeguarding Reporting System

How to set up your reporting channels, receive reports and handle all types of disclosure

Purpose

A safeguarding reporting system is the set of channels, procedures, roles and culture that enables staff, volunteers, participants, parents and partners to raise concerns and receive a response. This document explains how to set one up, how to manage it, and what to do when a concern arrives through any channel.

Read this document alongside: I3 (Response Flow Charts) — for the immediate response procedure; I1 (Incident Form and Log) — for how to record what is received; I4 (Internal Investigation Guide) — for what happens when an investigation is needed; FO Section J — policy authority for all these procedures.

1. The Four Reporting Channels

Your organisation should have all four channels available before any project begins. If any channel is not yet set up, set it up now — do not wait for a project to start. A note on timing: throughout this document, "report as soon as you are able" means within the same session or the same day — not necessarily within minutes. A person who has just received a distressing disclosure may need a moment to compose themselves, or may need to support the person at risk before they can report. This does not invalidate the report. A report made hours after a disclosure is still a report and is still acted on. See the Glossary entry for "Immediately (in safeguarding)".

Channel	
CHANNEL 1 Direct report to DSL	Always the first option. Call, message or go to the DSL directly. The DSL's contact details must be visible in the staff area, in the project folder and on Card 3 of the Quick Reference Cards (QRC). If the DSL is unavailable, go to the Alternate DSL or external backup.
CHANNEL 2 Incident Form Part A (I1)	The official written record. Completed by the person who received the concern — always within 24 hours of receiving it, immediately if possible. Submitted to the DSL. Supplements the verbal report — does not replace it.
CHANNEL 3 Anonymous reporting channel	For when a person is not comfortable giving their name. Only purpose-built verified platforms guarantee genuine anonymity — standard web forms and email do not, because they can capture device addresses (IP addresses). Verified platforms: Whispli (whispli.com), EQS Integrity Line (eqs.com), FaceUp (faceup.com), SpeakUp (speakup.com). See Section 9.2 for set-up guidance.



Funded by
the European Union

www.safe-spaces.eu

CHANNEL 4 Emergency services	112 (EU) / 999 (UK). For immediate physical danger. Free from any phone. No permission needed. After calling 112, tell the DSL immediately.
---------------------------------	---

2. Informal Disclosures — WhatsApp, Verbal, Email, Text

If a safeguarding concern is raised through an informal or unstructured channel — a verbal conversation in a corridor, a WhatsApp message, a text, an informal email — the same response procedure applies. An informal channel does not mean an informal response.

If the concern is received...	
Verbally in person	Thank the person. Ask them to wait briefly. Write down exactly what they said immediately (I1 Part A). Report to the DSL the same day — as soon as you are able.
Via WhatsApp, text or personal message	Screenshot the message with date and time visible. Paste the text into I1 Part A. Report to the DSL the same day — as soon as you are able. Do not forward the screenshot to anyone else.
Via informal email	Forward to the DSL and complete I1 Part A with the text of the email and date received. Do not forward to others.
Through a third party who tells you what someone else said	Write down what the third party told you (not the original person's words, but the third party's account of them). Note the date. Report to the DSL. This is a third-party report — treat it seriously.

DON'T

Do not have informal or inappropriate discussions about safeguarding concerns in public or informal settings — corridors, team dinners, WhatsApp groups. Information about a concern is shared only with those who need it to act on it. Even discussing a case "informally" with a trusted colleague who is not involved in the response is a breach of confidentiality and can cause secondary victimisation.

3. When the Reporter Does Not Want to Proceed — Third-Party and Unwilling Reports

Sometimes a person raises a concern but then says they do not want to make a formal report, or asks you to take no action. This creates a tension: their preference versus the organisation's duty of care.

Situation



Funded by
the European Union

www.safe-spaces.eu

A reporter asks for no action	Acknowledge their preference. Explain: "I understand you don't want to make a formal report. I need to let [DSL name] know that a concern has been raised, even if I can't give all the details. The DSL will decide whether any action is needed." Log the concern in I1 Part B. Report to the DSL.
A third party reports on behalf of someone who has not consented to disclosure	Log the third-party report in I1 Part B. Report to the DSL. The DSL assesses whether the duty of care requires action regardless of the person's consent. In most cases involving an immediate risk to safety, duty of care takes precedence. Document the decision and reasoning.
The person at risk asks you not to tell anyone	Do not promise confidentiality. Say: "I can't promise to keep this secret, because my job is to keep you safe. I will only share it with the person who needs to know, and I will tell you what I share and why." Then report to the DSL.

4. Notifying Alleged Perpetrators

The alleged perpetrator is entitled to know that a concern has been raised about them. However, they are not informed before the DSL has completed the initial triage and, in cases involving a staff member or volunteer, has consulted the Alternate DSL or external backup.

In most cases, the alleged perpetrator is informed at the point when precautionary action is communicated to them (I3 Flow Chart 3). Exceptions where notification is delayed or requires external guidance:

- Where there is an immediate risk to others requiring urgent separation.

- Where the police or statutory authorities have asked the organisation not to notify the person yet.

- Where informing the person immediately could compromise a statutory investigation. The DSL manages all communication with the alleged perpetrator. See I4 Section 4.1 for full guidance.

5. Confidentiality in the Reporting System

DO	
Share information only with those who need it to act on the concern.	Share with colleagues "just in case" or for informal advice.
Tell the person raising the concern what you will share, with whom, and why.	Promise confidentiality you cannot keep.
Use reference codes in all records. Real names in I1 Part C	Use real names in the case log or incident form body text.

(Identity Index) only, held by DSL.	
Refer to F0 Section K for the full confidentiality framework.	Assume that because you know something, you are entitled to share it.

Safeguarding data is classified as special category data under GDPR Article 9. All handling must comply with O3 (GDPR and Safeguarding Data Handling). The lawful basis for processing is in F0 Section K (not F.3 — see GDPR Article 9(2)(b) and 9(2)(c) for the relevant bases in urgent safeguarding situations).

6. Immediate Risk — Universal Application

Where there is an immediate risk to any person's safety, the immediate response procedure applies universally. The duty of care in an emergency extends to every person — regardless of age, vulnerability status, or any other characteristic. Age-specific measures (R3 for children, R4 for adults at risk) add to the universal procedure — they do not replace it or limit when it applies.

7. Setting Up the Anonymous Reporting Channel

To set up a verified anonymous reporting channel:

- Choose a purpose-built platform: Whispli, EQS Integrity Line, FaceUp or SpeakUp. Standard web forms and email cannot guarantee anonymity.
- Configure the platform so that no identifying information — including IP addresses — is collected.
- Test the channel before any project begins by submitting a test report and verifying it is received by the DSL.
- Publish the link prominently: on QRC Card 2 (Staff and Volunteers), QRC Card 3 (Participants), in the participant information, and on any relevant project materials.
- Review annually: is the channel being used? Are reports being responded to? Is the platform still verified?

References

F0 Safeguarding Policy Framework Sections J (Acting on Concerns), K (Confidentiality), L (Recording).
 I1 Incident Form and Log. I3 Response Flow Charts. I4 Internal Investigation Guide.
 O3 GDPR and Safeguarding Data Handling.
 GDPR Regulation (EU) 2016/679, Articles 4(5) (pseudonymisation), 9(2)(b) and (c) (processing of special category data), 6(1)(d) (vital interests).
 EU Whistleblower Protection Directive 2019/1937, Articles 8-9 (anonymous reporting channels).
 Glossary of Key Terms (Safe Spaces) — for definitions of all bolded terms in this document.



© Safe Spaces, 2026. This material is released under the Creative Commons Attribution 4.0 International licence (CC BY 4.0). Permission is granted to utilize, modify, and translate these resources for organizational use, provided the Safe Spaces project is formally credited. Access the complete toolkit at www.safe-spaces.eu.

Financial support provided by the European Union. Production of this document by the European Commission does not imply endorsement of the material; the perspectives expressed belong solely to the authors. Neither the National Agency nor the Commission accepts liability for any application of the information provided.



Funded by
the European Union

www.safe-spaces.eu