EPeKa

https://www.digitalvscorrupt.eu

WHISTLEBLOWER PROTECTION & ICT AGAINST CORRUPTION

EXPANDED TRAINING TOOLKIT FOR YOUTH WORKERS, CIVIL SOCIETY ACTORS AND EDUCATORS

Developed within the project "With Digitalisation Versus Corruption" (Erasmus+)

December 2025

ERASMUS-YOUTH-2023-CB
Project name: "With Digitalisation Versus Corruption" within the programme Erasmus Youth 2023 - Capacity building in the field of Youth - Western Balkans.

Project number: 101131572
The Project "With Digitalisation Versus Corruption" is co-funded by the European Union.
Coordinator:
EPEKA Scientific Research Association for Arts, Culture and Educational Programmes and Technology, Montenegro

Participating organizations:
- EPEKA Scientific Research Association for Arts, Culture and Educational Programmes and Technology, Serbia
- EPEKA Scientific Research Association for Arts, Culture and Educational Programmes and Technology, Social Enterprise, Slovenia
- EPEKA BERLIN EV, Germany
- UDRUZENJE AKUSTIKUM, Bosnia and Herzegovina
- INSTITUTE FOR APPLIED RESEARCH FOR BUSSINES, Republic of North Macedonia
- QENDRA OPEN DOORS, Albania
- FUNDACJA EUROPEJSKI INSTYTUT OUTSOURCINGU, Poland
- EUROPE FOR YOU, Czechia
- CENTER FOR EDUCATION AND TRAINING PRIZREN, Kosovo
- TRANSPARENCY INTERNATIONAL, Iceland
- PHIREN AMENCA INTERNATIONAL NETWORK, Belgium
- LYKIA IZCILIK VE DOGA SPORLARI KULUBU DERNEGI, Türkiye
- ARCIGAY APS, Italy
- Skupnost Občin Slovenije, Slovenia
- Institut Jožef Stefan, Slovenia

Authors:
- UDRUZENJE AKUSTIKUM, Bosnia and Herzegovina
- EPEKA Scientific Research Association for Arts, Culture and Educational Programmes and Technology, Montenegro
- EPEKA Scientific Research Association for Arts, Culture and Educational Programmes and Technology, Serbia
- EPEKA Scientific Research Association for Arts, Culture and Educational Programmes and Technology, Social Enterprise, Slovenia
- TRANSPARENCY INTERNATIONAL, Iceland

DISCLAIMER
Funded by the European Union. Views and opinions expressed are however 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.

table of contents

04 INTRODUCTION

05 INTRODUCTION AND LEARNING OUTCOMES

06 HOW TO USE THE TOOLKIT

07 SAFE FACILITATION PRINCIPLES

08 MODULE 1: UNDERSTANDING WHISTLEBLOWING

10 MODULE 2: LEGAL FRAMEWORKS AND PROTECTIONS

12 MODULE 3: DIGITAL SECURITY AND SAFE REPORTING (ICT)

14 MODULE 4: YOUTH WORK, ETHICS AND CIVIC COURAGE

15 MODULE 5: PRACTICAL STEPS FOR SAFE REPORTING

15 TRAINER GUIDANCE AND SAMPLE WORKSHOP AGENDA

23 RESOURCES AND CONCLUSION

INTRODUCTION

About this Toolkit

Whistleblowers play a crucial role in exposing corruption, fraud, abuse of power, conflicts of interest and violations of the public interest. By speaking up, they help protect communities, strengthen transparency and support democratic accountability. At the same time, reporting wrongdoing can expose individuals to stigma, retaliation, isolation and legal uncertainty.

This expanded toolkit brings together the original whistleblower training toolkit and the annex of practical tools prepared within the project "With Digitalisation Versus Corruption". It is designed as a practical resource for youth workers, civil society actors, trainers and educators who want to integrate anti-corruption learning into workshops, campaigns, youth exchanges and organisational development.

The toolkit combines core concepts, legal and ethical orientation, digital protection guidance, facilitation notes, case studies, ready-to-use exercises and printable templates. It is intentionally modular: sections can be delivered as a full training programme or used separately in short educational sessions.

What this document includes

The conceptual and training content from the original whistleblower toolkit.

The practical questionnaires, templates and exercises from the annex.

Additional trainer guidance, sample agenda, digital safety notes and facilitation support.

INTRODUCTION AND LEARNING OUTCOMES

Whistleblowers play a crucial role in exposing corruption, fraud, abuse of power, conflicts of interest and violations of the public interest. By speaking up, they help protect communities, strengthen transparency and support democratic accountability. At the same time, reporting wrongdoing can expose individuals to stigma, retaliation, isolation and legal uncertainty.

This expanded toolkit brings together the original whistleblower training toolkit and the annex of practical tools prepared within the project "With Digitalisation Versus Corruption". It is designed as a practical resource for youth workers, civil society actors, trainers and educators who want to integrate anti-corruption learning into workshops, campaigns, youth exchanges and organisational development.

The toolkit combines core concepts, legal and ethical orientation, digital protection guidance, facilitation notes, case studies, ready-to-use exercises and printable templates. It is intentionally modular: sections can be delivered as a full training programme or used separately in short educational sessions.

After working through the toolkit, participants should be able to:

- Explain what whistleblowing is and distinguish it from rumour, personal grievance or malicious disclosure.
- Recognise common forms of corruption and integrity risks that young people may encounter in education, employment, local services and community life.
- Understand the basic logic of whistleblower protection, including confidentiality, non-retaliation and access to reporting channels.
- Use safer digital habits when documenting or communicating sensitive concerns.
- Facilitate group discussion on ethics, civic courage and public interest without pressuring participants to disclose personal experiences.
- Guide participants through a basic risk-aware reporting process and signpost them toward trusted support structures.

HOW TO USE THE TOOLKIT

The toolkit is designed for flexible use. It can support a one-day introductory workshop, a multi-day training course, organisational capacity building, youth exchanges, peer-learning sessions or self-study. Trainers can select modules according to time, participant experience and local context.

Use format	How to use it
Full training curriculum	Run the modules in sequence as a one-day, two-day or extended programme.
Short workshop	Use one module and one practical exercise for a focused 60-90 minute session.
Youth work support material	Integrate case studies, ethics questions or digital safety content into broader civic education work.
Organisational development	Use the templates and reporting-system exercise to reflect on internal integrity mechanisms.

SAFE FACILITATION PRINCIPLES

Because this topic may touch on fear, injustice, workplace pressure and lived experience of corruption, facilitation matters as much as content.

- Create a psychologically safe learning space from the beginning. Clarify that participants do not need to share any personal or ongoing case.
- Use examples and scenarios rather than asking for real disclosures.
- Be careful with language. Not every suspicion is a proven fact, and not every reporting pathway is safe in every context.
- Encourage participants to verify facts, seek advice and understand risks before taking action.
- Adapt legal references, reporting bodies and referral pathways to the country where the workshop is delivered.
- Prepare a safeguarding plan in advance in case a participant reveals a live situation involving danger, harassment or serious misconduct.

Facilitator reminder

Do not ask: “Has anyone here reported corruption?”

Ask instead: “What could make reporting feel safe or unsafe for someone in this situation?”

MODULE 1: UNDERSTANDING WHISTLEBLOWING

Why this module matters

Many young people encounter unethical behaviour long before they learn the term whistleblowing. They may witness favouritism, misuse of project funds, bribery, nepotism, discrimination in access to opportunities, or quiet pressure to stay silent. Naming these experiences is the first step toward prevention and accountability.

What is whistleblowing?

Whistleblowing is the reporting of information about wrongdoing that affects the public interest or violates rules, duties or rights within an organisation, institution or community setting. Reports may be made internally, externally to competent authorities, or through protected channels provided by law or policy.

Key distinctions

A whistleblowing report is different from gossip, personal revenge or a vague accusation. Good practice requires a reasonable basis for concern, attention to evidence, and care for the safety of everyone involved.

Common forms of wrongdoing

- Corruption and bribery
- Fraud and false reporting
- Misuse of public or donor funds
- Abuse of power or conflicts of interest
- Environmental or public health risks
- Serious breaches of ethics, rules or rights

Core principles

- Public interest orientation
- Confidentiality and privacy
- Good-faith or reasonable-belief reporting

- Protection from retaliation
- Duty of institutions to receive and follow up reports

Questions for discussion

- Why do people stay silent even when they know something is wrong?
- What makes a young person trust or distrust a reporting system?
- How do power imbalances shape the decision to speak up?

Suggested activity (15 minutes)

Ask participants what first comes to mind when they hear the term “whistleblower”.

Map positive and negative associations on a flipchart.

Discuss why the term is often linked with both courage and risk.

MODULE 2: LEGAL FRAMEWORKS AND PROTECTIONS

Legal protection frameworks differ by country, but most credible systems share a common logic: people should be able to report wrongdoing through safe channels, their identity should be protected as far as possible, retaliation should be prohibited, and institutions should have clear duties to investigate or follow up.

Basic protection elements

Protection element	What it means in practice
Confidentiality	The identity of the reporting person should be protected and shared only on a strict need-to-know basis.
Non-retaliation	Dismissal, demotion, threats, harassment, exclusion or other reprisals should be prohibited.
Accessible channels	Internal and external mechanisms should be clear, usable and communicated in advance.
Follow-up duties	Reports should be acknowledged, assessed and processed in a timely and documented way.
Support	Advice, referral, legal aid or psychosocial support may be needed before, during and after reporting.

Choosing a reporting route

Route	Typical example	When it may be relevant
Internal reporting	An employer, school, organisation, ethics body or compliance channel	When the mechanism is credible and there is no immediate reason to fear cover-up or retaliation.
External reporting	A regulator, inspectorate, ombudsperson, anti-corruption body or another competent authority	When internal reporting is unsafe, ineffective, conflicted or legally inappropriate.

Confidential advice first	A trusted NGO, union, lawyer or support service	When the person needs help assessing risk, evidence and options before making a formal report.

Trainer notes

- Explain to participants that laws create a framework, but trust in practice depends on how institutions behave.
- Invite participants to identify the reporting bodies, ombudspersons, inspectorates or integrity agencies relevant in their own country.
- Stress that trainers should never give legal advice beyond their competence; they should signpost reliable services instead.

Mini-exercise

Ask participants to identify at least one reporting body, ombudsperson, inspectorate or integrity mechanism in their own country.
Let groups compare what information is easy to find and what remains unclear.

MODULE 3: DIGITAL SECURITY AND SAFE REPORTING (ICT)

Digital tools can help people document wrongdoing, communicate safely and preserve evidence. They can also expose identities through metadata, insecure devices, hacked accounts or careless sharing. For that reason, digital security should be treated as a practical safety skill, not as a technical luxury.

Common digital risks

- Tracking through personal devices, accounts or location services
- Metadata in photos, documents and message logs
- Unencrypted email or cloud storage
- Password reuse and weak account security
- Unsafe Wi-Fi networks and shared devices
- Phishing, social engineering and fake support requests

Digital tools at a glance

Type of tool	Examples	Typical use
Encrypted messaging	Signal, Threema	Safer private communication with end-to-end encryption
Encrypted email	Proton Mail, Tutanota	More secure email exchange for sensitive communication
Anonymous browsing	Tor Browser	Reduces traceability and supports safer access to public reporting pages
Secure file transfer	OnionShare	Allows safer sharing of documents without standard email attachments
Secure reporting platforms	GlobaLeaks, SecureDrop	Purpose-built systems for protected or anonymous submissions

Digital hygiene checklist

- Use long, unique passwords and enable two-factor authentication where possible.
- Separate sensitive communication from everyday accounts and casual apps.
- Remove metadata from files, photos and screenshots before sharing.
- Store evidence in an organised way and keep original versions unchanged.
- Be careful with forwarding, cloud sync and automatic backups.
- Assume that mainstream communication channels may reveal more information than you expect.

Practical exercise

Compare Signal and WhatsApp, or Proton Mail and Gmail.
Discuss which option offers stronger privacy protections, what metadata might still exist and what mistakes users commonly make.

MODULE 4:
YOUTH WORK, ETHICS AND CIVIC COURAGE

Whistleblowing is not only a legal matter; it is also an ethical question about responsibility, harm, solidarity and courage. Young people often struggle between loyalty to peers or institutions and loyalty to fairness, safety and the public good. Youth work can help them reflect on these dilemmas without forcing them into simplistic answers.

Values to explore

- Integrity: acting in line with values and responsibilities even when silence is easier.
- Civic courage: recognising that speaking up may involve discomfort, risk or social pressure.
- Empathy: understanding the impact of corruption and abuse on real people, especially those with less power.
- Responsibility: balancing the duty to avoid harm with the need to report serious wrongdoing.
- Solidarity: building support systems so that no one is left alone after raising a concern.

Reflection prompts

- When is it morally necessary to speak up?
- What happens when loyalty to a person conflicts with loyalty to fairness or safety?
- What support structures should exist before we expect young people to report wrongdoing?

MODULE 5: PRACTICAL STEPS FOR SAFE REPORTING

A safe reporting process is usually slower and more deliberate than people expect. The aim is not to act impulsively, but to understand the issue, protect the reporting person, preserve evidence, choose an appropriate channel and document the process.

1. Clarify the concern
What exactly happened? Who is affected? Is the issue illegal, unethical, unsafe or a breach of policy?

2. Record facts
Distinguish what you know, what you observed directly and what still needs verification.

3. Protect yourself
Review digital security, confidentiality risks and possible retaliation scenarios.

4. Seek advice
Consult a trusted support organisation, lawyer, union or experienced civil society actor.

5. Choose the channel
Assess whether internal, external or confidential preliminary advice is the safest first step.

6. Submit carefully
Share only what is necessary, keep copies and note dates, responses and reference numbers.

7. Monitor after reporting
Watch for retaliation, preserve records and seek psychosocial support if pressure escalates.

Important boundary
This toolkit supports preparedness and safer decision-making.
It does not encourage reckless disclosure or public naming without evidence, process or support.

TRAINER GUIDANCE AND SAMPLE WORKSHOP AGENDA

- Do not turn participants into investigators. The aim of the workshop is awareness, preparedness and safer decision-making.
- Use plain language and avoid overloading sessions with legal jargon.
- Plan at least one reflective activity, one practical exercise and one concrete take-away in each workshop block.
- When discussing tools, focus on principles of safety and suitability, not only on brand names.
- Always include a closing moment where participants can leave with support contacts, referral options or follow-up questions.

Sample one-day workshop agenda

Time	Session	Purpose
09:30-10:00	Opening, group agreement and expectations	Introduce the topic, create a safe framework, clarify confidentiality limits.
10:00-11:00	Module 1: Understanding whistleblowing	Definitions, myths, public-interest focus, first discussion exercise.
11:15-12:15	Module 2: Legal frameworks and protections	General protection logic, national adaptation, channel mapping.
12:15-13:00	Module 3: Digital security basics	Risk awareness, safe communication, comparison of tools.
14:00-15:00	Module 4: Ethics and civic courage	Values, dilemmas and reflection activity.
15:00-16:00	Module 5: Practical reporting steps	Risk-aware process, checklist, documentation and support.
16:00-17:00	Case studies and action planning	Small-group work, debrief, resources and evaluation.

CASE STUDIES FOR DISCUSSION AND ROLE-PLAY

Case studies help participants test their understanding without disclosing personal experiences. They work well in small groups, structured debates, reflection journals and role-play.

Case Study 1: Misuse of Youth Project Funds

A volunteer in a youth centre notices that invoices were submitted for equipment that was never purchased. The director explains that it is only temporary paperwork and asks the volunteer not to mention it.

Discussion questions

1. Which facts would need to be clarified before making an accusation?
2. What are the risks of reporting internally in this case?
3. What evidence should be preserved, and what should not be altered?
4. Who could provide confidential advice before a formal report is made?

Case Study 2: Environmental Hazard

A community member documents repeated illegal waste dumping near a river used by local residents. Municipal actors appear reluctant to intervene.

Discussion questions

1. What public-interest elements make this case urgent?
2. How can evidence be documented without exposing the person unnecessarily?
3. Would internal reporting be meaningful, or should an external route be considered?
4. Which digital risks should be considered when storing photos and location data?

Case Study 3: School Corruption and Nepotism

A student believes that scholarships are being awarded through personal connections rather than merit-based criteria. Teachers advise the student to keep quiet in order not to damage future opportunities.

Discussion questions

1. What distinguishes suspicion from proof in this example?
2. What support structures should exist for students who want to raise concerns?
3. When is it safer to report collectively or through a representative body?
4. How might fear of retaliation affect young people's willingness to act?

PRACTICAL TRAINING TOOLS AND PRINTABLE TEMPLATES

The following pages consolidate the practical annex into a set of ready-to-use forms and worksheets.

1. Pre-Training Questionnaire

Purpose: to assess participants' initial knowledge, confidence and assumptions about whistleblowing and corruption.

1. What does the term "whistleblower" mean to you?
2. Have you ever witnessed corruption or unethical behaviour in your environment?
3. Do you know any organisation where corruption can be reported safely?
4. How safe would you feel reporting corruption in your workplace or community?
5. What do you think are the biggest risks for whistleblowers?
6. Do you know whether your country has laws protecting whistleblowers?

Rate from 1 to 5:

Statement	1	2	3	4	5
I understand what whistleblowing is.	☐	☐	☐	☐	☐
I know how corruption can be reported more safely.	☐	☐	☐	☐	☐
I believe whistleblowers should be protected by law.	☐	☐	☐	☐	☐

2. Post-Training Evaluation Form

Please evaluate the workshop.

Rate from 1 (very poor) to 5 (excellent):

Statement	1	2	3	4	5
Content clarity	☐	☐	☐	☐	☐
Trainer performance	☐	☐	☐	☐	☐
Usefulness of the topic	☐	☐	☐	☐	☐
Practical value of exercises	☐	☐	☐	☐	☐
Overall satisfaction	☐	☐	☐	☐	☐

What did you learn during the training?

Which part was most useful?

What could be improved in future workshops?

---

3. Whistleblower Reporting Template

This template can be used to document a suspected corruption or integrity case before deciding on a reporting route.

Date of report	
Name (optional)	
Organisation / institution involved	
Description of the issue	
Location of the incident	
People involved (if known)	
Evidence available (documents, photos, emails)	
Already reported elsewhere?	YES / NO
Preferred contact method (optional)	

4. Safe Reporting Checklist

Stage	Key actions
Before reporting	Verify facts, collect evidence, protect your digital identity, use secure communication tools and seek advice from trusted NGOs or legal experts.
During reporting	Use official or anonymous channels where possible, keep copies of documents and limit sharing of sensitive information.
After reporting	Document any retaliation, seek support from trusted organisations and protect your privacy and mental wellbeing.

5. Digital Safety Comparison Worksheet

Compare two tools and discuss safety, privacy and usability.

Tool A	Tool B	Which is safer for sensitive communication and why?
Signal	WhatsApp	
Proton Mail	Gmail	

6. Corruption Risk Mapping Exercise

Instructions for groups:

- Divide participants into small groups and give each group a flipchart sheet.
- Ask them to identify possible corruption risks in education, healthcare, local government, youth programmes or the business sector.
- Have groups mark where corruption happens, who is affected and what can be done to report or prevent it.
- Invite each group to present their findings and compare patterns.

7. Group Exercise - Designing a Safe Reporting System

Participants work in groups and design a reporting system for an organisation. Each group should define:

- Reporting channels
- Protection measures
- Anonymity options
- Investigation procedures
- Follow-up communication
- Referral or support measures for the reporting person

8. Awareness Campaign Template

Campaign title	
Target audience	
Main message	
Communication channels	Social media / workshops / posters / video campaigns / other
Expected impact	

RESOURCES AND CONCLUSION

Suggested resources

- EU Directive 2019/1937 on the protection of persons who report breaches of Union law
- Council of Europe standards and recommendations related to protected reporting and integrity
- Whistleblowing International Network (WIN)
- Transparency International guidance on anti-corruption reporting and integrity systems
- Digital security resources from Access Now and the Electronic Frontier Foundation (EFF)
- Documentation for SecureDrop, GlobaLeaks and other secure reporting platforms

Conclusion

Whistleblowers protect communities, institutions and democracy. Supporting them means strengthening transparency, accountability and civic participation. For youth workers and civil society actors, the task is not only to explain the concept, but also to help create safer environments in which concerns can be raised responsibly and with support. Used well, this toolkit can help turn abstract anti-corruption values into practical skills, ethical reflection and collective action.

Introduction of participating organizations and their representatives in the project

Name and function	Organisation	Role/tasks
Zoran Dabetic	EPEKA Montenegro	Coordinator
Vedran Savić	UDRUZENJE AKUSTIKUM	Coordinator
Nermina Simoncic	EPEKA Slovenia	Coordinator
Stefan Simoncic	EPEKA Slovenia	Coordinator
Matej Tisaj	EPEKA RS	Coordinator
Milica Nedeljkovic	EPEKA RS	Assistant coordinator
Belma Muratovic	EPEKA Montenegro	Assistant coordinator
Jerica Lorenci	EPEKA Slovenia	Assistant coordinator
Atli Thor Fanndal	TRANSPARENCY INTERNATIONAL Iceland	Assistant coordinator

PARTNERS

EPEKA Montenegro (Lead organisation)
Scientific Research Association for Art, Cultural, Educational Programs and Technology EPEKA (Montenegro) operates in Berane, a rural area with high youth unemployment and limited access to non- formal education. Within DigitalVSCorrupt it coordinates overall delivery, management and monitoring, and leads national CB workshops focused on ICT supported transparency and community awareness in Montenegro.

EPEKA Slovenia
A non governmental social enterprise active in EU citizenship, youth work and inclusion. EPEKA Slovenia co-hosts the partner kick-off, supports management, and co-develops ICT based transparency modules inspired by the ERAR model; it also hosts the final conference and supports EU-level dissemination.

EPEKA Serbia
Youth - focused NGO from Niš with strong experience in mobility and inclusion (including Roma and migrant youth). In the project, EPEKA Serbia co-leads trainings, supports Kosovo–Serbia youth dialogue through joint activities with CET Prizren, and pilots local campaigns on integrity in public services.

EPEKA Germany
Member of the EPEKA network supporting intercultural learning and communication. Contributes to cross border dissemination, workshop design on civic engagement and media, and documentation of good practices across partners.

CET Prizren (Kosovo)
Center for Education and Training Prizren promotes democratic values and youth participation. In DigitalVSCorrupt it co-designs youth friendly training content, co-hosts CB workshops in Kosovo and collaborates with EPEKA Serbia to strengthen trust, dialogue and anticorruption literacy among youth.

Phiren Amenca (Belgium)
International Roma youth network with strong outreach and advocacy capacity. Leads EU level dissemination, supports inclusion measures across all activities, and mentors youth campaign teams to reach diverse audiences with inclusive narratives.

Transparency International Iceland
Brings global anticorruption know how, practical tools for risk mapping and reporting, and co-authors the youth work manual sections on corruption in public institutions and accountability pathways.

Institute for Applied Research (North Macedonia)
Supports the 'Corruption in Business' strand with sessions on procurement risks, conflicts of interest, and SME integrity pledges. Co-hosts national workshops with chambers/entrepreneurs.

QENDRA (Albania)
A youth oriented civil society centre engaging communities in non-formal education and civic action. Leads CB workshops in Albania and contributes case studies on local service integrity.

Europe for You (Czech Republic)
European civic organisation experienced in communication and youth mobilisation. Codesigns the campaign lab, supports creative dissemination formats and visual storytelling.

FEIO (Poland)
Education/outreach foundation contributing to research based activity design, quick polls and pre/post evaluation tools adaptable to youth settings.

AKUSTIKUM (Bosnia and Herzegovina)
Cultural organisation leveraging creative media and audio-visual methods. Co-leads the three 'video simulation' outputs (public sector, business, whistleblowing) including storyboarding and youth co-creation.

LIDSK (Turkey)
Youth development organisation focusing on civic skills and dialogue. Hosts CB workshops in Türkiye and contributes facilitation methods for diverse groups.

Arcigay (Italy)
National civil society organisation with expertise in rights based education and safe space facilitation. Contributes inclusion strategies, ethics protocols and campaign messaging on equality and integrity.

All partners collaborate via monthly coordination calls, shared templates and joint monitoring visits.

https://www.digitalvscorrupt.eu