



RECOVER e-Hub Community Guidelines

Safe, respectful, survivor-centred professional collaboration

Document detail	Information
Document	Community Guidelines
Controller	Kovos su prekyba žmonėmis ir išnaudojimu centras, VšĮ (KOPŽI)
Company code	304486353
Registered address	Draugystės g. 8F-236, LT-51264 Kaunas, Lithuania
Service	RECOVER e-Hub at ehub.recover-project.eu
Audience	Members, contributors, moderators, administrators, and authorised project personnel
Version	1.0
Last updated	22 October 2026
Effective date	Effective upon publication

Controller contact: info@recover-project.eu

RECOVER Project 101183243. Funded by the European Union. Views and opinions expressed are those of the author(s) only and do not necessarily reflect those of the European Union or the European Education and Culture Executive Agency (EACEA). Neither the European Union nor EACEA can be held responsible for them.

Contents

1. Purpose and scope
2. Community principles
3. Accounts, profiles, and identity
4. Safeguarding, confidentiality, and survivor privacy
5. Respectful and inclusive participation
6. Professional boundaries and safety
7. Quality, evidence, and responsible advice
8. Content, intellectual property, accessibility, and security
9. Rules for each e-Hub area
10. External tools and AI
11. Reporting a concern
12. Moderation and enforcement
13. Appeals and procedural fairness
14. Safeguarding and legal escalation
15. Account closure and continuing duties
16. Changes and acceptance
17. Member pre-post checklist
18. Moderator response guide

1. Purpose and scope

The RECOVER e-Hub connects people and organisations interested in recovery and reintegration work connected with trafficking and exploitation. These Guidelines protect the dignity, safety, privacy, and agency of people discussed in the community while enabling practical professional exchange.

They apply to profiles, the Community Hub, topic discussions, questions and answers, resources and the Knowledge Base, uploaded documents and media, comments, votes or reactions, follows, groups, messages, notifications, reports, and moderation decisions. They complement the Terms of Use and Privacy Policy.

The e-Hub is not an emergency service, confidential case-record system, referral mechanism, clinical service, legal service, or substitute for an organisation's safeguarding procedures.

The rules below apply to all members, including people with lived experience, professionals, researchers, public authorities, civil-society organisations, moderators, and administrators. Participation is voluntary and no one is required to disclose personal history.

2. Community principles

Principle	What it means in practice
Dignity and survivor agency	Respect each person's choices, identity, boundaries, and right not to disclose. Avoid victim-blaming, saviour narratives, sensationalism, and treating lived experience as content.
Safety before visibility	Do not publish information that could identify, locate, stigmatise, retraumatise, or expose a person, service, or safeguarding operation.
Trauma-informed participation	Offer choice, avoid unnecessary graphic detail, use content notes where discussion of harm is necessary, and accept that members may step away.
Professional integrity	Be honest about expertise, uncertainty, affiliations, funding, conflicts of interest, and the limits of advice.
Inclusion and accessibility	Welcome different countries, sectors, abilities, identities, and levels of experience. Use clear language and accessible shared materials where reasonably possible.
Evidence and learning	Distinguish evidence, professional experience, and personal opinion. Correct mistakes openly and cite reliable sources for consequential claims.
Accountability	Report harm, cooperate with moderation, and accept proportionate action when these Guidelines or the Terms of Use are breached.

3. Accounts, profiles, and identity

- Accounts are for people aged 18 or older. Do not create an account for a child or allow a child to use your account.
- Provide accurate registration and profile information. Do not impersonate another person, organisation, official, or professional role.

- Use one personal account unless KOPŽI has approved an organisational or service account. Do not share credentials.
- Only claim qualifications, affiliations, experience, or authority that you actually hold. Keep profile details current.
- Do not harvest member details, scrape profiles, build contact lists, or use e-Hub information for unsolicited marketing, recruitment, fundraising, or research.
- Use contact details obtained through the e-Hub only for the purpose for which the member reasonably shared them. Respect a request to stop contact immediately.

Profiles and community activity are intended to be visible only to authenticated members. This does not make them confidential or prevent authorised viewers from retaining copies.

4. Safeguarding, confidentiality, and survivor privacy

Protection of people affected by trafficking is the e-Hub's highest content priority. A useful professional example never justifies avoidable exposure. Do not upload or describe identifiable information about a survivor, client, witness, suspect, family member, staff member, volunteer, or service user.

4.1 Information that must not be posted

- Names, aliases, usernames, faces, voices, signatures, photographs, video, biometric details, or distinctive physical features.
- Phone numbers, email addresses, home or work addresses, live location, travel plans, device identifiers, social handles, or message screenshots.
- Exact combinations of age, nationality, language, family status, dates, small locality, workplace, school, team, shelter, or service provider that could identify someone by inference.
- Case numbers, police or court documents, immigration status, referral forms, intake notes, medical or counselling records, safeguarding records, or correspondence with authorities.
- Health, disability, mental-health, sexual-life, ethnicity, religion, political belief, criminal allegation, or exploitation information linked or linkable to a person.
- Details of trafficking routes, safe locations, security arrangements, investigative methods, or service operations that could endanger people or help offenders evade detection.

4.2 Safe use of practice examples

Risky approach	Safer approach
A real case with a changed name	Use a composite or fictional scenario that combines non-identifying learning points from several situations.
Exact age, date, city, route, and service	Use broad ranges or regions only if needed, remove dates, and omit service or route details.
A screenshot with names blurred	Recreate only the minimum relevant information in plain text; hidden metadata and context can still identify people.
A survivor consented to sharing	Check whether disclosure is necessary, proportionate, freely chosen, informed, revocable, and consistent with safeguarding. Consent alone does not remove platform risk.
A dramatic account to show impact	Describe the professional challenge and learning objective without graphic or sensational detail.

Before posting, ask whether someone who knows the person, place, service, or case could combine the details and work out who is involved. If yes or uncertain, do not post. Seek advice through an approved confidential channel instead.

4.3 Images, recordings, and documents

- Upload only material you are authorised to share and that has been checked for names, faces, metadata, tracked changes, comments, hidden sheets, revision history, geolocation, and embedded attachments.
- Do not upload graphic evidence of violence, exploitation, self-harm, or abuse. If sensitive subject matter is necessary, use a non-graphic summary and a clear content note.
- Do not record or redistribute member content, private messages, or restricted material without permission and a lawful reason.
- Never use an image of a survivor as decoration, proof, fundraising material, or illustration without a specific lawful, ethical, and safeguarding assessment.

5. Respectful and inclusive participation

Challenge ideas and practices without attacking people. The following conduct is not allowed:

- Harassment, bullying, intimidation, stalking, threats, humiliation, dog-piling, repeated unwanted contact, or encouraging others to target a person.
- Hate speech, dehumanising language, slurs, or discrimination based on race, colour, ethnicity, nationality, migration status, religion, sex, gender, gender identity, sexual orientation, disability, age, health, socio-economic status, or another protected or vulnerable status.
- Victim-blaming, disbelief based on stereotypes, sexualisation, voyeurism, moral judgement, or language that reduces a person to exploitation experienced.
- Sharing another member's personal information, private messages, or off-platform activity without a legitimate safety reason and appropriate moderator channel.
- Deliberately derailing discussions, flooding, repetitive provocation, coordinated manipulation, or evading a moderator instruction.
- Retaliation against a person who reports a concern, corrects misinformation, sets a boundary, or participates in an investigation.

5.1 Constructive disagreement

19. State the point you disagree with and explain why.
20. Separate facts, professional judgement, and personal experience.
21. Ask clarifying questions before assuming intent.
22. Offer a source, alternative method, or practical next step.
23. Step away or ask a moderator for help if the exchange becomes personal or unsafe.

6. Professional boundaries and safety

- Do not use the e-Hub to identify, recruit, solicit, groom, assess, diagnose, counsel, investigate, or directly manage a person affected by trafficking.
- Do not contact a survivor or potential survivor because of information found on the e-Hub. Use recognised referral and safeguarding channels and respect consent and professional roles.
- Do not present peer discussion as medical, psychological, legal, immigration, safeguarding, or law-enforcement advice. State limits and refer to qualified local services where appropriate.
- Do not promise confidentiality, safety, outcomes, funding, placement, legal status, or access to services that you cannot guarantee.
- Do not offer jobs, accommodation, travel, financial support, research participation, interviews, media exposure, or personal services to vulnerable people through posts or messages without appropriate approval and safeguarding.
- Disclose material conflicts of interest, commercial relationships, referral fees, sponsorship, or funding that could affect a recommendation.

If someone may be in immediate danger, contact the appropriate local emergency service or authorised national referral or safeguarding mechanism. Do not post identifying details and do not assume a moderator is monitoring in real time.

7. Quality, evidence, and responsible advice

- Make clear whether a statement is based on research, law or official guidance, organisational practice, professional experience, or personal opinion.
- Cite the original or authoritative source for claims that could materially affect safeguarding, health, legal rights, programme design, funding, or public policy.
- Do not fabricate sources, credentials, quotations, statistics, case outcomes, endorsements, or consensus.
- Avoid universal claims. Explain context, limitations, uncertainty, and whether an approach has been evaluated with the population discussed.
- Do not recommend unsafe physical activity, trauma exposure, disclosure exercises, or high-risk interventions without appropriate qualifications, screening, consent, adaptation, and safeguarding.
- Correct significant errors promptly. If content has already influenced a decision, clearly note the correction rather than silently replacing it.

Use the terminology requested by an individual where known. Avoid labels that imply blame, helplessness, criminality, or a single permanent identity.

8. Content, intellectual property, accessibility, and security

- Post only content you created, content you are authorised to share, or content permitted by an applicable licence or legal exception. Attribute authors, organisations, funders, and licences accurately.
- Do not upload paywalled, confidential, embargoed, proprietary, or copyrighted material without permission. Link to the legitimate source where possible.
- Do not remove attribution, watermarks, safety notices, licence terms, or funding acknowledgements from RECOVER or third-party materials.
- No spam, deceptive promotion, affiliate links, unauthorised fundraising, pyramid schemes, scams, or irrelevant repeated posting.
- No malware, phishing, credential requests, exploit code, attempts to bypass access controls, or security testing without written authorisation.
- Do not scrape, bulk-download, index, train a model on, or republish member content without documented permission and a lawful basis.
- Use descriptive titles, accessible document formats, meaningful link text, captions or transcripts where possible, and enough context for another professional to evaluate the resource.

9. Rules for each e-Hub area

Area	Good use	Do not
Community and topic discussions	Network, discuss professional themes, share non-identifying practice experience, and build cross-sector cooperation.	Treat the community as a confidential supervision room, publish case details, mass-message members, or dominate discussions with promotion.
Questions and answers	Ask one focused question, explain relevant non-identifying context, and distinguish peer experience from professional advice.	Seek an emergency decision, request identification of a person, or present peer answers as binding advice.
Resources and Knowledge Base	Upload authorised resources, describe the audience and licence, add version and date, and preserve source attribution.	Upload confidential records, unlicensed copies, files with hidden personal data, or materials that cannot be safely reused.

Area	Good use	Do not
Comments, votes, reactions, and follows	Add substance, correct information, signal useful contributions, and follow topics for legitimate professional purposes.	Coordinate voting, trade votes, use reactions to harass, manipulate rankings, or flag content merely because you disagree.
Groups and messages	Use the smallest appropriate audience, maintain professional boundaries, and report unwanted contact.	Assume a private channel is a secure case system, forward messages without permission, or send repeated unwanted contact.

10. External tools and AI

- Never enter confidential, personal, special-category, case, or security-sensitive information from the e-Hub into an external AI, translation, transcription, search, or document tool unless the operator has formally approved the tool and processing arrangement.
- Review AI-assisted content for factual accuracy, bias, unsafe advice, invented citations, copyright issues, and inappropriate disclosure before posting.
- Disclose material AI assistance when it produced substantive analysis, translation, imagery, or recommendations. A simple spelling or formatting aid does not normally require disclosure.
- Do not use synthetic survivor stories, faces, voices, quotes, testimonials, or case evidence in a way that could mislead, sensationalise, or substitute for genuine consent and lived experience.
- AI output is not professional authority. The member who posts it remains responsible for the content and consequences.

11. Reporting a concern

Use the report control on the relevant item where available. For privacy exposure, account compromise, urgent safeguarding, or a report that cannot be submitted through the interface, contact info@recover-project.eu. Give moderators only the minimum information needed to understand the concern.

24. Preserve your own safety. Do not engage with a threatening account or download suspicious files.
25. Report the specific content, account, or message and describe the rule or risk involved.
26. Do not repost sensitive content to prove that it exists.
27. For suspected account compromise, include the username and approximate time, but never send a password or reset code.
28. For urgent real-world danger, contact the appropriate local emergency or authorised safeguarding service first; the e-Hub is not continuously monitored.

Good-faith reporting is protected. Knowingly false, malicious, discriminatory, or retaliatory reports may themselves breach these Guidelines.

12. Moderation and enforcement

Moderators may act to protect people, preserve the purpose of the e-Hub, comply with law, and maintain reliable knowledge. Action may be taken on member-only, group, or message content where KOPŽI has lawful access and a safety, security, or service reason to review it.

Level	Typical examples	Possible response
Level 1 - correctable	Off-topic or duplicate content, unclear title, missing citation, accidental formatting or	Reminder, edit request, move or merge, label, temporary hide, or informal

Level	Typical examples	Possible response
	accessibility issue, low-level discourtesy.	correction.
Level 2 - serious	Repeated incivility, unsupported consequential claims, unwanted promotion or contact, copyright issue, non-immediate privacy breach, ignoring moderator instructions.	Remove or restrict content, formal warning, feature restriction, temporary suspension, or required acknowledgement.
Level 3 - severe or high risk	Identifiable survivor or case data, credible threat, doxxing, grooming or exploitation, discriminatory abuse, graphic illegal content, scam, phishing, malware, account takeover, ban evasion, or retaliation.	Immediate hide or removal, account lock or suspension, evidence preservation, safeguarding or security escalation, permanent ban, and referral to authorities where lawful and necessary.

Moderators should prioritise immediate safety, privacy, and prevention of further spread; consider severity, reach, intent, impact, vulnerability, repetition, prior warnings, and willingness to correct; use the least restrictive effective response unless urgent risk requires immediate containment; and limit reports and evidence to authorised people with a need to know.

Moderators may redact identifiers, add a safety label, correct categorisation, close a discussion, disable downloads, or remove content. Where evidence is needed for security, safeguarding, legal claims, or a lawful authority request, KOPŽI may preserve a restricted copy for a limited period.

13. Appeals and procedural fairness

- A member may appeal a material content restriction, suspension, or ban through info@recover-project.eu, normally within 30 days of notice.
- The appeal should identify the decision, explain the claimed error, and provide relevant non-sensitive context. Do not repeat removed personal data.
- Where practicable, a person not solely responsible for the original decision should review the appeal.
- The review may uphold, vary, or reverse the action. KOPŽI should provide a concise outcome and retain a limited audit record.
- Repeated identical appeals, abusive contact, or attempts to bypass restrictions may be closed without further review.

Nothing in this process limits a person's right to use another remedy available under the Terms of Use, data-protection law, platform law, or national law.

14. Safeguarding and legal escalation

Moderators are not investigators. When a report suggests imminent danger, exploitation, child abuse, serious violence, self-harm, a security incident, or another legally reportable matter, they should follow the operator's approved safeguarding and incident-response procedure.

29. Contain: restrict access to the content or account where necessary to reduce immediate harm.
30. Minimise: do not copy or circulate sensitive material beyond authorised responders.
31. Escalate: contact the designated safeguarding, privacy, security, or legal lead using the approved channel.
32. Refer: use local emergency, national referral, child-protection, or law-enforcement channels only where authorised, lawful, necessary, and proportionate.
33. Document: record essential facts, actions, authority, and timing without adding speculation or unnecessary personal data.
34. Support: communicate in a trauma-informed way and avoid promising an outcome that cannot be guaranteed.

15. Account closure and continuing duties

- Members remain responsible for content they submit and for maintaining copies they need for their own records, subject to confidentiality and licence rules.
- Deleting an account may not instantly remove all contributions, quotations, moderator records, backups, or copies held by other members. The Privacy Policy explains the applicable deletion and historical-content rules.
- Confidentiality, intellectual-property, professional-boundary, and non-retaliation duties continue after a member leaves the e-Hub.
- A member may request correction or removal of personal data through info@recover-project.eu. Urgent exposure of survivor or case data is treated as a priority removal concern.

16. Changes and acceptance

KOPŽI may update these Guidelines to reflect new features, risks, legal requirements, or community learning. Material changes should be dated, summarised, and communicated through the e-Hub. Where appropriate, members may be asked to acknowledge the revised version before continuing to post.

The version in force at the time of conduct will normally guide review, while urgent safety rules may apply immediately. Continuing to use the e-Hub after the effective date means that you accept the updated Guidelines, unless a different form of acknowledgement is required.

17. Member pre-post checklist

Check	Question to ask before posting
Purpose	Does this help professional learning, collaboration, or safe implementation of recovery approaches?
Identity	Could a person, service, location, or case be identified directly or by combining details?
Authority	Am I authorised to share this, and does the e-Hub audience need it?
Safety	Could this expose, stigmatise, retraumatise, locate, or invite unwanted contact with anyone?
Evidence	Have I separated evidence, experience, and opinion and cited consequential claims?
Rights	Do I own the content or have permission or a licence to share it?
Tone	Is the wording respectful, inclusive, non-sensational, and open to correction?
Tools	Have I removed hidden metadata and avoided sending sensitive information to AI or external tools?
Audience	Would I be comfortable if another member saved or forwarded this?
Pause	If I am uncertain, can I ask a moderator through a protected channel before posting?

18. Moderator response guide

Trigger	First action	Then assess
Identifiable survivor or case data	Hide access immediately; do not download unless necessary.	Reach, copies, urgency, safeguarding duty, and whether an affected person must be informed.
Threat or imminent harm	Escalate through the emergency or safeguarding protocol.	Credibility, immediacy, location if lawfully known, and authorised referral route.
Harassment or hate	Protect the target and restrict contact or content.	Severity, protected or vulnerable status, repetition, coordination, and retaliation risk.
Misinformation or unsafe practice	Add a warning or temporarily hide if harm is plausible.	Evidence quality, professional consequence, correction feasibility, and reach.
Spam, scam, phishing, or malware	Disable links or files and lock the suspicious account.	Affected users, credential exposure, related accounts, and security notification.
Copyright or ownership complaint	Restrict disputed material where appropriate.	Complainant authority, licence, attribution, counter-position, and applicable process.

For moderation, privacy, safeguarding, or security questions, use info@recover-project.eu. Never copy unnecessary sensitive content into ordinary email.