

P2 DSL Responsibilities Guide

What the Designated Safeguarding Lead does, when, and how

Purpose of this document

This guide explains the full responsibilities of the Designated Safeguarding Lead (DSL) in the Safe Spaces framework. It covers all tiers — from a micro-organisation with one staff member and an external backup, to a large organisation with a dedicated safeguarding function. Use it alongside the DSL Appointment document (P1) and the Safeguarding Policy Framework (B3, Section F).

This guide is for: the DSL and Alternate DSL (read before taking up the role and keep as a reference throughout); senior management and boards (to understand what the DSL role entails); and partners (to understand the DSL's authority).

1. What the DSL Is — and Is Not

The Designated Safeguarding Lead is the named, trained person responsible for coordinating the organisation's safeguarding response. The role exists in every tier of organisation.

THE DSL IS....	THE DSL IS NOT...
The named point of contact for all safeguarding concerns from staff, volunteers and participants.	A police officer, investigator or therapist.
The person who logs concerns, makes triage decisions and coordinates the response.	The only person responsible for safeguarding. Every person in the organisation has a safeguarding responsibility.
The person with authority to make statutory referrals without management approval.	A person who should investigate concerns alone or make findings without a second reviewer.
The person who builds and maintains the monitoring plan for active cases.	A person who can promise confidentiality. Confidentiality in safeguarding means need-to-know sharing, not secrecy.
The person who reports safeguarding concerns to the board and, where required, to funders.	A single point of failure. Every organisation must have an Alternate DSL or external backup.

2. The Seven-Step DSL Response



Funded by
the European Union

www.safe-spaces.eu

When a concern reaches you as DSL, follow these seven steps in order. They apply at every tier.

Step	
1. RECEIVE	Listen to the person reporting. Write down exactly what they tell you in their own words. Do not investigate at this stage. Do not share what you have heard before you have assessed it. If the person is distressed, use Psychological First Aid (PFA) before proceeding.
2. LOG	Open the Incident Log (I1 Part B) immediately. Assign a case reference code (e.g. "Case 2025-07"). Record the date and time of receipt. Do this before assessing, consulting or acting. Even if the case is later closed with no action, the log shows it was received and considered. An unlogged concern effectively never happened. Note: if a staff member or volunteer reports late — hours or even a day after the disclosure — log the concern with the actual time it was received by you, and note when the original disclosure or observation occurred. A late report is still a report.
3. ASSESS	Ask four questions: 1. Is there immediate physical danger right now? If yes, call 112 before anything else. 2. What type of concern is this? (Disclosure, observation, allegation, or third-party report.) 3. Who is involved? If a staff member or volunteer is alleged to have caused harm, consult the Alternate DSL or external backup before acting. 4. What is the jurisdiction? Which country are the people in? This determines which external services apply.
4. CLASSIFY	Apply the concern classification: MINOR: low-level welfare concern, no immediate risk, requires monitoring and documentation. MODERATE: pattern of concern or single concerning incident requiring DSL assessment and possible precautionary action. MAJOR: immediate risk to safety, statutory referral threshold, emergency response required. Note: what is Minor can become Major with repeat behaviour. Review classification at each case review.
5. CONSULT IF NEEDED	Consult the Alternate DSL (Tier 2/3) or external backup (Tier 1) when: the concern involves a staff member or volunteer; you are uncertain about next steps; or the case is outside your experience. Consult an external safeguarding advisor when: the case

	involves a child; you are uncertain whether to make a statutory referral; or the case is Major. Document every consultation in I1 Part B: who, when, what was decided.
6. ACT	Choose the appropriate response. Options, used alone or in combination: - Safety planning: with the person at risk, decide what practical steps make them safer right now. - Precautionary action: ask the alleged perpetrator to step back from contact with participants. Protective, not punitive. Communicate in writing. - Statutory referral: formally notify police, child protection services or other statutory authorities. You have authority to do this without management approval. - Internal management action: your organisation's disciplinary or HR process. - No further action: this is a formal decision, not the absence of a decision. Document with full reasoning.
7. COMMUNICATE AND MONITOR	Tell the person who reported: the concern was received and is being acted on. Tell the person at risk: what support is available and what happens next. Begin the monitoring plan now — not when the case is resolved. The monitoring plan specifies: named contact person; contact schedule (frequency, channel, time); risk indicators to watch; support in place; review date; closure criteria. All decisions and communications are recorded in I1 Part B.

3. Tiered Responsibilities — What Changes at Each Tier

The seven steps above apply at every tier. The following responsibilities are in addition to the core seven steps, and vary by tier.

TIER 1

Tier 1 Additional Responsibilities

Because you are working alone or nearly alone, these are especially important:

- Contact your external backup at the start of every project — not only when something goes wrong. A brief call to confirm they are still available and aware of the current project is good practice.
- Document every decision carefully. At Tier 1, your case log (I1 Part B) may be the only record if a case is later reviewed externally. Write down what you decided and why, including when you decided to take no further action.
- You must not conduct an internal investigation alone. Any case requiring formal investigation involves your external backup and, wherever possible, an external safeguarding advisor.



Funded by
the European Union

www.safe-spaces.eu

- Know your local statutory services before your project begins. Use the Country Legal Supplement and R3 (if working with under-18s) to identify the relevant child protection services and emergency numbers in the country where your project takes place.

Finding external support at Tier 1:

- Your external backup: named in P1. Contact within 24 hours of any significant concern.
- National Agency: your Erasmus+ or ESC National Agency may be able to provide or signpost to safeguarding support. Contact them proactively.
- NSPCC Helpline (UK): 0808 800 5000. For international contexts, equivalent national child protection helplines are listed in the Country Legal Supplement.
- Peer organisation DSL: if you have a mutual backup agreement with a peer organisation, this is the person to call for a case consultation.

TIER 2

Tier 2 Additional Responsibilities

At Tier 2, the most important addition is the joint decision-making requirement:

- All case decisions above "no further action" are made jointly by the DSL and Alternate DSL. This is mandatory, not optional. It protects both individuals from isolated judgement errors and strengthens accountability.
- The Alternate DSL maintains awareness of all active cases — they are not a backup who only engages during handovers. They are an informed second person throughout.
- DSL responsibilities in partnerships (O1 and O2): as the lead DSL you are responsible for signing partnership agreements and monitoring partner compliance throughout the project.
- Reporting to the board: at minimum annually, using O4 (Annual Self-Assessment). This includes anonymised case data, training completion rates and any policy changes.
- DSL handover: when a DSL or Alternate DSL changes role, a formal handover is required. The outgoing DSL briefs the incoming DSL on all active cases, and transfers custody of I1 Parts B and C.

TIER 3

Tier 3 Additional Responsibilities

At Tier 3, the DSL is a dedicated or near-dedicated role:

- Dedicated safeguarding time: the DSL role at Tier 3 requires protected time in your schedule. It cannot be consistently squeezed around other responsibilities when complex cases arise.
- Support pool oversight: if you have a support pool, you are responsible for briefing pool members, maintaining their safeguarding awareness, and ensuring they do not exceed their authority. Support pool members assist — they do not lead.
- External safeguarding advisor: maintain an active relationship, not just an emergency contact. Consider commissioning a consultancy review of complex cases and an annual external review of your safeguarding practice.
- Partnership compliance: proactively monitor partner safeguarding standards throughout each project using O2, not only at signing and annual review.

- Regular board reporting: quarterly data-level reporting as well as the annual full review.

4. Consolidated DSL Responsibilities Across the Pack

The DSL has responsibilities that are described in several documents across the Safe Spaces pack. This section consolidates them in one place so nothing is missed.

Context	
Accommodation and sleeping arrangements (R3 Section 8)	DSL must approve all accommodation arrangements for projects involving under-18s. No accommodation arrangement for under-18 participants may proceed without DSL sign-off.
Travel and residential activities (A1, A2)	DSL reviews and approves pre-departure risk assessments for all overnight and travel activities. DSL is contactable at all times during residential projects.
Risk register (B2, R1)	DSL is responsible for maintaining the safeguarding risk register and ensuring it is reviewed at minimum annually and before every significant project activity.
Online and digital activities (A3)	DSL approves the acceptable use policy and is notified immediately of any online safeguarding concern.
Children in the project (R3)	DSL ensures child-specific measures (R3) are in place before any project involving under-18s begins.
Adult participants at risk (R4)	DSL ensures a confidential needs assessment is conducted for any adult participant who may be at additional risk, before the project begins.
Partnership compliance (O1, O2)	DSL signs the partnership safeguarding agreement. DSL monitors partner compliance throughout the project using O2.
Anonymous reports (I2)	DSL is responsible for receiving, logging and assessing all anonymous reports through the organisation's verified anonymous reporting channel.
Alleged perpetrator management (I4)	DSL manages all communication with the alleged perpetrator during and after an investigation, in line with I4. The alleged perpetrator is not informed of the concern before the DSL has made a triage decision.
Misconduct disclosure (I4)	When a concern involves a member of staff or volunteer, the DSL considers whether to check and contribute to the Misconduct Disclosure Scheme (misconduct-disclosure-scheme.org).

Case closure (I4)	DSL formally closes cases using documented criteria. Closure requires sign-off by both DSL and Alternate DSL.
Annual review (O4)	DSL leads the annual self-assessment (O4) and presents anonymised findings to the board.
Training (P4)	DSL ensures all staff, volunteers and board members have completed appropriate safeguarding training. DSL maintains the training record (P4).
Data protection (O3)	DSL is the organisational safeguarding data custodian. DSL holds I1 Parts B and C in restricted, access-controlled storage.

5. DSL Wellbeing

Managing safeguarding concerns under pressure, with incomplete information, while maintaining confidentiality, has a cumulative effect. This is not a failure — it is an occupational reality for anyone in a safeguarding role.

- After a Major case, debrief with your Alternate DSL, external backup or external safeguarding advisor before moving on to the next task.
- Secondary trauma — the emotional impact of regular exposure to others' distress — is real and must be taken seriously by the organisation, not only by the DSL.
- The organisation has a duty to provide access to wellbeing support for the DSL. This may include: peer supervision with a qualified safeguarding professional; access to an Employee Assistance Programme or equivalent; and regular line management conversations that include space for the DSL to talk about the demands of the role.
- If you are a Tier 1 DSL working largely alone, proactively build a peer support connection — another DSL at a peer organisation who you can speak to informally when a case is difficult.

References

B3 Safe Spaces Safeguarding Policy Framework v2.0, Sections F, J, K, L.
 P1 DSL Appointment and Terms of Reference (Safe Spaces).
 I1 Incident Form and Log (Safe Spaces).
 I4 Internal Investigation Guide (Safe Spaces).
 O1 Partnership Safeguarding Agreement (Safe Spaces).
 O2 Monitoring Safeguarding in Partnerships (Safe Spaces).
 O3 GDPR and Safeguarding Data Handling (Safe Spaces).
 O4 Annual Self-Assessment and Review (Safe Spaces).
 NSPCC DSL Role Description: learning.nspcc.org.uk
 Misconduct Disclosure Scheme: misconduct-disclosure-scheme.org



Funded by
the European Union

www.safe-spaces.eu

© 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