

Chapter 3 – Tool 1: Policy audit template

This template is designed to help youth organisations and NGOs working with youth conduct an evidence-based audit of how their policies and practices respond to OGBV. It links each item to basic, observable evidence, so the audit does not rely only on “opinion” but on verifiable sources. The structure is inspired by EU-level guidance on cyber violence, GBV, and data protection¹.

1. Audit information

- Organisation name:
- Date:
- Auditors (internal / external):
- Main sources of evidence (tick or list):
 - ☐ Policy documents (safeguarding policy, code of conduct, online safety rules)
 - ☐ Training materials and attendance records
 - ☐ Incident-reporting logs / registers (if any)
 - ☐ Evaluation or feedback surveys with young people
 - ☐ Interviews with at least 3–5 staff and 3–5 young people
 - ☐ Other _____

¹ European Institute for Gender Equality (EIGE). (2023). *Combating cyber violence against women and girls*. Publications Office of the European Union. https://eige.europa.eu/sites/default/files/documents/combating_cyber_violence_against_women_and_girls.pdf

United Nations Development Programme (UNDP). (2025). *Global action against online gender-based violence: Making digital spaces safe*. United Nations. <https://www.undp.org/press-releases/making-digital-spaces-safe-global-action-against-online-gender-based-violence>

European Commission. (n.d.). *Legal framework of EU data protection*. European Commission – Directorate-General for Justice and Consumers. https://commission.europa.eu/law/law-topic/data-protection/legal-framework-eu-data-protection_en

2. Policy and governance

Questions	Evidence needed	Rating (Yes/Partial/No/Under development)	Comments
Does the organisation have a written policy or statement that explicitly names online gender-based violence (OGBV) or technology-facilitated GBV?	Text of policy / code of conduct; date of adoption.		
Does at least one policy document link online safety to broader gender-equality and human-rights commitments (e.g., GBV, child-/youth-protection, digital-rights)?	Cross-reference to overarching strategies, declarations, or memoranda of understanding.		
Is there a clear statement that the organisation adopts a zero-tolerance approach to OGBV and harmful online behaviour (for staff, volunteers, partners, and young people)?	Clause in policy explicitly naming OGBV and stating consequences.		

3. Definitions and scope of OGBV

Questions	Evidence needed	Rating (Yes/Partial/No/Under development)	Comments
Does the policy define key forms of OGBV (e.g., cyber-stalking, doxxing, image-based abuse, coordinated trolling/hate speech)?	Definitions section in policy or companion guidance.		
Do definitions acknowledge that OGBV can lead to or overlap with offline violence and harassment (online-offline continuum)?	Policy language linking online incidents to broader safeguarding and protection systems.		
Are definitions written in an age-appropriate, survivor-centred way that avoids victim-blaming or over-broad "misconduct" language?	Analysis of wording; if possible, feedback from young people on clarity and fairness.		

4. Confidentiality, data protection, and safeguarding

Questions	Evidence needed	Rating (Yes/Partial/No/Under development)	Comments
Do you have written rules on how personal data and evidence (screenshots, messages) from OGBV cases are stored, shared, and deleted?	Internal data-protection / confidentiality guidelines; retention schedule.		
Are staff trained on how to handle evidence without re-traumatising survivors or exposing them to further risk (e.g., secure storage, minimal sharing)?	Training records; training materials on evidence-handling and digital safety.		
Is there a youth-friendly description of how you protect privacy when someone reports OGBV (e.g., "who will see this, why, and for how long")?	Screenshots or text of reporting instructions; translations or adapted versions for younger audiences.		

5. Reporting, response, and support pathways

Questions	Evidence needed	Rating (Yes/Partial/No/Under development)	Comments
Are there multiple, accessible reporting channels for OGBV (online and offline), including options for anonymity where appropriate?	List of channels (e.g., form, email, helpline, trusted staff; mention of anonymity where used).		
Is there a clear description of how long someone can expect to wait for a response and how they will receive feedback?	Policy or FAQ documents; if available, logs of responses to reports.		
Are there documented procedures linking reported OGBV to youth-specific support services (e.g., counselling, legal aid, digital-safety advice)?	Referral pathways; written agreements with GBV / mental-health services.		

6. Training, capacity, and staff culture

Questions	Evidence needed	Rating (Yes/Partial/No/Under development)	Comments
Is there a regular, mandatory training plan on OGBV, digital safety, and trauma-informed practice for staff and volunteers?	Training plan/calendar; attendance lists; training materials		
Have staff been trained on how to listen to and respond to disclosures without pressuring young people to take formal action?	Training materials; if possible, short staff self-assessment or interview notes		
Does the organisation have safeguarding or HR procedures that hold staff accountable for perpetrating or failing to respond to OGBV?	HR/safeguarding policy; documented disciplinary procedures and case-review mechanisms		

7. Inclusion, intersectionality, and youth participation

Questions	Evidence needed	Rating (Yes/Partial/No/Under development)	Comments
Does the policy explicitly recognise that OGBV risk and access to support differ by gender, disability, migration status, sexuality, and other intersecting factors?	Policy language; strategy or guidance documents mentioning intersectionality		
Are youth survivors or youth-led groups involved in reviewing or co-designing OGBV-related policies and campaigns?	Minutes of youth-participation meetings; youth-advisory-group terms of reference		
Does the organisation monitor or gather feedback from marginalised groups about their experiences of online safety?	Feedback forms, focus-group records, or survey reports		

8. Monitoring, evaluation, and improvement

Questions	Evidence needed	Rating (Yes/Partial/No/Under development)	Comments
Does the organisation keep anonymised records of OGBV incidents and responses for monitoring and learning?	Incident register or log (with identities removed); M&E framework mentioning OGBV indicators		
Does the organisation review these records and feedback at least once per year to update its policies and practices?	Reports of feedback-loop meetings; policy-revision dates and change logs		
Are there measurable indicators linked to OGBV-related outcomes?	Strategic plan or M&E matrix listing OGBV-related indicators		

9. Action plan and recommendations

Main strengths identified

Main gaps identified:

Priority short-term actions (next 3–6 months) & responsible person/team

Medium- to long-term improvements (next 6–24 months) & responsible person/team

Name & Role

Signature
