Link Up

PUBLIC SERVICE AWARENESS MODULES

Co-funded by the European Union

2025-1-DE02-KA220-ADU-000350564

LINK UP: Digital Empowerment and Community Engagement for Third-Country National Women

2025-1-DE02-KA220-ADU-000350564

WP2: Public Service Awareness Modules

Module 1: Accessing e-government services

Module 1: Accessing e-government services

Module overview

Field	Details
Audience	Trainers, educators, social workers, and facilitators working with TCN women
Duration	3-5 hours
Delivery method	Face-to-face / Online / Blended
Scope	E-government systems, source verification, privacy, accessibility, safe facilitation, and referral boundaries
Lead partner(s)	Münchener Akademiker Plattform e.V. (Germany); Future Development Initiative (Belgium)

Purpose and professional stance

Public services may provide information, appointments, applications, payments, case updates, or evidence online. Trainers need enough system knowledge to explain these functions without turning a group session into account support, legal advice, or casework. They also need to design practice that protects privacy, preserves participant control, works on common devices, and points to verified human support.

E-government systems differ by authority, service, and eligibility route. This module therefore teaches a source-checking and facilitation method rather than a fixed sequence of portal clicks. Any live example must be checked before use.

TCN women are not a uniform group. Participants may bring substantial multilingual, professional, administrative, and digital expertise. Barriers may arise from portal design, language provision, disability access, device or connectivity constraints, unfamiliar administrative systems, identity requirements, previous harmful experiences, or limited access to trusted assistance. Trainers must avoid treating these structural conditions as personal deficits.



Trainer competencies

On successful completion, trainers can:

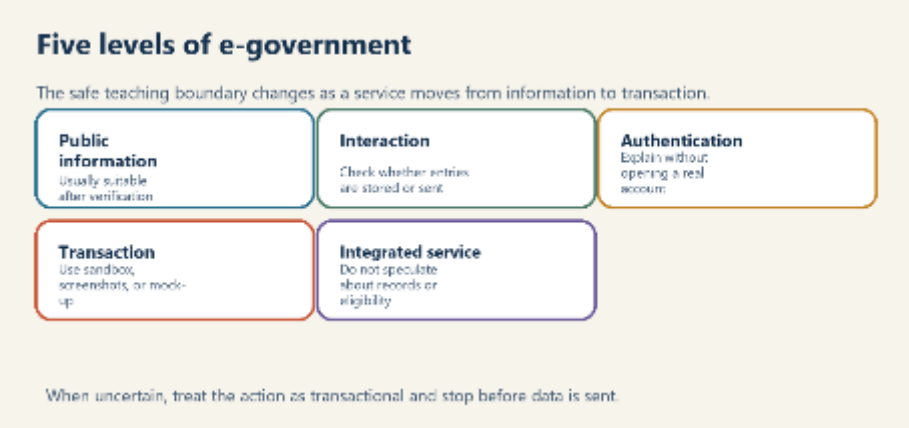
1. **Explain the domain:** distinguish public information, interaction, authentication, transaction, and integrated service levels, and accurately explain eID, portal states, and assisted routes.
2. **Facilitate safe practice:** plan and deliver a short, demo-only e-government activity in which participants retain control and no real account, submission, document, credential, or personal record is used.
3. **Protect privacy and safety:** apply data minimization, identify phishing and shared-device risks, interrupt unsafe disclosure, and document incidents without unnecessary personal data.
4. **Design for inclusion:** adapt one objective for mixed digital, language, literacy, disability, device, and bandwidth needs while avoiding stereotypes and public ranking.
5. **Evaluate sources:** verify an official source, identify a safe stopping point, distinguish public from transactional content, and prepare a current backup.
6. **Maintain professional boundaries:** separate procedural education from legal or case advice and make an appropriate referral when accuracy, authorization, safeguarding, or case responsibility exceeds the trainer role.

1. E-government domain foundation

1.1 System levels

E-government is not one type of website. A service may operate at one or more levels:

Level	Typical function	Trainer implication
Public information	Office hours, eligibility summaries, document lists, fees, rights, and contact details	Usually suitable for a live demonstration after source verification. Information can still be outdated or incomplete.
Interaction	Search, calculators, downloadable forms, chat, contact requests, or appointment availability	Check whether entries are stored or sent. Use fictional or blank demonstrations only.
Authentication	Account access through password, app, eID, code, or identity provider	Explain the process without opening a real account or displaying a credential. Identify support for people who cannot use the method.
Transaction	Application, booking, upload, declaration, payment, consent, or status action	Do not complete in group training. Use screenshots, a sandbox, a mock-up, or a fictional flow.
Integration or proactive service	Data is exchanged across authorities, a pre-filled service is offered, or a status triggers another process	Explain that data may move between bodies under defined rules. Do not speculate about a person's record, entitlement, or legal consequences.



Digital availability does not guarantee digital accessibility, entitlement, or successful completion. A portal may be one route among several, or it may depend on a separate in-person identity check.



1.2 Public information and transactions

The distinction determines what is safe to demonstrate.

- **Public information** can normally be viewed without identifying the visitor. It can be used to teach navigation, source checking, required document reading, fees, opening times, and support routes.
- **A transaction** changes or requests something, sends information, creates a record, reserves a time, uploads evidence, accepts terms, or makes a payment. Even a contact form or appointment search may transmit data.
- A page can move from public information to a transaction without an obvious warning. Trainers should identify and mark the stopping point in advance.
- A consent statement does not make group processing safe. Real transactions belong in a private, authorized support context, not in teaching practice.

Before using a page, ask: Does this action only retrieve public information, or could it store, send, match, reserve, pay, or change a record? If uncertain, treat it as transactional and stop before the action.



1.3 eID and authentication

Electronic identification (eID) is a mechanism for proving or linking identity online. Depending on the system, authentication may use a password, one-time code, identity card, mobile app, bank identity, biometric check, or a national or cross-border identity provider. Authentication proves access according to a system's rules; it does not by itself establish eligibility for a service.

Trainers should be able to explain:

- the difference between creating an account, proving identity, signing a declaration, and receiving a service decision;
- that passwords, personal identification numbers, recovery answers, QR login codes, and one-time codes are credentials and must not be shared;
- that access methods may require a compatible phone, phone number, card reader, app store account, address, or prior in-person registration;
- that failed access can result from technical, identity-matching, account, eligibility, or service problems, which a trainer should not diagnose by guessing; and
- that official assisted-digital, telephone, postal, proxy, or in-person routes may exist and must be verified through authoritative sources.

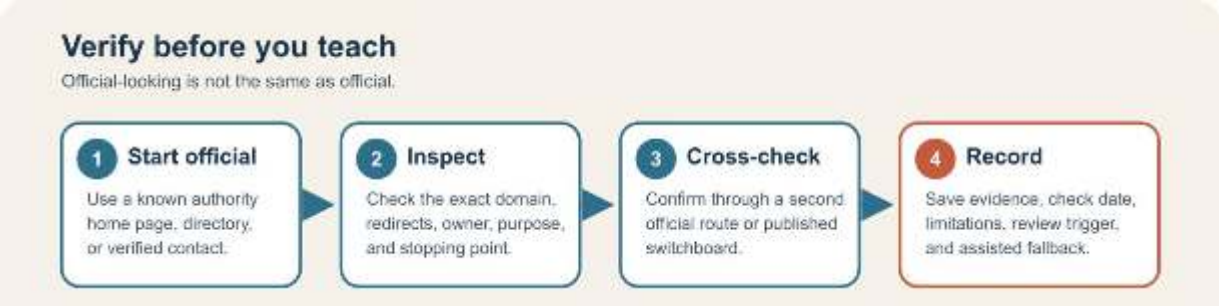
Never ask a participant to authenticate to demonstrate competence. Do not create, hold, recover, or operate an account on another person's behalf unless this is an authorized casework function governed by the trainer's organization and conducted outside the training activity.



1.4 Verifying an official source

Logos, professional design, search-engine ranking, advertising, and `https` do not prove that a page is official. Use a repeatable verification process:

1. Start from a known public authority home page, official government directory, or independently verified printed contact.
2. Read the full domain, including spelling and the ending. Check redirects and shortened links before relying on them.
3. Identify the authority responsible for the service and confirm that the page names that authority consistently.
4. Cross-check the service through a second official route, such as the authority directory, official switchboard, or a linked national or municipal portal.
5. Confirm current contact information, language options, accessibility information, costs, and assisted or offline routes.
6. Record the exact landing page, date checked, checker, evidence used, and any unresolved limitation.
7. Recheck shortly before delivery rather than assuming a saved link or screenshot remains current.



A third-party page can be useful context but must not be presented as the deciding authority for eligibility, deadlines, fees, or legal requirements. Search results marked as advertisements require particular caution.



1.5 Portal change and error states

Portals change labels, layouts, domains, authentication providers, language coverage, and required steps. Common states include:

- 404 or redirected pages after a service moves;
- planned maintenance, service outage, or a queue;
- session timeout or an expired link;
- browser, cookie, script, app-version, or device incompatibility;
- field-validation errors that do not identify the actual problem;
- identity details that do not match an authority record;
- a submission button that appears inactive;
- an uncertain submission with no visible receipt; and
- an inaccessible document, captcha, scanner, or upload requirement.

Trainer response should model uncertainty accurately. Do not invent a workaround, tell someone to change identity data, or repeat a real submission when its status is unclear. Return to a verified public entry point, check official service-status information, preserve any non-sensitive error wording, and identify an official support route. If teaching materials no longer match the live page, pause the demonstration and update the materials rather than asking participants to guess.



1.6 Shared devices and public connections

Shared or borrowed devices create risks from saved credentials, browser history, downloads, autofill, cached documents, notifications, screenshots, and another person's account. Private browsing reduces some local history but does not make a device, network, download, or transaction private.

In training:

- use public pages and fictional materials only;
- do not save passwords, identity details, downloads, or document images;
- prevent browser autofill from inserting a trainer's data;
- use separate fictional profiles for practice;
- clear fictional downloads and close tabs after the demonstration; and
- ensure peer support never requires handing over a real account or credential.

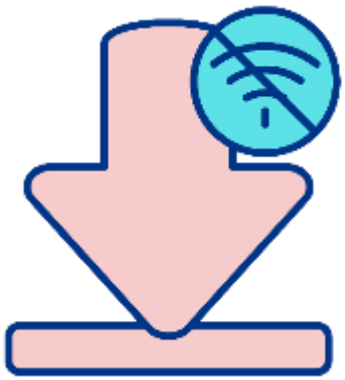
For real use outside training, trainers may explain published security guidance such as logging out and avoiding saved credentials but should direct the person to an official or authorized support setting if privacy cannot be assured.



1.7 Assisted and offline routes

An online route is not automatically the best or only route. Depending on local provision, alternatives may include an authority office, telephone service, postal form, library, municipal digital-support desk, accredited NGO, interpreter arrangement, disability support, or authorized representative process.

Validate each route. Record who provides it, what it can and cannot do, opening or response times, language and accessibility support, cost, appointment rules, authorization requirements, and how the details were verified. Never describe a community contact as authorized case support without evidence.



1.8 Fake sites, phishing, and manipulation

Phishing may arrive through email, SMS, messaging apps, social media, search advertisements, QR codes, or calls. Indicators include:

- a lookalike or misspelled domain;
- a shortened or concealed destination;
- an unexpected request to log in, pay, install software, enable remote access, or share a code;
- urgency, threat, secrecy, or a promise that discourages independent checking;
- unusual payment methods or accounts;
- poor alignment between sender, authority, service, and destination; or
- a page copied from a real authority but hosted elsewhere.

No single visual clue is decisive. The safe decision is to stop, avoid the supplied link or contact, open the service through a separately verified route, and use the authority's published reporting channel. Trainers should use invented examples that contain no live malicious link or scannable code.



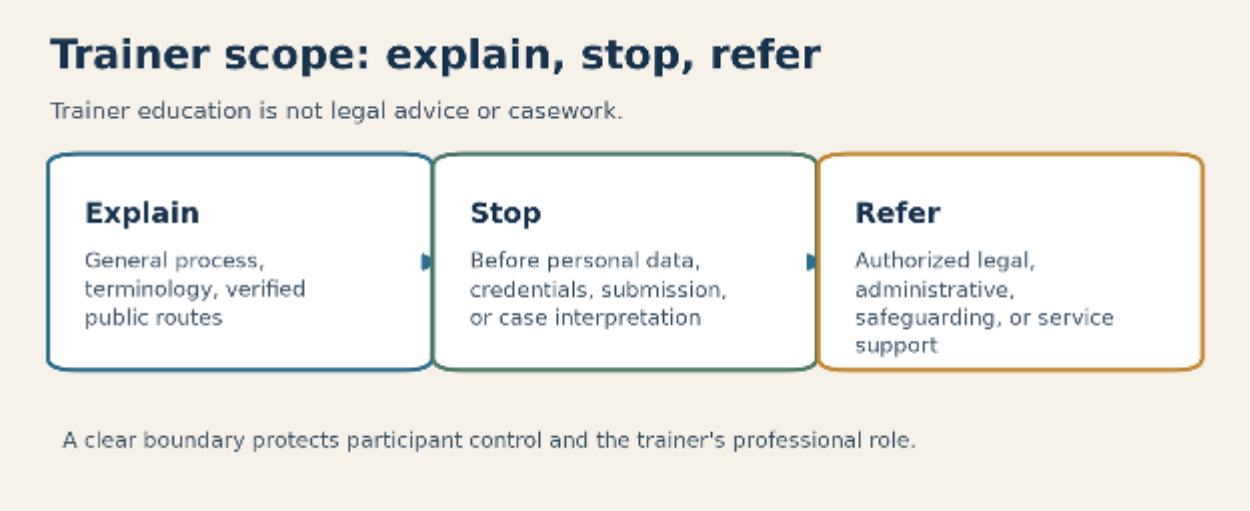
1.9 Trainer scope and referral boundary

A trainer may explain general terminology, demonstrate public navigation, help compare official routes, and teach a verification method. A trainer should not:

- determine legal status, entitlement, deadlines, appeal strategy, or likely case outcome;
- interpret an official decision as legal advice;

- recommend false, incomplete, or strategically altered information;
- access a case record or communicate as the participant without authorization;
- retain documents or credentials for later help; or
- imply that completing a workshop guarantees access to a service.

Use a transparent boundary statement: “I can explain the general process and help locate the official route. I cannot advise on your individual legal or administrative case. Let us identify the authorized service that can do that.”



Three-step trainer boundary: explain the general process, stop before personal data or case interpretation, and refer to authorized support.



2. Participant context and privacy-safe needs analysis

Needs analysis should improve design without creating a shadow case-management record. Collect only information necessary to choose format, pace, access support, and materials. Participation should be voluntary, and people should be able to request support privately.



Asset-based principles

- Ask what strategies, languages, devices, and support methods people already use.
- Do not infer competence from age, accent, literacy, education, clothing, country of origin, migration category, or length of residence.
- Separate unfamiliarity with one portal from general digital competence.
- Describe portal, language, access, and institutional barriers rather than labelling a person as “hard to reach” or “low ability.”
- Do not ask participants to disclose legal status, case history, benefit use, health information, identity numbers, or reasons for needing a service.
- Offer choices without requiring a public explanation.



Low-data methods

Method	Appropriate information	Privacy control
Anonymous access poll	Phone, computer, shared device, no device, internet or print preference	Use aggregate counts; do not attach names.
Choice cards	Prefer demonstration, paired pointing, individual practice, audio, print, larger text, or more time	Allow private selection and more than one choice.

Method	Appropriate information	Privacy control
Fictional task observation	Scrolling, opening a menu, identifying an authority, or returning to a start page	Observe a mock task; do not use a real service case.
Partner consultation	Aggregate language, scheduling, accessibility, childcare, or support patterns	Ask for trends, not participant files or case details.
Optional private access request	Interpreter, captioning, screen-reader, mobility, quiet-space, or other delivery adjustment	Route through the organization's approved accessibility process and restrict access.
Trainer resource scan	Device supply, charging, connectivity, staffing, room privacy, and referral capacity	Record organizational conditions, not participant identities.

Planning from the findings

Convert only aggregate findings into design decisions. For example, "six places need loan phones" is preferable to a named list in teaching notes. Prepare at least two ways to engage with the same safe objective. Avoid dividing people into publicly labelled ability groups; use optional support stations, adjustable task cards, and discreet trainer check-ins.

Do not collect information merely because it might be useful later. Set a deletion point for temporary access-planning data according to organizational policy.



3. Ethics, privacy, security, and safeguarding

3.1 Non-negotiable training rules

During any demonstration, trainer practice, or model workshop, do not:

- create or open a real government account;
- enter a real name, address, date of birth, identity number, password, recovery answer, or one-time code;

- upload or display an identity card, residence document, certificate, decision letter, medical record, payslip, or other personal file;
- submit a real form, application, appointment, declaration, consent, or payment;
- photograph, record, cast, or store a participant's screen or document;
- invite participants to describe their case in the group;
- use a trainer's personal account as a demonstration shortcut; or
- allow urgency or course completion pressure to override a participant's choice to pause, skip, observe, or leave.

Use public pages, redacted and rights-cleared screenshots, sample forms, fictional profiles, a controlled mock-up, or an official training environment. Check mock data carefully so it cannot be mistaken for a real person, live credential, valid identifier, or active contact.



3.2 Data minimization

Data minimization means collecting and accessing only what is necessary for a defined purpose. For training design:

1. State the purpose before collecting anything.
2. Ask whether the session can run without the data; if yes, do not collect it.
3. Prefer anonymous aggregate information.
4. Limit access and retention under organizational policy.
5. Do not reuse attendance or access data for case discussion, publicity, or evaluation without a valid process.
6. Record training quality through non-identifying observations such as timing, material clarity, and support demand.

GDPR principles are a professional design reference, not a substitute for the organization's data-protection assessment or legal advice.



3.3 Learner control and informed participation

In facilitated sessions, learner control means that the participant controls her device, decides whether to take part in an activity, and can stop without penalty or public explanation. Consent does not remove the trainer's duty to prevent an unsafe activity. A participant cannot make display of a real password or document appropriate for group practice by agreeing to it.

Trainers should announce the fictional-data boundary before devices are opened, repeat it at transaction stopping points, and provide a non-device observation route that meets the same session purpose.



3.4 Trainer decision guide

Situation	Immediate trainer decision	Follow-up
A participant starts showing a real document	Pause, shield the material from view, ask the person to put it away, and return to fictional data without blame.	Offer a verified private support route if requested. Do not record document details.
A participant opens a real login page	Stop before credentials are entered and close or move away from the page.	Restate the demo-only boundary and use a mock-up.

Situation	Immediate trainer decision	Follow-up
A participant discloses a password or code	Stop display and sharing; do not repeat, copy, or test it.	Follow the organization's security incident route and direct the person to official credential-protection guidance. Record only what policy requires.
A participant asks whether she is legally eligible	Explain the trainer boundary and locate an official or qualified advice route.	Do not predict eligibility or interpret the case.
A suspicious message appears	Do not click, reply, forward, scan, or call the supplied contact.	Use a separately verified authority channel and its reporting process.
The live portal conflicts with the lesson	Pause the lesson step and name the uncertainty.	Verify the current source, use the prepared offline backup, and version the correction.
A portal is inaccessible to a participant	Offer an equivalent format or supported route rather than requiring another participant to take control.	Record the access barrier without personal case data and report it through the approved channel.
A participant appears distressed or coerced	Stop the activity, preserve choice and privacy, and follow the organization's safeguarding procedure.	Share only necessary information with the designated safeguarding lead. Do not investigate in the group.

3.5 Safeguarding and incident response

Trainers must know the organization's named safeguarding contact, emergency procedure, data-incident process, and referral limits before delivery. If a concern arises:

1. Make the immediate environment safer without promising secrecy that cannot be kept.
2. Listen only enough to identify the next safe action; do not investigate or request evidence.
3. Explain what must be shared, with whom, and why, when it is safe to do so.
4. Use the approved reporting route and the minimum necessary information.
5. Keep teaching notes separate from safeguarding or case records.
6. Debrief through professional supervision, not with other participants.

Emergency and reporting duties vary. Trainers must follow current local law and organizational policy rather than improvising from this module.



4. Guided source-verification practice

Use this self-study practice to examine one public-information service and one assisted or offline route. Do not test a real transaction.

Validation procedure

1. **Define scope:** identify the service topic, intended teaching use, and what will not be covered.
2. **Establish ownership:** reach the service from an official authority home page or directory and identify the responsible public body.
3. **Check the address:** inspect the exact domain, redirects, certificate warnings, and whether search results include advertisements or lookalikes.
4. **Cross-check:** confirm the service through a second independent official route or the authority's published switchboard.
5. **Inspect public content:** check purpose, date cues, fees, documents, deadlines, language provision, accessibility statement, and the point at which authentication or data entry begins.
6. **Test access modes:** inspect the public page on a narrow phone viewport and a computer, at 200 percent zoom, with keyboard navigation where applicable, and under reduced bandwidth if feasible.
7. **Verify support:** confirm an official telephone, office, postal, assisted-digital, interpreter, disability, or complaints route and any limits or costs.
8. **Prepare a backup:** save a dated, rights-cleared fictional or blank teaching representation and a print route that does not expose personal data.
9. **Record evidence:** note exact URLs, the check date, methods, known limitations, and change triggers.
10. **Decide:** mark the resource `suitable for the defined example`, `suitable with a stated limitation`, or `do not use`.



Source-checking worksheet

Record field	Required entry
Service and responsible authority	Formal names
Intended training use	Public-information step only
Official landing page	Exact URL and route used to verify it
Cross-check evidence	Second official route or verified switchboard
Transaction stopping point	The first action that could authenticate, store, send, reserve, pay, or change data
Access review	Phone, desktop, zoom, keyboard, language, document format, and known barriers
Assisted or offline route	Provider, contact, function, limits, hours, cost, and authorization status
Safety review	Lookalikes, redirects, login, uploads, payments, shared-device risks, and reporting route
Decision	Approved, limited, or do not use, with reason
Control information	Checked date and change trigger

Do not approve a resource if authority ownership cannot be established, the domain is suspicious, essential requirements conflict across official sources, or no safe stopping point can be defined. Escalate unresolved accuracy questions to the named authority or designated resource owner.



5. Accessible instructional design

5.1 Design from the objective

A trainer plan should specify one observable, safe action, such as comparing two source routes or identifying the transaction stopping point in a fictional flow. Do not define success as completing a real application.

Use a predictable sequence:

1. orient to purpose, boundaries, and choices;
2. model one short action and verbalize the decision;
3. offer supported practice with fictional material;
4. invite performance in more than one mode;
5. give specific feedback on the decision and safety behaviour; and
6. close with a verified human-support route.



5.2 Accessibility requirements

- Use meaningful headings, descriptive link text, consistent labels, and one principal action per step.
- Use plain language for trainer-created directions and explain unavoidable official terminology without changing its legal meaning.
- Pair icons and colour with text; never use colour alone to communicate status.
- Maintain readable contrast, visible focus, keyboard access, logical reading order, and reflow at 200 percent zoom.
- Add concise alt text to informative images. Mark decorative images as decorative in the authoring tool.
- Caption videos accurately and provide a transcript. Do not rely on auto-captions without review.
- Avoid timed interactions. If a timer is unavoidable in an external system, explain extension and alternative routes.
- Provide accessible documents rather than image-only PDFs. Check tags, headings, reading order, link labels, and selectable text.
- Read instructions aloud when useful, while retaining text for participants who prefer reading.
- Build in processing time and quiet participation methods.

For language and literacy adaptation, LASLLIAM can inform differentiated scaffolding for adult migrants. A2-B1 plain-language materials and multilingual support may be appropriate in some settings, but the trainer must establish local needs rather than assume a level.



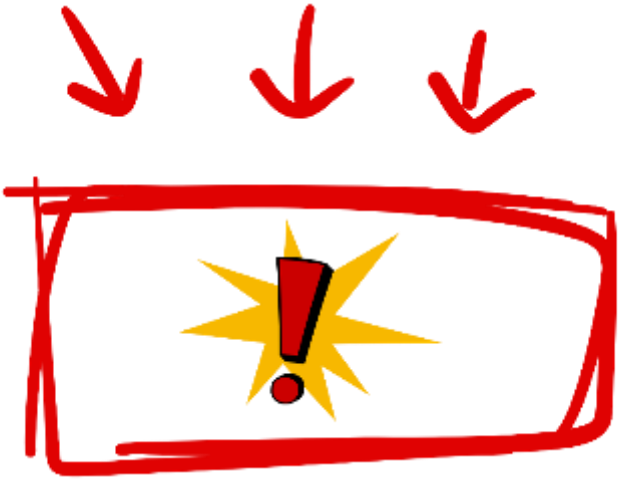
5.3 Mixed-level differentiation

Keep the same safety standard and core objective while varying support:

- **More structure:** numbered screenshots, a pre-opened verified page, one action per card, trainer modelling, and a paired pointer role.
- **Standard route:** a short fictional scenario, verified starting link, and decision checklist.

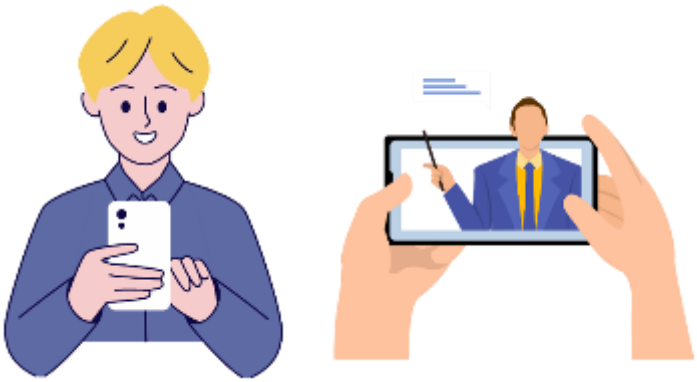
- **Greater challenge:** compare two official routes, explain a change or error state, or evaluate the adequacy of an assisted route.
- **Alternative performance:** spoken explanation, pointing, ordered cards, keyboard navigation, or a written decision note.

Do not make faster participants informal caseworkers. Peer support can cover fictional navigation, but each person retains device control, and no peer sees real information. Avoid public ability labels and competition based on speed.



5.4 Phone-first design

- Design first for a narrow screen, touch input, mobile menus, software keyboards, limited storage, and interrupted connectivity.
- Keep URLs short only through verified official redirects or printed QR codes whose destination is written beside them. Recheck every QR destination before use.
- Do not require scanning a code when the session is displayed on the same phone; provide a tappable and readable route.
- Ensure screenshots show the relevant context, domain, and date, not only a cropped button.
- Explain when the mobile and desktop paths differ; do not force identical steps.
- Keep fictional downloads small and identify where a phone stores them.



5.5 Print and low-bandwidth adaptation

A print pack should include a dated source note, fictional scenario, numbered screenshots or text equivalents, authority and domain cues, the transaction stopping point, an assisted route, and a warning that live details must be rechecked. It must not look like an official application or contain a functional credential.

For low bandwidth, use compressed accessible images, transcripts instead of mandatory video, downloadable instructions, a prepared offline mock-up, and a no-device route to the same objective. Never represent a static copy as live or current; display the capture date and verification status.



6. Facilitation and troubleshooting

Facilitation standards

- State purpose, demo-only boundaries, choices, and referral limits before practice.
- Demonstrate slowly enough to expose decisions, not merely clicks.
- Keep instructions observable and neutral: “Find the authority name” rather than “This is easy.”
- Normalize portal difficulty without lowering expectations or using deficit framing.
- Check understanding through trainer-observed fictional performance, not personal disclosure.
- Use groups of approximately 6-10 participants per trainer for device practice; add a co-trainer or rotate small groups when support demand is higher.
- Plan private questions without turning the session into individual casework.
- End with accurate uncertainty where necessary: “This needs verification” is safer than a confident guess.



Troubleshooting guide

Problem	Safe trainer response	Avoid
Saved link no longer works	Return to the verified authority home page, search again, and record the change.	Substituting the first similar search result.
Screenshot differs from the portal	Pause, identify the changed element, use the backup, and update the version after verification.	Asking participants to click around until it works.
Page lacks a familiar language	Check official language options and verified support. Use translation as navigation support and verify consequential details in the authoritative version.	Presenting machine translation as authoritative legal wording.
Public page reaches login	Stop before login and explain the boundary. Identify private authorized support or an offline route.	Demonstrating with any real account.
Requirement or fee is unclear	Record the uncertainty and use an official contact or qualified referral.	Guessing from another participant's case.
Error follows a real submission outside training	Do not repeat the submission. Direct the person to a verified status or support route in a private setting.	Taking over the account in class.
Captcha or document is inaccessible	Use the authority's accessibility or assisted-service route and document the barrier through the approved process.	Requiring a peer to view private data.
Suspicious message creates urgency	Stop interaction and independently reach the authority.	Clicking to "check whether it is real."
Internet fails	Use the dated offline exemplar and focus on source and safety decisions.	Claiming the cached content is current.

Problem	Safe trainer response	Avoid
No private device is available	Use fictional print or projected material and provide a verified assisted route.	Treating shared login as the only option.

7. Quality assurance and maintenance

Pre-delivery check

The designated resource owner should confirm:

- the learning objective is trainer-focused and observable;
- the model workshop clearly states its purpose and boundaries;
- no activity requests real data, account access, upload, submission, or payment;
- live sources passed the verification procedure and show a checked date;
- assisted and offline routes are current and their limits are described;
- phone, print, low-bandwidth, language, and accessibility routes are available;
- screenshots and mock data are fictional, rights-cleared, dated, and free of hidden personal data;
- phishing examples contain no live malicious destination;
- scope and safeguarding referrals name current organizational roles.



Maintenance cycle

- Recheck live links and stopping points within 48 hours before delivery.
- Conduct a documented full review at least every six months.
- Review immediately after a domain, authority, fee, eligibility, eID, interface, accessibility, security, or referral change.
- Assign a named content owner and backup owner.
- Keep version, checked date, evidence, and known limitations with each live example.

- Withdraw materials that cannot be verified; do not leave them published with only a general warning.
- Record non-identifying delivery feedback, incidents, access barriers, and portal changes in the approved quality system.

Quality review should test both correctness and teachability. A technically accurate resource is not ready if a trainer cannot identify the safe stopping point, explain uncertainty, provide an accessible alternative, or locate qualified help.



8. Model workshop for trainer critique

This 75-minute model workshop lets trainers examine the module's facilitation, safety, and inclusion principles in practice.

Hypothetical context: 6-10 adult participants, mixed phone access, no real accounts, one verified public-information page, fictional profiles, and a print backup.

Time	Exemplar trainer move	Safety and inclusion evidence for trainers to inspect
0-8 min	Establish the limited objective, participant choices, demo-only rule, and scope boundary.	Observation is an equal option; no reason for opting out is requested.
8-20 min	Model how to reach the authority from a verified start point and distinguish public information from the transaction stopping point.	Full domain and authority are visible; the trainer verbalizes why `https` and a logo are insufficient.
20-35 min	Facilitate paired analysis of a fictional service need using a public page and printed equivalent.	One person retains device control; profiles contain no real identifiers; roles can change without speed ranking.

Time	Exemplar trainer move	Safety and inclusion evidence for trainers to inspect
35-48 min	Compare an invented suspicious message with the independently reached official route.	The example has no live link or code; participants are not asked to inspect their own messages.
48-62 min	Introduce a planned portal-change or error card and ask groups to choose a safe trainer-supported response.	Expected response includes pause, verification, backup, and official support, not improvisation.
62-70 min	Use a fictional observation prompt to check whether the source, stopping point, and help route can be identified.	Performance can be spoken, pointed, ordered on cards, or demonstrated; no transaction occurs.
70-75 min	Close with verified assisted and offline routes and restate the limit of workshop support.	Contacts have a checked date and stated function; no individual cases are discussed.

Trainer analysis prompts

Use these prompts to critique the model workshop:

1. Where does the exemplar protect participant control, and where could control still be weakened by room layout, pacing, pairing, or trainer language?
2. What evidence shows that the public page and help route are current and authoritative?
3. Which moment carries the greatest privacy or safeguarding risk, and what preventive instruction should come immediately before it?
4. How would the plan change for screen-reader use, emerging print literacy, no personal phone, low bandwidth, or a participant ready for more challenge?
5. Which trainer statements explain general process, and which could drift into legal or case advice?
6. Does the fictional observation prompt produce evidence of a safe decision, or only recall of a click sequence?
7. What should be removed or shortened to keep the example focused and safe?



9. Trainer quiz

1. Participant control

During fictional paired practice, one participant says she would rather observe and her partner reaches for her phone. What is the best trainer response?

- A. Allow the partner to control the phone because the activity contains no login.
- B. Ask the participant to explain publicly why she does not want to practise.
- C. Stop the handover, confirm that observing is an equal option, and offer a trainer device or printed route if she later chooses to participate.
- D. Exempt the pair from the session objective and continue with the rest of the group.

2. Demo-only practice

A trainer wants to demonstrate an appointment portal whose calendar appears only after account authentication. What is the best design decision?

- A. Use a dated mock-up or official sandbox and stop the live demonstration before authentication.
- B. Log in with the trainer's account while hiding the password from the projector.
- C. Invite a volunteer to log in while the rest of the group looks away.
- D. Create a shared course account using invented identity information.

3. Source verification

A government-looking service page is the first search result and uses `https`. What should the trainer do before approving it for a session?

- A. Approve it because encryption and search ranking provide sufficient evidence.
- B. Approve it if its logo matches an authority's printed leaflet.
- C. Ask a partner organization whether staff have seen the page before.
- D. Reach it from a known authority route, inspect the exact domain and redirects, confirm ownership, and cross-check through a second official route.

4. Phishing response

In a workshop, a participant shows an unexpected message demanding an immediate fee through a government-branded link. What is the best trainer decision?

- A. Open the link on the trainer's device to inspect the payment page safely.
- B. Ask her not to use the message, move the discussion away from personal details, and verify the service through an independently sourced official route.
- C. Forward the message to the group so everyone can compare the sender address.
- D. Advise deletion immediately without checking whether the authority has a reporting process.

5. Source currency

A saved public-service link worked when it was last checked. What should a trainer do before using it in a session?

- A. Use it because it passed an earlier review.
- B. Check only that the link opens on the trainer's laptop.
- C. Verify the authority, function, limits, mobile access, assisted route, and current contact details before use.
- D. Replace it with the first current search result.

6. Mixed needs

A group includes confident smartphone users, participants who prefer print, and a screen-reader user. Which plan is strongest?

- A. Divide the group publicly into basic and advanced tables and give the screen-reader user a peer operator.
- B. Keep one safe decision objective, offer equivalent phone, accessible digital, and print performances, and vary scaffolding without public ranking.
- C. Demonstrate only on a projector, so every participant receives identical instruction.
- D. Let confident users finish a real transaction while others use the fictional task.

7. Data minimization

Which pre-session needs-analysis approach best applies data minimization?

- A. Collect names, residence categories, and target services in case individual support is needed later.
- B. Ask the referring partner to send participants' case notes to help the trainer choose examples.
- C. Record each participant's digital skill score and immigration situation in the attendance sheet.
- D. Gather anonymous aggregate device and format preferences, use the approved private route for access adjustments, and collect no case details.

8. Legal and case boundaries

A participant asks whether an error message means her application will be refused under local law. What is the best trainer response?

- A. Explain that the trainer cannot interpret her case or predict the decision, help locate official status support, and refer legal questions to a qualified service.
- B. Explain the most likely legal outcome based on previous participants' experiences.
- C. Ask to inspect her account privately after the workshop before deciding whether to refer.
- D. Tell her that technical errors never affect administrative deadlines.

9. Portal change

Minutes before a session, the verified portal layout no longer matches the prepared screenshots. What should the trainer do?

- A. Use the screenshots without mentioning the difference because the objective is general.
- B. Pause the live sequence, verify the current route and stopping point, use the dated backup if needed, and update the controlled materials before reuse.
- C. Ask participants to explore the new layout and report which route seems correct.
- D. Switch to a similar unofficial guide that still matches the screenshots.

10. Safe facilitation plan

Which approach best applies this module's guidance in a facilitated session?

- A. Ask participants to memorize e-government system levels before viewing a portal.
- B. Teach the current menu sequence as the correct route for every future session.
- C. Use a fictional activity that verifies the source, protects participant control, supports equivalent access, and stops or refers appropriately.
- D. Require every participant to complete the same online form independently.

10. References

1. European Commission, Joint Research Centre. European Framework for the Digital Competence of Educators: DigCompEdu.
2. Vuorikari, R., Kluzer, S., and Punie, Y. DigComp 2.2: The Digital Competence Framework for Citizens - With New Examples of Knowledge, Skills and Attitudes. Publications Office of the European Union, 2022.
3. European Union. Regulation (EU) 2016/679, Article 5: Principles Relating to Processing of Personal Data.
4. World Wide Web Consortium, Web Accessibility Initiative. How to Meet WCAG 2.2 (Quick Reference).
5. Council of Europe. Literacy and Second Language Learning for the Linguistic Integration of Adult Migrants (LASLLIAM).
6. European Commission. The European Digital Identity Regulation.
7. European Union Agency for Cybersecurity. Phishing.
8. World Wide Web Consortium, Web Accessibility Initiative. Understanding WCAG 2.2.
9. European Commission. eGovernment Benchmark.

LINK UP: Digital Empowerment and Community Engagement for Third-Country National Women

2025-1-DE02-KA220-ADU-000350564

WP2: Public Service Awareness Modules

Module 2: E-health literacy

Module 2: E-health literacy

Module overview

Field	Details
Audience	Trainers, educators, social workers, and facilitators working with TCN women
Duration	4-6 hours
Delivery method	Face-to-face / Online / Blended
Scope	Digital health-information navigation, critical evaluation, privacy, inclusion, and safe referral boundaries
Lead partner(s)	EduChange Network (Austria)

Purpose and limits



This module prepares trainers to facilitate safe, inclusive e-health literacy sessions with TCN women. It develops digital and facilitation competence; it does not prepare trainers to diagnose, interpret test results, recommend treatment, assess clinical urgency, or provide medical, legal, or case-management advice.

The model workshop gives trainers a structured case for analysing facilitation decisions with public and fictional material.

Core safeguards:

- use public information, fictional data, prepared screenshots, or a fictional portal;
- never require personal health disclosure;
- never access a participant's portal, record, appointment, prescription, or real health form;
- use current official provider, interpreter, safeguarding, and emergency routes; and

- stop a training task when urgent help may be needed and activate the organization's official procedure without diagnosing or triaging.



Trainer competencies

By completing the module, the trainer can:

1. **Map the e-health domain:** accurately distinguish health information literacy from clinical decision-making and map national, regional, local, and provider-specific information and service routes.
2. **Evaluate sources and misinformation:** apply the expanded P-A-D-S method to compare public-health, provider, civil-society, commercial, and influencer content, then justify a resource decision with evidence.
3. **Protect confidentiality and consent:** design practice that uses no personal health data, explain portal and shared-device boundaries, and manage interpreter consent and confidentiality appropriately.
4. **Facilitate inclusively:** adapt an e-health session for language, literacy, disability, culture, phone access, low bandwidth, and print use without deficit framing or forced disclosure.
5. **Maintain professional boundaries:** respond safely to requests for diagnosis, treatment, test interpretation, or triage and activate validated urgent, emergency, safeguarding, and routine referral routes.
6. **Correct misinformation without shame:** use a calm, evidence-led dialogue that preserves dignity, addresses commercial influence, and supports digital well-being.

1. Trainer foundation

1.1 Health information literacy

Health information literacy is the capacity to **find, understand, appraise, and use** information and services in ways that support informed contact with appropriate care. In e-health settings, it also includes navigating interfaces, recognizing data requests, managing privacy, comparing claims, and knowing when a digital search should stop.

It is shaped by the system as much as by the individual. Dense language, inaccessible design, unfamiliar service structures, unstable migration circumstances, cost, limited data, and changing eligibility rules can create barriers. A trainer therefore improves the task and environment rather than labelling a person as having a deficit.

A safe training task supports a person to locate and assess a route. It does not ask the person to apply online content to a diagnosis or treatment decision. A page can be trustworthy and still be inappropriate for a person's jurisdiction, language, access rights, age group, or immediate situation.



1.2 Map the e-health ecosystem

Do not present e-health as one website. Distinguish the relevant system layers and responsible providers.

System layer	Typical functions	Trainer checks
National	Public-health guidance, entitlements, prevention, national directories, emergency information	Authority, jurisdiction, language versions, review date, accessibility
Regional or municipal	Local service directories, public-health programmes, eligibility and referral routes	Geographic coverage, residency rules, contact route, current service details

System layer	Typical functions	Trainer checks
Provider-specific	Clinic information, appointment instructions, patient portal, telehealth	Public versus private areas, account requirements, costs, data collection, support channel
Professional or civil-society	Recognized professional guidance, patient support, specialist helplines	Governance, funding, evidence, remit, independence, escalation route
Commercial platform	Search, booking, symptom content, products, advertising	Sponsorship, ranking logic, fees, profiling, data use, claim quality
Social or influencer channel	Personal experience, community explanation, rapid sharing	Identity and expertise, evidence, commercial ties, emotional pressure, correction history

Terms such as “official,” “free,” “covered,” “doctor,” and “emergency” may have different local meanings. Confirm them rather than translating them literally.

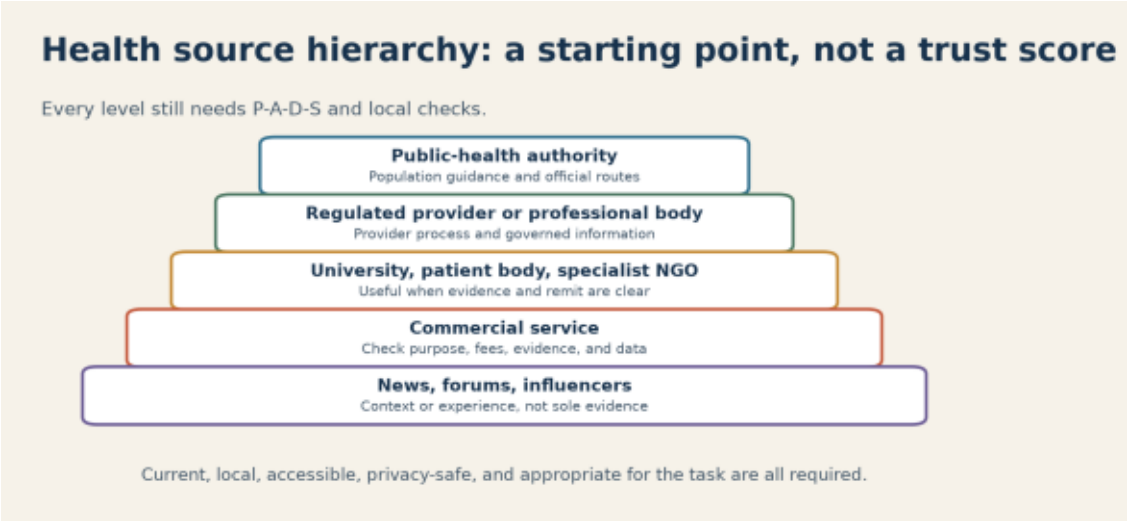


1.3 Use a source hierarchy without blind trust

Use the hierarchy as a starting point, not a substitute for evaluation:

1. **Current competent public-health authority:** usually preferred for population guidance and official service routes within its jurisdiction.
2. **Regulated healthcare provider or professional body:** often appropriate for provider processes or professionally governed information.
3. **University, evidence-based patient organization, or established specialist NGO:** potentially valuable where authorship, evidence, funding, and remit are clear.
4. **Commercial health or booking service:** may be usable when its purpose, fees, advertising, evidence, and data practices are transparent.

5. **News, social media, forums, testimonials, and influencer content:** useful for understanding questions or experiences, but not sufficient evidence for a health claim.



Public bodies can host outdated pages, and commercial pages can reproduce accurate material. The decision must consider currency, jurisdiction, purpose, evidence, accessibility, privacy, and the action the trainer intends to demonstrate.



1.4 Apply P-A-D-S in depth

P-A-D-S is a memorable first-pass evaluation method. Trainers should model the questions below rather than using publisher status or page appearance as a shortcut.

Check	Deeper questions	Warning signs	Safe trainer decision
P - Publisher	Who is legally or professionally	No accountable organization;	Verify identity on an independent

Check	Deeper questions	Warning signs	Safe trainer decision
	responsible? Is authorship visible? What is the publisher's jurisdiction, expertise, governance, and funding?	copied logo; unclear author; hidden sponsorship	official channel and compare with another competent source
A - Aim	Is the content informing, recruiting, selling, collecting data, entertaining, or influencing behaviour? Who benefits? Are adverts and affiliate links labelled?	Miracle or guaranteed outcome; urgency to buy; fear or shame; request to abandon professional care	State the purpose plainly; do not use the source as sole support for a health claim
D - Date	When was the content produced, clinically reviewed, and last updated? Have service routes or eligibility rules changed?	No date; old screenshots; broken routes; comments mistaken for an update	Check current official information and record a last-validated date
S - Support	What evidence supports the claim? Are limitations and uncertainty stated? Is there a routine professional route and a separate urgent route? Is the advice appropriate to this country and audience?	Testimonials presented as proof; single study overstated; no limitations; no contact or safety route	Triangulate with an independent source and direct personal questions to a qualified service

Add four cross-checks to every P-A-D-S review:

- **Jurisdiction:** Is the information valid where the session takes place?
- **Accessibility:** Can people perceive, understand, navigate, and use it on the available device?
- **Privacy:** What data, cookies, account, location, or permissions does it request?
- **Equity:** Could cost, eligibility, language, gender assumptions, or disability exclude the intended group?



P-A-D-S source check: publisher, aim, date, and support, with jurisdiction, accessibility, privacy, and equity cross-checks.



1.5 Patient portals and privacy boundaries

A patient portal can contain diagnoses, results, messages, prescriptions, appointment history, identifiers, insurance details, and proxy access to a child's record. Even a brief screen share can expose sensitive information.

During any training connected to this module:

- use a fictional prototype, vendor sandbox approved for training, or static screenshots containing invented data;
- do not ask anyone to log in, reveal a password, share a one-time code, download a record, or change a real appointment;
- do not stand over a person while they access a real portal or offer to "help quickly" outside the group;
- do not photograph screens or retain names, patient numbers, notifications, QR codes, or metadata; and
- refer account recovery, proxy access, result questions, and record corrections to the provider's official support route.

Prepared demonstrations must be visibly labelled **fictional**. Replace realistic identifiers with obviously invented values and check that image metadata, browser tabs, notifications, and filenames reveal nothing real.



1.6 Misinformation, commercial pressure, and digital well-being

Misinformation is false or misleading content shared without necessarily intending harm. Disinformation is deliberately deceptive. Both can exploit uncertainty, limited access to care, experiences of discrimination, language gaps, or a desire to protect family members. Repetition, popularity, professional-looking design, a medical title, testimonials, and a large follower count do not establish reliability.

Trainers should examine the claim, not attack the person who encountered it. Compare the claim with current independent sources; identify omitted uncertainty, commercial incentives, manipulated images, false authority, or advice to avoid qualified care. Do not amplify a harmful post by displaying live accounts, handles, or links when a fictional reconstruction will teach the same method.

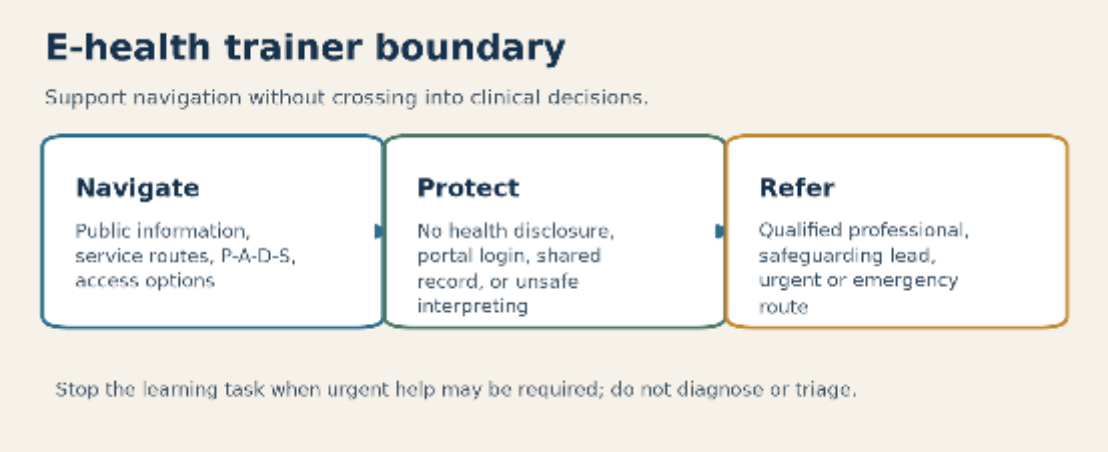
Health searches can also create anxiety, compulsive checking, or exposure to targeted advertising. Model a digital well-being stop plan:

1. pause when searching becomes repetitive, frightening, or unproductive;
2. close duplicate or low-quality results;
3. write one non-diagnostic navigation question;
4. consult one or two validated sources; and
5. use a qualified routine or urgent support route as appropriate.



1.7 Scope, referral, and urgent escalation

Within trainer scope	Outside trainer scope	Required boundary response
Explain interface labels and public service routes	Interpret a test result, image, diagnosis, medicine, dose, risk score, or clinical letter	Stop viewing the information, state the limit, protect privacy, and offer the validated provider contact route
Demonstrate P-A-D-S on fictional or public content	Recommend treatment or tell someone whether to start, stop, or change care	Do not advise; route the question to a qualified healthcare professional
Explain that routine, urgent, emergency, and safeguarding routes differ	Decide how serious symptoms are or conduct triage	Do not question the person to classify urgency; follow the predetermined local escalation procedure
Activate an official route when a person reports immediate danger or the training scenario directs urgent action	Diagnose the cause or delay action while searching online	Stop training, contact the official urgent or emergency route, and follow organizational safeguarding policy



Before delivery, record the official local emergency number, urgent non-emergency route, safeguarding lead, and venue procedure. If immediate danger is reported, prioritize safety and the official route. A trainer may activate a predetermined escalation process; this is not diagnosis or triage. Never rely on a search engine, chatbot, group vote, or influencer account for an emergency decision.





2. Participant context and needs analysis

Needs analysis should reveal barriers to participation without collecting health histories or framing people as deficient. Make every response optional and explain how it will improve access.

Safe methods

- **Anonymous access scan:** ask about preferred language, device type, data or Wi-Fi access, confidence with links and forms, print preference, and accessibility formats. Do not ask why an accessibility format is needed.
- **Environmental scan:** test venue privacy, screen visibility, charging, connectivity, noise, seating, assistive technology, and whether others can overhear an interpreter.
- **Fictional task walk-through:** observe how volunteers navigate a neutral public service example using invented details. Assess the design and instructions, not the person's health knowledge.
- **Community-partner consultation:** ask trusted organizations which system terms, access rules, and service routes are commonly confusing. Do not request client case details.
- **Optional individual access conversation:** offer a private route to request captions, large print, breaks, interpretation, or extra navigation time. Record only the adjustment needed and retain it under organizational policy.
- **Choice-based planning:** provide phone, computer, observation, paired, and printed routes. Do not assume phone ownership, digital independence, literacy, or willingness to discuss women's, mental, or child health.

Use neutral planning language such as "the portal requires several undocumented steps" or "the session needs a low-data option," not "the group lacks ability." Treat multilingualism, community knowledge, and experience navigating multiple systems as assets.

Minimum planning record

Record only operational information:

Planning field	Appropriate record
Languages and communication	Requested session languages, interpretation, captions, plain-language or visual support
Access	Device mix, connectivity, print need, assistive-technology compatibility
Service routes	National, regional, provider, routine, interpreter, safeguarding, urgent and emergency routes
Facilitation	Group size, privacy of room, support staffing, time, opt-out and break arrangements

Planning field	Appropriate record
Prohibited data	No symptoms, diagnoses, pregnancy status, mental-health history, child-health history, portal details, identifiers, or immigration case details



3. Privacy, consent, and safeguarding

3.1 Apply data-protection principles

Where the GDPR applies, health data are specially protected personal data. Whether or not a specific delivery falls under the GDPR, use its core principles as a minimum design discipline alongside applicable national law and organizational policy:

- **lawfulness, fairness, and transparency:** state what is collected, why, by whom, and for how long;
- **purpose limitation:** do not reuse attendance or access information for health profiling;
- **data minimization:** design the session so no health data are needed;
- **accuracy:** correct operational records and do not record inferred health information;
- **storage limitation:** delete temporary access-adjustment and assessment files according to policy;
- **integrity and confidentiality:** restrict access, use approved storage, and prevent screen or audio exposure; and
- **accountability:** document validation, consent arrangements, incidents, and corrective actions.

Consent to attend training is not consent to reveal health information, use an interpreter, appear in a recording, or let a trainer view a portal. Obtain separate, informed, specific, and voluntary agreement where any of those processing activities is genuinely necessary. Avoid them wherever possible.



3.2 Shared phones, browsers, and search history

Private or incognito mode does not guarantee privacy from the device owner, network, employer, platform, or downloaded files. For a shared-device demonstration:

1. use generic fictional queries and public pages;
2. ask the device owner before changing settings, clearing data, or downloading anything;
3. disable or avoid autofill, notifications, location sharing, saved passwords, and account synchronization;
4. do not scan personal QR codes, accept health cookies unnecessarily, or save screenshots;
5. check tabs, downloads, clipboard, recent files, and search suggestions at the end; and
6. offer a trainer device or print route so nobody must use a shared personal phone.

Never promise that deleting history erases all traces. Explain the limitation in plain language.



3.3 Interpreters and consent

An interpreter supports communication; the interpreter does not provide clinical advice or decide for the person. Before the session:

- use a trained interpreter bound by confidentiality where available;
- do not use a child as interpreter and avoid relying on a relative for sensitive content;
- explain the interpreter's role, confidentiality limits, and any remote-platform data route in a language the person can understand;

- confirm that interpretation is voluntary and that the person can request a different arrangement or stop;
- speak to the person directly, use short complete statements, and allow interpretation time; and
- check meaning without asking the interpreter to summarize, filter, persuade, or add a medical opinion.

Nodding, silence, or attendance alone does not demonstrate informed consent. Use a neutral understanding check, for example: “Please tell me what the interpreter will do and what choices you have.” Do not ask for a health example to test understanding.



3.4 Sensitive topics: women, mental health, and child health

Resources may be important but can also disclose identity, family circumstances, pregnancy, violence, reproductive choices, mental distress, or a child’s information. Trainers should:

- introduce topics as optional examples, not assumptions about anyone present;
- use neutral titles on handouts and screens when visibility could expose participation;
- avoid graphic imagery, diagnostic checklists, compulsory discussion, or public reading aloud;
- distinguish adult and child consent, proxy access, confidentiality, and safeguarding rules in the relevant service context;
- identify women-specific, gender-inclusive, mental-health, child-health, violence-support, and interpreter routes from responsible providers; and
- offer private access to a general service directory without asking why it is wanted.



3.5 Respond to distress or disclosure

Do not investigate, counsel, or promise absolute confidentiality. Use this sequence:

1. **Pause and protect privacy:** stop screen sharing or group discussion and move only if doing so is safe and agreed.
2. **Acknowledge:** say, “Thank you for telling me. You do not need to give details here.”
3. **Clarify role, not symptoms:** explain that the trainer cannot assess or advise medically.
4. **Offer choice:** provide the approved routine support, safeguarding lead, or interpreter route without pressure.
5. **Escalate immediate danger:** activate the official urgent or emergency process and organizational safeguarding procedure.
6. **Record minimally:** document only what policy requires, factually, in approved storage, and never in trainer reflection notes.
7. **Follow up operationally:** check that the referral process was offered or activated, not the person’s diagnosis or treatment.

If a confidentiality or data incident occurs, stop the exposure, preserve safety, inform the designated data-protection or safeguarding contact, follow the incident procedure, and do not circulate the information while seeking help.



4. Guided source-evaluation practice

This self-study practice builds professional judgement about sources.

Lab brief

Review three candidate resources for one neutral navigation purpose, such as finding a public primary-care directory or interpreter-information page:

- one competent public-health or government source;
- one provider, professional body, patient organization, university, or specialist NGO source; and
- one commercial, sponsored, search-result, social, or influencer source.

Do not use personal symptoms, accounts, location history, or real appointments. Work from public pages in a clean training browser.

Validation procedure

1. Define the exact facilitation purpose and relevant service scope.
2. Record the direct URL, page title, owner, and date checked; do not rely on search ranking.
3. Apply all P-A-D-S questions and the jurisdiction, accessibility, privacy, and equity cross-checks.
4. Verify important claims or service routes against a second independent competent source.
5. Test on a phone-sized screen and, where possible, with keyboard navigation, text enlargement, and a screen reader.
6. Check language options, reading load, headings, link labels, captions, contact alternatives, costs, eligibility, and low-bandwidth performance.
7. Identify data requests, cookies, trackers, account requirements, advertising, sponsorship, and potential phishing confusion.
8. Assign one decision: `approved`, `approved with stated limitations`, or `not approved`.
9. Note a change trigger such as a system redesign, policy change, broken link, or reported safety issue.

Validation record

Field	Evidence to record
Purpose and audience	The single task the resource supports; service scope and language
Publisher	Responsible body, expertise, governance, and independently verified identity
Aim and funding	Informational, service, commercial, advocacy, data-collection, advertising, or mixed purpose
Date and evidence	Publication/review date, cited evidence, uncertainty, comparison source

Field	Evidence to record
Support routes	Routine contact, interpreter/accessibility help, urgent or emergency signposting where relevant
Access and inclusion	Phone use, keyboard, zoom, screen reader, captions, readability, languages, print alternative
Privacy and security	Public/login status, data fields, cookies, downloads, permissions, phishing or impersonation risk
Decision	Suitable status, limitations to state, check date, and change trigger

Lab analysis

Consider why the strongest source is appropriate for the defined task, identify one reason it could still fail the intended audience, and specify an accessible fallback. A prestigious source may still be unsuitable if it is outdated, inaccessible, outside the relevant jurisdiction, or unnecessarily collects data.



5. Accessible and culturally responsive facilitation

5.1 Facilitation principles

- Use health-literacy universal precautions: assume any system can be unfamiliar and make navigation explicit for everyone.
- Start from participants' existing strategies and multilingual knowledge; avoid testing who is "good" or "bad" at digital health.
- Explain purpose, privacy, choice, and trainer scope before showing content.
- Demonstrate one route at a time, pause at decision points, and describe why a click or source choice is safe.

- Allow observation, paired practice, independent practice, or no-device participation in facilitated delivery.
- Use fictional names and neutral service-navigation tasks. Never invite stories to make the session feel relevant.
- Correct the material or facilitation barrier before attributing difficulty to a person.
- Build in breaks and a clear way to pause or leave a sensitive example without explanation.



5.2 Readable and accessible design

Apply WCAG 2.2 principles and its readable guidance as appropriate to the prepared materials:

- use descriptive headings, meaningful link text, consistent navigation, and visible focus order;
- identify page and passage language and explain unusual words, abbreviations, icons, and medical-system terms;
- use short sentences, active voice, one instruction per step, and a glossary without infantilizing adults;
- support text enlargement and reflow; do not place essential words inside images;
- provide sufficient contrast, captions, transcripts, alt text, and keyboard-operable controls;
- do not use color, sound, position, or icons as the only way to convey meaning; and
- test the actual phone, print, screen-reader, and low-bandwidth versions rather than assuming equivalence.

Readable presentation does not make clinical content suitable for trainer interpretation. Accessibility and scope must both be satisfied.



5.3 Multilingual, phone, and print adaptations

Need	Adaptation	Quality control
Multilingual access	Dual-language glossary, verified language switch, trained interpreter, translated step cards	Verify system terms with competent reviewers; date and version translations; avoid machine translation for safety-critical wording without review
Phone-first access	Numbered taps, portrait screenshots, large targets, short URLs, low-data pages	Remove notifications and personal data; test current operating systems; provide charging and trainer devices
Print or offline access	High-contrast step cards, source-check sheet, service name and official contact route	Add jurisdiction and last-checked date; explain that print can become outdated; never print portal records
Low literacy	Plain language, visual sequence, demonstration, optional audio, extra processing time	Preserve adult tone; avoid compulsory reading aloud or speed-based tasks
Sensory, motor, or cognitive access	Keyboard route, screen-reader-compatible text, captions, reflow, breaks, uncluttered steps	Test with relevant assistive technology and offer an equivalent non-digital route

LASLLIAM can guide language-and-literacy scaffolding for adult migrants. Use it to support participation, not to infer language level from nationality, accent, education, or migration status.



5.4 Non-shaming misinformation correction

Use the sequence **connect, examine, compare, choose**:

1. **Connect:** “It makes sense to check a claim that promises a clear answer.”
2. **Examine:** ask permission to look at the claim’s publisher, aim, date, and support.
3. **Compare:** use one current independent source and name relevant uncertainty or commercial influence.
4. **Choose:** agree on a safe information or professional-support route; do not demand a public retraction.

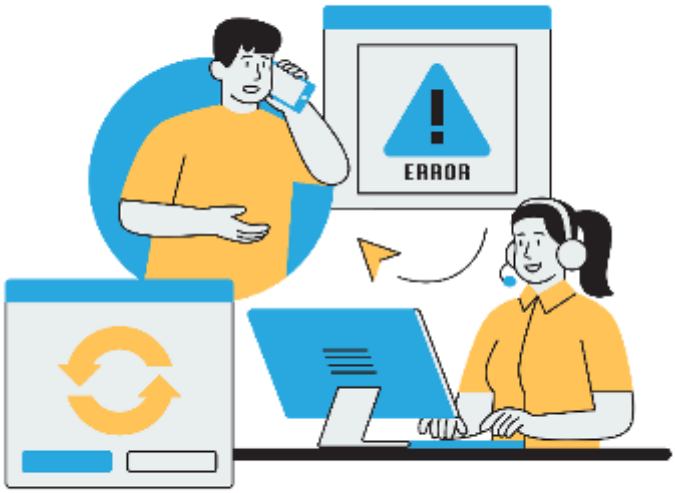
Avoid ridicule, fact-dumping, political labelling, or asking who shared the claim. Correct privately when public correction could expose a person’s health concern. If the content advises immediate harmful action or avoidance of urgent care, state the safety boundary clearly and activate the appropriate official route.



6. Troubleshooting and safe responses

Situation	Trainer response	Avoid
Official link is broken or redirects unexpectedly	Stop, use the independently verified organization homepage or phone route, and flag the resource for review	Guessing a new URL or using a sponsored result
Search result resembles an official appointment message	Open no embedded link; find the provider's contact independently and verify the message through that channel	Replying, entering credentials, or calling a number in the message
Two competent sources disagree	Compare jurisdiction, audience, date, evidence, and purpose; state uncertainty and refer personal decisions to a professional	Choosing by visual polish or search position
Page requests login or health details	Stop and return to a public or fictional demonstration	Creating an account or using a participant's details
Translation changes a system or safety term	Pause use of the material and obtain qualified review	Asking an unbriefed attendee to improvise sensitive translation
Internet or device fails	Use dated print cards or a prepared offline fictional demonstration	Asking participants to use personal data or accounts as a workaround
Search content causes distress	Pause, close the content, offer a break and validated support route, and follow the disclosure process if needed	Probing for a personal story or continuing for the schedule

Situation	Trainer response	Avoid
A request crosses into test interpretation or treatment	State the boundary and offer the qualified provider route	Giving a "general" interpretation that could be taken as personal advice
Immediate danger is reported	Stop training and activate the official urgent or emergency and safeguarding procedure	Online searching, diagnosis, triage questioning, or group discussion



7. Model workshop for trainer analysis

This 75-minute example uses public or fictional material and requires no health disclosure.

Exemplar metadata

Field	Exemplar detail
Intended participants	A hypothetical group of TCN women attending an optional facilitated workshop
Sample duration	75 minutes
Sample purpose	Introduce one public service route, P-A-D-S, privacy boundaries, and where to obtain qualified help
Required preparation	Two current public resources, fictional screenshots, approved routine and emergency routes, interpreter and accessibility plan

Sample flow to critique

Time	Facilitation move	Sample participant action	Embedded safeguard
0-10 min	Explain purpose, confidentiality, choice, trainer scope, breaks, and official urgent route	Choose phone, print, observation, or paired mode without giving a reason	No disclosure; no real account
10-20 min	Show how national, regional, and provider routes differ	Match three fictional service needs to the correct system layer	Neutral scenarios only
20-35 min	Model P-A-D-S on a validated public page and a reconstructed commercial claim	Identify publisher, aim, date, support, and one uncertainty	No live harmful post; no diagnosis
35-50 min	Demonstrate a public service directory on phone and print	Follow a fictional route to find a public contact and accessibility option	No login, booking, form, or location history
50-65 min	Facilitate a shared-phone privacy and misinformation scenario	Suggest a privacy control and a non-shaming correction phrase	Fictional device and data
65-75 min	Summarize safe stopping points and routine versus urgent routes	Name where a fictional person could obtain qualified help	No symptom classification or treatment advice



Trainer analysis prompts

- Where does the exemplar clearly separate digital navigation from diagnosis, treatment, and triage?
- Which step could accidentally invite disclosure, and how would you rewrite the instruction?

- Does the selected resource work for the relevant service scope, phone access, language mix, and accessibility requirements?
- How will the trainer explain shared-device limits without creating fear or claiming that history can be fully erased?
- Which examples may be sensitive in relation to women's, mental, or child health, and what neutral alternative preserves the skill?
- What evidence would show that facilitation was respectful and usable without collecting health information?
- Which routine, interpreter, safeguarding, urgent, and emergency routes must be identified before this exemplar can be delivered?



8. Trainer quiz

1. During practice, a person opens a phone notification showing a flagged laboratory result and asks the trainer what it means. What is the best trainer response?
    - A. Give a general explanation but avoid naming a diagnosis.
    - B. Stop viewing it, state that the trainer cannot interpret results, protect privacy, and offer the provider's official contact route.
    - C. Ask the group whether anyone has received a similar result.
    - D. Search the test name on a reputable public-health website and summarize it.
2. Which approach is safest for demonstrating patient-portal navigation?
    - A. Ask a volunteer to log in while hiding the person's name.
    - B. Create a real account using a trainer-controlled email address.
    - C. Use a participant's portal only for the menu screen and log out immediately.
    - D. Use a clearly labelled fictional prototype, approved sandbox, or static screenshots with invented data.
3. A trainer needs a source for demonstrating how to find current vaccination service eligibility in the workshop's region. Which is the best initial choice?
    - A. A current regional public-health page that states jurisdiction, update date, eligibility basis, and official contact route.
    - B. A regulated clinic's four-year-old article with a booking link but no regional eligibility details.
    - C. A patient forum thread with recent personal accounts from the same city.
    - D. A sponsored influencer post citing one study and linking to a private booking platform.
4. A trained interpreter is available. A participant nods when interpretation is offered but appears uncertain about what will be shared. What should the trainer do?
    - A. Continue because nodding is sufficient consent in a group setting.
    - B. Ask the interpreter to decide whether the participant understands.
    - C. Explain role, confidentiality limits, data route, and choices in understandable language, then verify voluntary consent.
    - D. Replace the interpreter with a relative who already knows the participant.
5. A model workshop will use phones that may be shared with family members. Which plan best protects privacy?
    - A. Require private browsing and promise that it leaves no trace.
    - B. Use generic fictional searches and public pages, avoid logins/downloads, explain history limits, and offer trainer-device or print alternatives.
    - C. Ask participants to clear all browser and app data before attending.

- D. Use realistic symptom searches so participants can practise deleting them afterward.

6. A participant repeats an online claim that one supplement is a guaranteed cure. What is the best facilitation response?
   - A. State that health content on social media is always false.
   - B. Ask who shared it so the group can judge that person's credibility.
   - C. Display the original account and invite the group to refute it publicly.
   - D. Acknowledge the concern, ask permission to examine the claim with P-A-D-S, and compare it with an independent current source.
7. A text message says an appointment will be cancelled unless the recipient signs in through a shortened link within ten minutes. What should the trainer model?
   - A. Do not use the link; independently find the provider's official contact and verify the message through that route.
   - B. Open the link in private browsing so credentials are protected.
   - C. Reply to the message and ask it to confirm the person's date of birth.
   - D. Forward it to another phone to see whether the warning still appears.
8. During a session, a person says they have severe chest pain and difficulty breathing now. What is the best trainer action?
   - A. Ask structured questions to determine whether an ambulance is necessary.
   - B. Find an official symptom page and read the warning signs together.
   - C. Stop the training task and activate the organization's official emergency procedure without diagnosing or delaying for an online search.
   - D. Give the routine clinic number and continue while the person calls later.
9. A trainer is adapting a public-service navigation demonstration for screen-reader users and adults who prefer simpler text. Which change is best?
   - A. Put every instruction into one labelled screenshot so the sequence stays together.
   - B. Use semantic headings, descriptive links, plain-language steps, text alternatives, keyboard access, and tested reflow.
   - C. Replace text labels with color-coded medical icons.
   - D. Read the unchanged complex page aloud while participants follow on their phones.
10. A proposed session asks participants to list symptoms, compare diagnoses, interpret test results, and choose treatment websites. What is the best trainer critique?
    - A. Replace those tasks with fictional public navigation, source evaluation, privacy practice, and clear professional and emergency routes.
    - B. Keep the tasks but add a disclaimer that the trainer is not responsible for decisions.
    - C. Keep symptom comparison but remove only the treatment-website task.

- D. Invite a more digitally confident participant to lead the test-result discussion.

References

1. Redecker, C. (2017). *European Framework for the Digital Competence of Educators: DigCompEdu*. Publications Office of the European Union. https://publications.jrc.ec.europa.eu/repository/handle/JRC107466
2. Vuorikari, R., Kluzer, S., and Punie, Y. (2022). *DigComp 2.2: The Digital Competence Framework for Citizens, with new examples of knowledge, skills and attitudes*. Publications Office of the European Union. https://publications.jrc.ec.europa.eu/repository/handle/JRC128415
3. European Parliament and Council of the European Union. (2016). *Regulation (EU) 2016/679 (General Data Protection Regulation)*, especially Articles 5, 9, and 32. https://eur-lex.europa.eu/eli/reg/2016/679/oj
4. World Health Organization. (n.d.). *Improving health literacy*. https://www.who.int/activities/improving-health-literacy
5. World Wide Web Consortium. (2023). *Web Content Accessibility Guidelines (WCAG) 2.2*, including Guideline 3.1, Readable. https://www.w3.org/TR/WCAG22/#readable
6. Council of Europe. (2022). *Literacy and Second Language Learning for the Linguistic Integration of Adult Migrants (LASLLIAM)*. https://www.coe.int/en/web/language-policy/laslliam

LINK UP: Digital Empowerment and Community Engagement for Third-Country National Women

2025-1-DE02-KA220-ADU-000350564

WP2: Public Service Awareness Modules

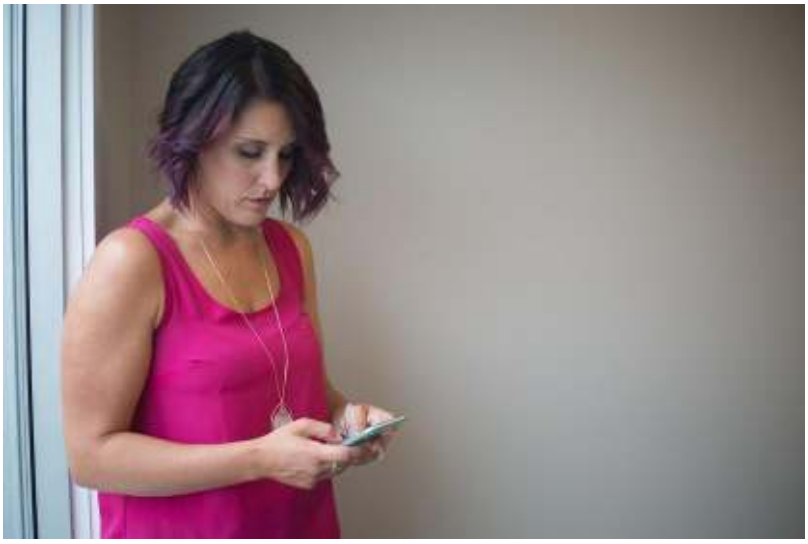
Module 3: Digital financial skills

Module 3: Digital financial skills

Module overview

Field	Details
Audience	Trainers, educators, social workers, and facilitators working with TCN women
Duration	3-5 hours
Delivery method	Face-to-face / Online / Blended
Scope	Digital financial services, transaction safety, fraud prevention, privacy, inclusive facilitation, and referral boundaries
Lead partner(s)	Balkan Bridge (Bulgaria)

This is digital-skills education, not financial advice. Trainers do not recommend a bank, payment provider, loan, investment, remittance route, or other financial product. Applicable law, provider terms, fees, access rules, and redress arrangements must be checked before use.



Trainer competencies

On successful completion, the trainer can:

1. Map at least five roles in a financial-service ecosystem and distinguish regulated, agent, commercial, and unregulated roles using an official register.
2. Analyse a fictional payment or remittance for transaction state, payer outlay, recipient amount, fees, exchange effects, timing, and recourse without endorsing a provider.
3. Apply and explain the four-part STOP check to simulated payment and social-engineering scenarios.

4. Plan a non-sensitive needs analysis and an inclusive phone, visual, multilingual, and print facilitation sequence without collecting personal financial data.
5. Facilitate a non-blaming fraud response, including proportionate evidence handling, post-incident actions, safeguarding, and referral boundaries.
6. Evaluate current sources for authority, currency, accessibility, jurisdiction, and appropriate use.

1. Professional foundation

1.1 Financial-service ecosystem

Digital money services are an ecosystem, not a single app. A trainer should be able to locate these roles in a fictional case:

- **Customer and payee:** the person or organisation initiating or receiving value.
- **Bank or credit institution:** may hold deposits and provide cards, transfers, or account access, subject to its authorisation.
- **Payment or electronic-money institution:** may provide transfers, cards, or stored electronic value without being a deposit-taking bank.
- **Card scheme, processor, or technical platform:** may route information or transactions but may not be the customer's contractual provider.
- **Digital wallet:** stores payment credentials or electronic value, depending on its design. The label `wallet` does not establish its legal status or protections.
- **Money-transfer or remittance provider:** arranges domestic or cross-border transfers, sometimes through agents and cash-out partners.
- **Merchant, marketplace, telecom provider, or cash agent:** may initiate, accept, distribute, or support a service without being responsible for every complaint.
- **Regulator, ombudsman, alternative-dispute-resolution body, consumer authority, police, and cybercrime service:** have different oversight, complaint, redress, or reporting functions.
- **Community organisation or trainer:** can provide education and signposting, but is not a provider, investigator, lawyer, debt adviser, or fraud-recovery service.

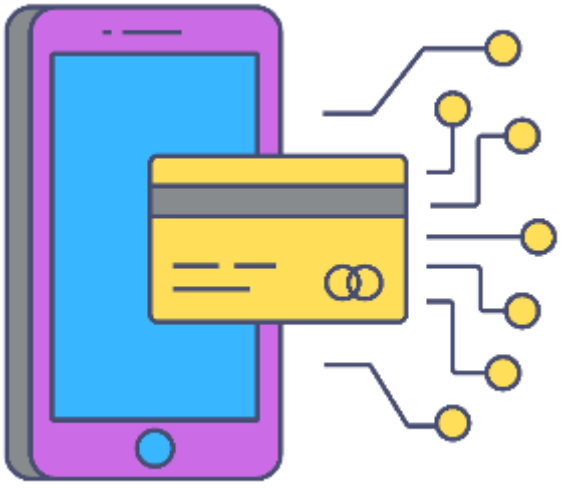


1.2 Regulated, agent, and unregulated roles

Regulation is specific to a legal entity, activity, and jurisdiction. It is not established by a professional website, app-store listing, familiar logo, social-media account, or claim that a service is `licensed`.

Category	Trainer interpretation	Verification action
Authorised or registered provider	Appears on the relevant official register for the service and jurisdiction	Match legal name, register number, permitted activity, domain, and any restrictions
Agent or intermediary	Acts for another entity and may have a narrower role	Verify both the agent relationship and the principal provider on an official source
Unregulated or out-of-scope service	May be lawful for some activities but lacks the assumed financial protection	State the limitation neutrally and do not imply equivalent recourse
Unknown or impersonated entity	Identity or authority cannot be verified independently	Stop; do not use contact details supplied by the claim itself

Regulated does not mean risk-free, cheapest, suitable, or guaranteed. Unregulated does not automatically mean illegal. Trainers explain how to verify status and compare features; they do not make suitability decisions for others.



1.3 Education, not financial advice

Within scope, a trainer may:

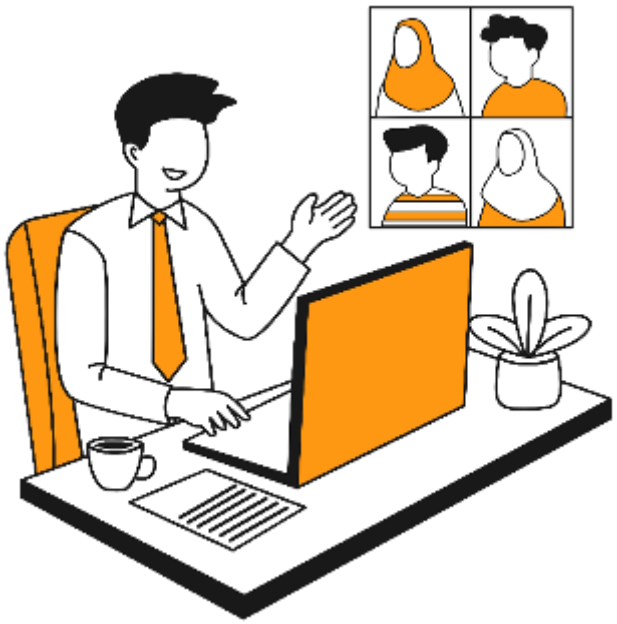
- explain general concepts and decision steps;
- compare fictional or validated public information against neutral criteria;
- demonstrate a fictional interface or sandbox;

- identify warning signs and official verification routes; and
- signpost to qualified, independent support.

Outside scope, a trainer must not:

- select or rank a product for an individual;
- advise whether to borrow, invest, transfer, buy, sell, or disclose case-specific finances;
- interpret individual legal rights, tax, benefits, debt, immigration status, or entitlement;
- promise recovery, reimbursement, confidentiality beyond policy, or a particular provider outcome; or
- handle money, credentials, complaints, or negotiations on a participant's behalf.

Use a boundary statement such as: `I can explain a general checking process and show verified support routes. I cannot recommend a product or advise on your individual financial decision.`



2. Transactions, costs, and product neutrality

2.1 Core concepts trainers must distinguish

- **Balance:** an amount displayed for an account or wallet. `Current`, `ledger`, and `available` balances may differ because of holds, pending items, overdrafts, or provider rules.
- **Payment:** a broad transfer of value for goods, services, bills, or another purpose. Card payments, payment links, direct debits, and transfers follow different processes.
- **Transfer:** an instruction to move funds between accounts or users. A bank transfer may be difficult to reverse after execution.
- **Digital wallet:** a tool that may hold credentials, tokenised cards, or stored value. Security, fees, funding, cash-out, and recourse differ by wallet.
- **Remittance:** a domestic or cross-border money-transfer service. The sender's fee alone does not show what the recipient receives.
- **Payee and identifier:** the intended recipient and the account number, IBAN, wallet handle, phone number, or other routing detail. A familiar display name is not sufficient verification.
- **Authentication and authorisation:** proving access is not the same as knowingly approving a transaction. A PIN, password, biometric, or one-time passcode has a stated purpose that must be read before use.



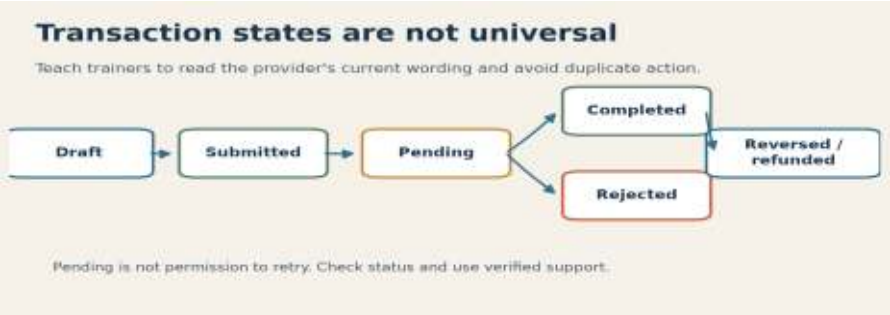
2.2 Transaction states

Interface wording varies. A trainer should avoid treating any label as universal.

- **Draft or initiated:** details exist, but the instruction may not have been authorised or sent.
- **Authorised or submitted:** approval was given; cancellation may already be limited.

- **Pending or processing:** no final outcome is shown. Do not teach a duplicate retry; verify status and use official support.
- **Completed or settled:** the provider records completion, which may not mean cash is immediately available to the recipient.
- **Rejected or failed:** the instruction was not completed; confirm whether any hold or fee remains before retrying.
- **Cancelled:** an instruction was stopped under the provider's rules.
- **Reversed:** a previously recorded amount was returned or undone by a provider process.
- **Refunded:** a merchant or provider initiated a return; timing and destination can vary.

Terms such as `chargeback`, `recall`, and `refund` are not interchangeable. Eligibility and deadlines depend on transaction type, facts, contract, and local law.



Transaction-state flow from draft and submitted to pending, completed, rejected, reversed, or refunded.



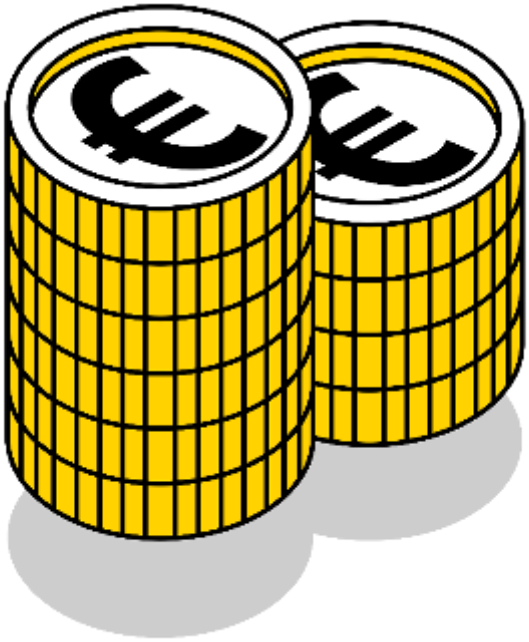
2.3 Total cost and exchange

A neutral comparison separates:

- payer outlay: amount paid plus upfront and funding fees;
- recipient amount: the amount expected after conversion and deductions;
- stated exchange rate and any exchange-rate margin;
- intermediary, correspondent, card, cash-out, delivery, or recipient fees;

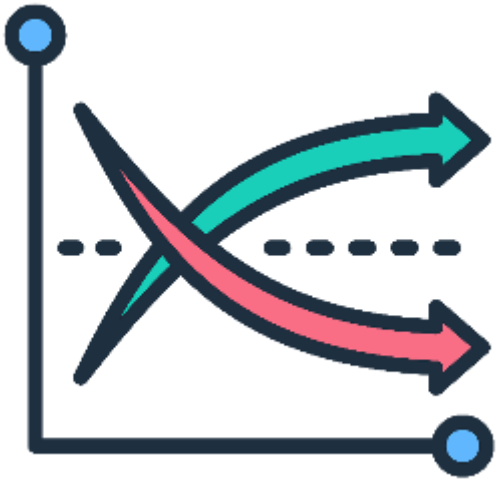
- data, travel, documentation, and time costs;
- delivery estimate and what happens if a transaction is delayed or fails; and
- cancellation, complaint, error, and fraud routes.

Do not compare services using only a headline fee or promotional rate. Record the date, currency pair, amount, delivery method, and source because quotes change. If a fee or exchange term cannot be verified, label it `not verified`; do not estimate it.



2.4 Product-neutral comparison

Use the same criteria for every option: verified legal entity and status, service type, total cost, recipient amount, timing, access requirements, data/device implications, transaction states, accessibility, support, complaints, and redress. Separate facts from trainer commentary. A commercial screenshot must be labelled as an interface example, not an endorsement.



2.5 Budgeting and numeracy scaffolding

Budgeting examples are useful only as fictional facilitation artefacts. They must not invite disclosure of income, benefits, debt, dependence, or spending.

For low numeracy, trainers should:

- use round fictional amounts before decimals, percentages, or exchange rates;
- show one operation per line and name the operation in words;
- use visual groups, number lines, or labelled columns without relying on colour alone;
- distinguish `amount sent`, `fee`, `total paid`, and `amount received`;
- model calculator use and estimation as valid strategies, not remediation;
- allow extra processing time and offer an equivalent print version; and
- check understanding through explanation of a fictional decision, not speed or mental arithmetic.



Avoid deficit language. Difficulty may arise from unfamiliar notation, language, interface design, stress, vision, interrupted education, or a mismatch between the example and local practice.

3. STOP, social engineering, and fraud response

3.1 The STOP decision check

STOP is a pause routine for simulations and facilitated sessions:

1. **Source:** Was the service opened independently through an official app, saved address, card number, or verified website rather than an unexpected link, QR code, search advertisement, or caller instruction?
2. **To whom:** Do the payee name and identifier match independently verified information? Has a known contact requested an unusual change?
3. **Overview:** Are amount, currency, fee, exchange, reference, timing, purpose, and transaction state clear before authorisation?
4. **Pause:** Is there urgency, secrecy, fear, pressure, remote access, or a request for a password, PIN, card detail, biometric action, or one-time code?

STOP is not a guarantee that a transaction is safe. It creates time to leave the contact channel, verify independently, and seek qualified support.



STOP payment check: verify the source, intended recipient, transaction overview, and pressure or credential requests before acting.

3.2 Social engineering

Social engineering manipulates trust, authority, fear, affection, scarcity, or helpfulness. Channels include phishing email, smishing text, vishing calls, fake websites or apps, malicious QR codes, social media, compromised contacts, in-person approaches, and remote-access tools.

Examples relevant to migrants and people experiencing situational vulnerability include impersonated:

- banks, police, tax, immigration, visa, benefits, healthcare, or delivery services;
- employers, recruiters, landlords, utility companies, schools, charities, interpreters, or community leaders;
- family emergencies, romance contacts, or remittance recipients;
- loan, prize, refund, grant, document, or fee requests;
- investment or crypto offers promising guaranteed returns or no risk;
- `safe account`, money-mule job, account-rental, or cash-forwarding requests; and

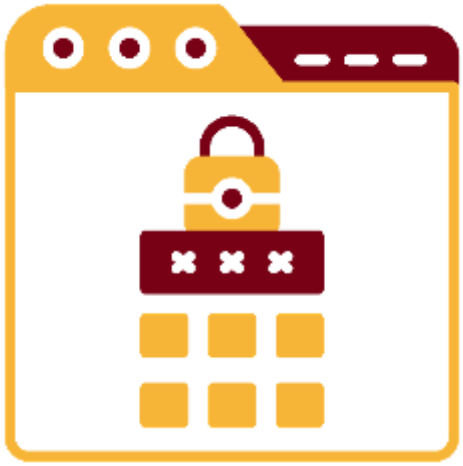
- fraud-recovery agents who demand advance payment or credentials.



Fraudsters may exploit language barriers, unfamiliar systems, insecure housing or devices, urgency around documents, isolation, financial stress, or dependence on another person. These are conditions exploited by offenders, not faults in the targeted person. Avoid stereotypes and do not describe a group as inherently vulnerable or careless.

3.3 Credentials and remote access

A caller or message must never be given a password, full PIN, or one-time code. A genuine one-time code can still authorise a criminal's action if it is disclosed or entered under instruction. Trainers should model reading the code's stated purpose, refusing remote screen control, ending the contact, and opening a verified channel independently.



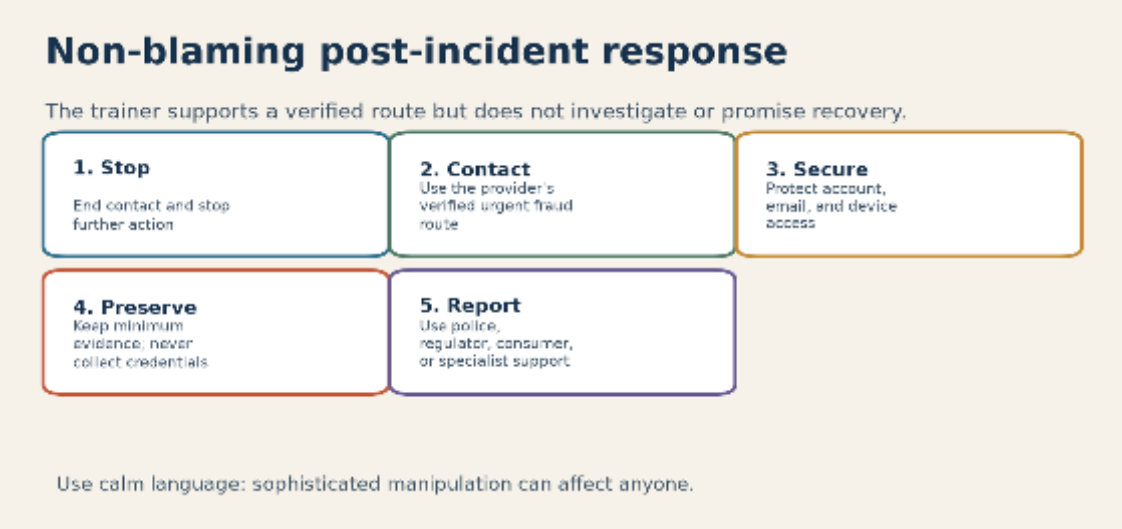
3.4 Non-blaming post-incident response

When money, credentials, or device access may have been compromised, teach a calm sequence without investigating the case:

1. End contact and stop further payments, links, code sharing, and remote access. Address immediate physical safety first.

2. Contact the relevant provider promptly through its verified urgent fraud route. The provider may advise securing access, blocking an instrument, disputing, or requesting a transfer recall; the trainer does not predict eligibility or success.
3. Secure affected email, account, and device access from a trusted device, following verified provider or qualified cyber-support guidance.
4. Preserve only proportionate evidence such as sender details, dates, transaction references, and original messages. Do not forward harmful links or collect passwords, PINs, one-time codes, full card details, or unrelated conversations.
5. Use appropriate official police, cybercrime, regulator, consumer, or specialist support routes for the jurisdiction.
6. Offer a choice of private support and acknowledge that sophisticated manipulation can affect anyone. Do not ask, `Why did you do that?`

Useful wording is: `Thank you for telling me. This is not your fault. We can pause. I cannot investigate or promise recovery, but I can help you locate a verified urgent support route.`



Five-part non-blaming response: stop, contact the provider, secure access, preserve minimum evidence, and report through verified routes.

3.5 Consumer recourse

Recourse is a route, not a guaranteed outcome. An appropriate pathway may include:

- the provider's urgent fraud or security channel;
- the provider's formal complaint process and deadline;
- an independent ombudsman or alternative-dispute-resolution body;
- a financial regulator or consumer-protection authority;
- police or national cybercrime reporting; and
- specialist legal, debt, migrant, domestic-abuse, or financial-abuse support.

Trainers explain the sequence and preserve participant choice. They do not decide liability, submit a complaint as the participant, or promise that money will be returned.



3.6 Financial abuse and coercion

Warning patterns can include forced transfers or loans, confiscated cards or documents, surveillance of spending or messages, withheld money, debt created in another person's name, forced account access, threats linked to immigration or housing, or control of a shared device.

If abuse or coercion is disclosed:

- speak only when privacy and safety permit;
- listen without demanding proof or details;
- explain relevant confidentiality limits and safeguarding duties;
- ask which contact method is safe rather than sending material automatically;
- follow organisational safeguarding procedures and validated specialist referrals; and
- use emergency services only for immediate danger under local protocol.

Do not confront the suspected abuser, mediate, inspect an account, create a secret account plan, or leave digital or printed material that could increase risk. Obtain specialist guidance and centre the affected person's informed choice within legal safeguarding duties.



4. Needs analysis, privacy, and safeguarding

4.1 Non-sensitive needs analysis

Collect only information needed to plan access. Use anonymous or group-level options where possible. Appropriate planning topics include:

- preferred teaching languages and need for a qualified interpreter;
- comfort with common icons and payment vocabulary in general;
- preferred phone, large-screen, audio, visual, or print format;
- accessibility, pacing, childcare, timing, and low-bandwidth needs; and
- whether observation, paired fictional practice, or individual fictional practice is preferred.

Do not ask whether someone has an account, card, debt, benefit, remittance habit, fraud history, legal status, income, balance, or financial dependency. Do not infer financial capability from migration status, language, literacy, age, disability, or device ownership. Record accommodations, not diagnoses or financial narratives.



4.2 Strict no-real-transaction protocol

During training and facilitated sessions, do not:

- open, create, or access a real bank, wallet, card, payment, credit, remittance, investment, or crypto account;
- request or view a real balance, statement, transaction, payee, account number, IBAN, card, identity document, PIN, password, biometric, or one-time code;
- make or rehearse a real transfer, payment, withdrawal, purchase, refund, deposit, or `small test` transaction;
- ask anyone to install a financial app, click a live payment link, scan a live QR code, or share a real financial screen;
- photograph, record, upload, email, or retain financial screens or documents; or
- set any task that uses real financial information outside the session.

Use fictional profiles, redacted trainer-created screens, print cards, offline prototypes, trusted sandboxes, or videos with no live account. An ATM or branch visit can only be observational: no card insertion, PIN entry, balance view, cash action, or personal enquiry forms part of training.

If real information appears unexpectedly, stop the display, ask the person to close or lock it, avert the group view, and do not touch the device or repeat the information. Follow the organisation's privacy or incident process if exposure occurred.



4.3 Privacy by design

Apply GDPR Article 5 principles where applicable and use them as good practice elsewhere:

- lawfulness, fairness, and transparency;
- purpose limitation;
- data minimisation;
- accuracy;
- storage limitation;
- integrity and confidentiality; and
- accountability.

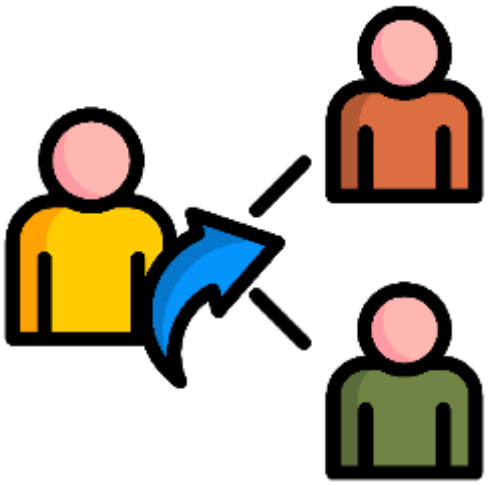
Attendance and accommodation records must be separated from activity artefacts. Use fictional names and identifiers, collect the minimum, restrict access, define deletion dates, and never place case disclosures in shared feedback. Consent does not make unnecessary collection appropriate.



4.4 Safeguarding and referral boundaries

Before delivery, identify a named safeguarding lead, private escalation route, interpreter protocol, emergency procedure, and specialist financial-abuse referral. Explain that a trainer may need to share a minimum amount when law or safeguarding policy requires it; do not promise absolute confidentiality.

A trainer provides a warm referral by locating and explaining a verified route, with consent where possible. A trainer does not diagnose, investigate, transport evidence, speak as the person, or remain the sole support for an urgent case.



5. Guided source-evaluation practice

Purpose

This self-study practice helps prevent outdated, commercial, or unsafe information from entering a facilitated session. Use no personal data and make no contact about a real case.

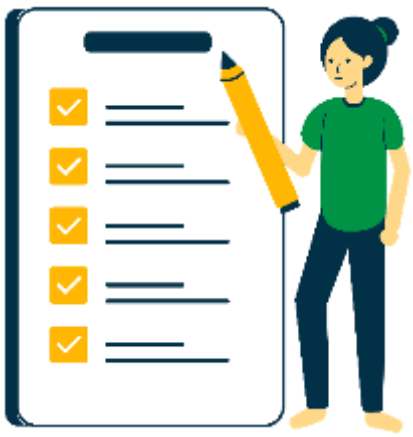
Trainer task

Select one official regulatory or consumer resource, one official fraud-reporting or urgent-support route, and one public fee or product-information source relevant to a fictional scenario. For each resource:

1. Open it independently, not through a scenario's message or link.
2. Identify the owner, legal entity, jurisdiction, purpose, and intended audience.
3. Confirm authority through an official regulator or government domain where relevant.
4. Check publication or update date, live contact details, scope, deadlines, and known limitations.
5. Test phone readability, keyboard access, meaningful headings and links, text alternatives, captions or transcripts, language options, and a printable route.
6. Separate official facts from commercial claims, sponsored search results, or trainer interpretation.
7. Decide `suitable`, `suitable with a stated limitation`, or `reject`, and note the reason and checked date.

Reject or quarantine a resource if ownership is unclear, fee data is undated, links redirect unexpectedly, access is unsafe, claims cannot be corroborated, or the resource requests unnecessary personal information.

Only resources marked `suitable` may enter the model workshop or another facilitated session. Set uncertain resources aside until all required checks are complete.



6. Inclusive facilitation design

Mobile and low-bandwidth

- Design phone-first in portrait view, with short screens, clear back and stop routes, large controls, and no horizontal scrolling.
- Never assume personal smartphone ownership. Offer an equivalent large-screen, printed, or trainer-demonstrated route.
- Provide downloadable low-bandwidth files and static fictional screens; do not make live video or app installation essential.
- For shared devices or public Wi-Fi, use only fictional or offline materials. Do not open real services or save identifiers, autofill, images, or downloads.

Visual and readable

- Use descriptive headings, plain language, short steps, readable type, strong contrast, and generous spacing.
- Pair icons and colour with text labels; never encode risk or state by colour alone.
- Provide alt text for meaningful images, captions and transcripts for media, keyboard operation, visible focus, and logical reading order.
- Use the applicable WCAG 2.2 success criteria and test the actual LMS and downloadable file, not only the source document.

Multilingual and literacy-aware

- Pre-teach a small, reviewed glossary without assuming that a direct translation has the same banking meaning.
- Use qualified language support for sensitive content; do not depend on children, relatives, or unbriefed peers to interpret a disclosure.
- Read instructions aloud when useful, display the same words, and model one fictional decision at a time.
- Apply LASLLIAM-informed scaffolding: distinguish language, literacy, digital familiarity, and conceptual knowledge rather than treating them as one ability.
- Permit silence, observation, repetition, and extra processing time without public correction.

Product-neutral and trauma-aware

- Use more than one fictional interface pattern so familiarity with a brand is not mistaken for competence.
- Do not require disclosure or participation in a fraud or abuse scenario.
- Give advance notice of coercion or loss themes and provide an equivalent neutral scenario.
- Correct unsafe decisions calmly and specifically. Attribute fraud to offender tactics, not gullibility.



7. Facilitation troubleshooting

Situation	Trainer response
A demo or connection fails	Move to the validated print or offline version; do not open a personal account as a substitute
A fictional transaction remains pending	Model checking status and verified support; do not repeat the transaction
A participant opens a real financial app	Stop, avert the display, ask them to close it, collect nothing, and restate the boundary without blame
A fee sheet is outdated or undated	Quarantine it, mark the claim unverified, and complete resource validation before reuse
A participant asks which provider is best	Return to neutral criteria and refer individual suitability questions to qualified independent support
A real fraud disclosure occurs in a group	Stop public detail, offer a private choice, use the verified urgent route, and follow safeguarding and privacy procedure
A password, code, or card detail is exposed	Stop viewing and recording; do not copy it; follow the privacy-incident route and verified provider guidance
Numeracy demands block the task	Reduce information, use round fictional values and visual steps, allow a calculator, and assess the decision rather than speed
Distress or coercion is indicated	Do not probe or mediate; check immediate safety, explain limits, and use the safeguarding pathway
A resource conflicts with applicable rules	Pause its use and obtain current guidance from the competent authority; do not improvise legal interpretation



8. Model workshop for trainer analysis

This 90-minute example applies the module's facilitation principles. All profiles, amounts, screens, messages, and provider names are fictional.

Time	Facilitation move	Exemplar participant action for trainer analysis
0-10 min	State no-real-transaction, privacy, choice, and no-advice boundaries; show fictional materials	Select an observation, print, or paired fictional format without disclosing financial experience
10-25 min	Map a fictional bank, wallet, remittance agent, regulator, and complaint route	Place role cards and identify which authority claim still requires verification
25-45 min	Think aloud through STOP on a phone-sized fictional transfer screen	Identify source, payee, total cost, status, and pressure cue; stop before simulated authorisation
45-60 min	Compare two fictional remittance quotes with round amounts and a visual cost strip	Distinguish payer outlay from recipient amount without selecting a product
60-80 min	Facilitate an OTP impersonation and post-incident response scenario	Choose non-blaming stop, verified contact, minimal evidence, and referral actions
80-90 min	Revisit boundaries and display verified support routes	Explain where a fictional case leaves trainer scope and enters qualified support



Trainer analysis prompts

- Mark every point where a real transaction, personal disclosure, product endorsement, or data capture could accidentally occur.
- Identify what must be verified before delivery and what should remain fictional.
- Check whether each participant action demonstrates a decision rather than memory, speed, or app familiarity.
- Adapt one segment for a shared phone, low bandwidth, screen-reader use, low numeracy, and emerging literacy.
- Replace any deficit or blame wording with a neutral description of offender tactics and support options.
- Identify a safe stop route, an equivalent opt-out, and the trainer's referral boundary in each scenario.



9. Trainer quiz

1. During a workshop, a participant asks the trainer to help make a real low-value transfer so the practice feels authentic. What is the best trainer decision?
    - A. Decline, restate the no-real-transaction boundary, and use a fictional screen with the same decision steps.
    - B. Permit it if the participant operates the phone and hides the balance.
    - C. Observe without speaking, provided the amount is below an arbitrary low-value limit.
    - D. Ask the participant to complete it privately and report whether it worked.
2. A trainer is preparing a comparison of two digital remittance providers. Which approach is most appropriate?
    - A. Rank the provider with the highest app rating after noting that fees can change.
    - B. Verify legal entities and status, then compare the same amount, total cost, recipient amount, timing, access, and recourse without recommending either.
    - C. Prefer the regulated provider because regulation proves it is cheapest and suitable.
    - D. Compare headline fees and ask participants which brand they trust most.
3. A fee handout from a reputable organisation has no review date and conflicts with a provider's current public information. What should the trainer do?
    - A. Keep it because independent organisations are more neutral than providers.
    - B. Average the two fee figures and label the result approximate.
    - C. Quarantine the handout, verify dated authoritative sources and conditions, and update the resource record before use.
    - D. Use it only in print so participants do not follow the old link.
4. In a fictional drill, a caller who knows the account holder's name says an OTP is needed to cancel fraud. What response should the trainer model?
    - A. Read only the first half of the OTP, then ask the caller to confirm the account.
    - B. Enter the OTP if its message mentions security rather than payment.
    - C. Keep the caller waiting while searching the telephone number online.
    - D. End the call without sharing or entering the OTP, then contact the provider through an independently verified urgent route.
5. A participant privately says they may have paid a fraudster ten minutes ago. What is the best initial trainer response?
    - A. Respond without blame, stop further contact, support prompt use of the provider's verified fraud route, and follow privacy and safeguarding boundaries.

   - B. Collect screenshots and credentials so the trainer can determine exactly what happened first.
   - C. Ask the group whether anyone has recovered money from the same scam.
   - D. Wait until the session ends to avoid causing distress or embarrassment.
6. A trainer's fictional investment message promises guaranteed returns and says a regulator has approved the opportunity. How should it be facilitated?

   - A. Explain that guarantees are acceptable when a regulator is named and the starting amount is small.
   - B. Treat guarantees and authority claims as warning signs, verify independently, avoid investment advice, and point to official warning and reporting routes.
   - C. Compare the promised return with a savings account to decide whether the claim is realistic.
   - D. Remove the guaranteed figure but retain the offer as a neutral product-comparison example.
7. A planned venue has shared tablets and public Wi-Fi. Which design decision best meets the module standard?

   - A. Allow real account access in private-browser mode and clear the history afterwards.
   - B. Ask participants to use mobile data for authentication while the shared tablet displays balances.
   - C. Use offline fictional screens or print alternatives only, save no identifiers, and explain shared-device privacy risks.
   - D. Let participants decide whether the convenience outweighs the privacy risk.
8. In a fictional fee comparison, several participants find decimals and exchange rates difficult. What should the trainer do?

   - A. Skip total cost and focus on recognising the provider logo and send button.
   - B. Pair participants by speed so stronger participants can complete the calculations for others.
   - C. Ask for real remittance amounts because familiar numbers are easier to understand.
   - D. Start with round fictional values, separate amount, fee, total, and recipient amount visually, permit calculators, and assess the decision rather than speed.
9. A trainer wants evidence for a fraud-response drill while protecting privacy. Which collection plan is best?

   - A. Record performance against a checklist using fictional case IDs and no credentials; for a real disclosure, collect nothing beyond the minimum required by the authorised safeguarding process.

- B. Save screenshots in a restricted folder because access control makes full evidence proportionate.
- C. Ask participants to forward suspicious messages after deleting their names and account numbers.
- D. Record the role-play on personal phones and delete recordings after marking.

10. A fictional transfer remains marked `pending`, and the sender is unsure whether it was completed. What should the trainer model?

    - A. Repeat the transfer with a smaller amount to test whether the first one failed.
    - B. Do not repeat it; check the recorded status and use the provider's independently verified support route.
    - C. Treat `pending` as equivalent to `rejected` and begin a new transfer.
    - D. Ask the recipient to confirm the amount before checking the provider's status.

11. References

- Council of Europe. (2022). *Literacy and Second Language Learning for the Linguistic Integration of Adult Migrants (LASLLIAM): Reference guide*. https://www.coe.int/en/web/language-policy/laslliam
- European Banking Authority. (2024). *Opinion on new types of payment fraud and possible mitigants*. https://www.eba.europa.eu/sites/default/files/2024-04/363649ff-27b4-4210-95a6-0a87c9e21272/Opinion%20on%20new%20types%20of%20payment%20fraud%20and%20possible%20mitigations.pdf
- European Banking Authority. (n.d.). *Frauds and scams*. https://www.eba.europa.eu/activities/information-consumers/frauds-and-scams
- European Union. (2016). *Regulation (EU) 2016/679 (General Data Protection Regulation)*, Article 5, Principles relating to processing of personal data. https://eur-lex.europa.eu/eli/reg/2016/679/oj
- European Union Agency for Cybersecurity. (2020). *ENISA Threat Landscape 2020: Phishing*. Used here for phishing and social-engineering methods. https://www.enisa.europa.eu/sites/default/files/publications/ETL2020%20-%20Phishing%20A4.pdf
- Redecker, C. (2017). *European Framework for the Digital Competence of Educators: DigCompEdu*. Punie, Y. (Ed.). Publications Office of the European Union. https://publications.jrc.ec.europa.eu/repository/handle/JRC107466
- Vuorikari, R., Kluzer, S., and Punie, Y. (2022). *DigComp 2.2: The Digital Competence Framework for Citizens, with new examples of knowledge, skills and attitudes*. Publications Office of the European Union. https://publications.jrc.ec.europa.eu/repository/handle/JRC128415
- World Wide Web Consortium. (2023). *Web Content Accessibility Guidelines (WCAG) 2.2*. W3C Recommendation. https://www.w3.org/TR/WCAG22/

LINK UP: Digital Empowerment and Community Engagement for Third-Country National Women

2025-1-DE02-KA220-ADU-000350564

WP2: Public Service Awareness Modules

Module 4: Cultural event calendars

Module 4: Cultural event calendars

Module overview

Field	Details
Audience	Trainers, educators, social workers, and facilitators working with TCN women
Duration	2-4 hours
Delivery method	Face-to-face / Online / Blended
Scope	Finding, checking, comparing, and communicating information about cultural and social events
Lead partner(s)	Stichting Netwerkpro (Netherlands)

Information literacy and voluntary, informed choice are the outcomes. Registration and attendance are never required evidence of success.



Trainer competencies

By the end of this module, trainers can:

1. **Distinguish scope** by correctly classifying event-calendar cases as Module 4 or broader community-information cases as Module 5.
2. **Evaluate event information** by checking ownership, currency, organizer identity, venue confirmation, commercial purpose, and ticket or registration routes.
3. **Evaluate feasibility** by recording stated, missing, and uncertain information about total cost, travel, timing, eligibility, caring responsibilities, accessibility, and cancellation.
4. **Apply privacy and safer-practice principles** by minimizing data, identifying scam indicators and unnecessary app permissions, and avoiding claims that a provider, venue, journey, or event is safe.

5. **Design inclusive facilitation** that supports participant-led choice across physical, sensory, communication, digital, social, language, literacy, mobile, print, and offline needs.
6. **Explain information-literacy evidence** as source verification, comparison, and proportionate decisions rather than registration, attendance, disclosure, or social participation.

1. Scope and professional boundaries

Module 4 and Module 5

Module 4 addresses time-bound cultural and social events: exhibitions, performances, festivals, library activities, community arts, language exchanges, family activities, and similar listings. It covers event details, organizer and ticket checks, feasibility, registration information, and optional attendance planning.

Module 5 addresses broader local initiatives, services, community news, campaigns, support organizations, volunteering, and ongoing groups. A calendar may contain both. Classify the **information need**, not only the website. An event listing remains in Module 4; a page about joining the organizing association, accessing a service, or following local policy belongs in Module 5.

Do not expand Module 4 into tourism promotion, cultural assimilation, or attendance recruitment. The trainer's role is to strengthen informed choice, not to decide what counts as valuable culture or successful participation.



Core terms for trainer use

- **Calendar provider:** The platform that collects, ranks, or displays listings. It may be a municipality, venue, tourism body, community organization, social platform, or commercial marketplace.
- **Organizer:** The body responsible for delivering the event. It may differ from the calendar provider, venue, promoter, or ticket seller.
- **Venue:** The physical or digital location hosting the event. Venue confirmation can help detect incorrect or fraudulent listings but does not guarantee quality or safety.

- **Ticket or registration source:** The route that collects a booking, payment, or participant data. A link is not trustworthy merely because it appears beside a genuine event name.
- **Sponsored listing:** Placement influenced by payment or promotion. Prominence is not evidence of suitability or reliability.
- **Accessibility information:** Stated conditions that support participation. Missing information must be marked `not stated`, not inferred.



2. Professional foundation

Due diligence across the event chain

Treat the calendar provider, organizer, venue, and ticket source as separate actors. Trust in one must not be transferred automatically to another.

Calendar provider checks

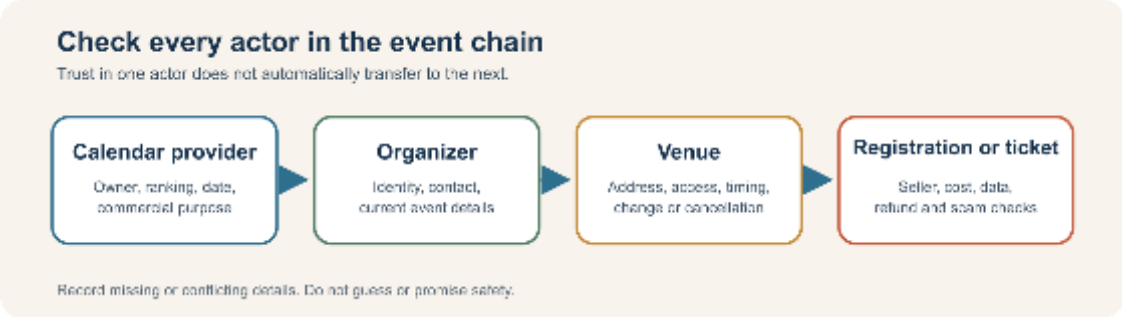
- Identify the owner, purpose, geographic coverage, editorial or moderation process, contact route, and commercial model.
- Check whether paid placement, affiliate links, popularity, or personalization affects ranking.
- Check update dates, account requirements, cookie or tracking choices, app permissions, language support, and accessible alternatives.
- Compare important details with the organizer or venue rather than relying on an aggregator alone.

Organizer and venue checks

- Confirm that the organizer is named and has a consistent official or recognized public presence and contact route.
- Compare event title, date, time, address, audience conditions, access information, and cancellation notices across current pages.
- Look for realistic descriptions and clear responsibility. Testimonials, follower counts, branding, and HTTPS alone are not verification.
- Confirm who answers access, safeguarding, ticket, refund, or complaint questions. Do not imply that a response guarantees a safe experience.

Ticket and registration checks

- Reach the seller from the organizer's or venue's current page where possible; inspect the domain before entering data or paying.
- Confirm seller status, price, currency, fees, refund and transfer terms, cancellation process, and official resale or waiting-list route.
- Treat direct-message sales, urgent bank transfer or cryptocurrency requests, mismatched domains, and requests to bypass the official route as stop signals.
- Do not use a real participant account, payment, identity document, or contact detail in training.



Event information chain showing separate checks for the calendar provider, organizer, venue, and registration or ticket route.

Currency, changes, and cancellation

Search engines can surface an old listing that still looks active. A saved screenshot is evidence of what was displayed, not evidence that the event remains current.

Before presenting an example and before any optional journey, check:

- the full date, year, start and finish time, time zone, and registration deadline;
- the organizer's and venue's current pages, including change or cancellation notices;
- whether the address, room, online link, language, price, and access arrangements have changed;
- whether the event is sold out and whether an official waiting list exists; and
- how registered people are notified and what happens to payments and submitted data after cancellation.

Teach uncertainty explicitly. Use `confirmed on [date]`, `not stated`, `conflicting information`, or `requires direct confirmation`. Never repair missing details by guessing.

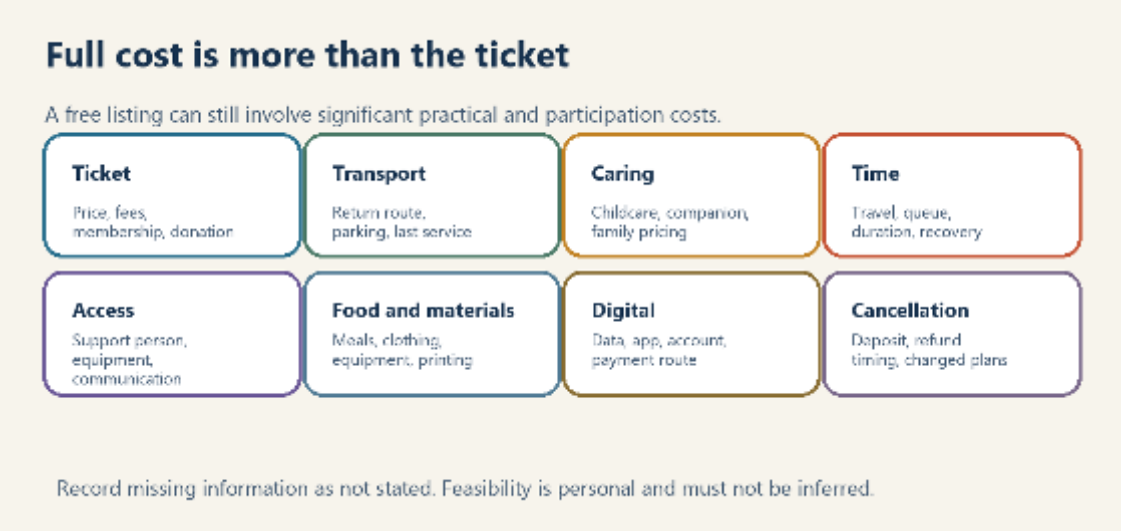


Full cost and feasibility

`Free` usually describes the ticket, not the whole experience. A sound analysis can include:

- ticket, booking, membership, platform, payment, or mandatory donation fees;
- return transport, parking, fuel, tolls, and the last available return service;
- childcare or other caring arrangements, companion or support-person costs, and family pricing;
- food, clothing, equipment, mobile data, printing, and cloakroom costs;
- deposits, cancellation exposure, refund timing, and currency conversion;
- travel time, queueing, event duration, recovery time, weather, and schedule compatibility; and
- cognitive effort, sensory load, language demand, social pressure, and confidence attending alone.

Check whether concessions require evidence and whether `per person`, `per family`, or age rules are clear. Missing cost information is not zero cost. Feasibility is personal and can change; trainers support comparison without requesting financial, family, health, or immigration details.



Eight full-cost factors for an event: ticket, transport, caring, time, access, food and materials, digital requirements, and cancellation.

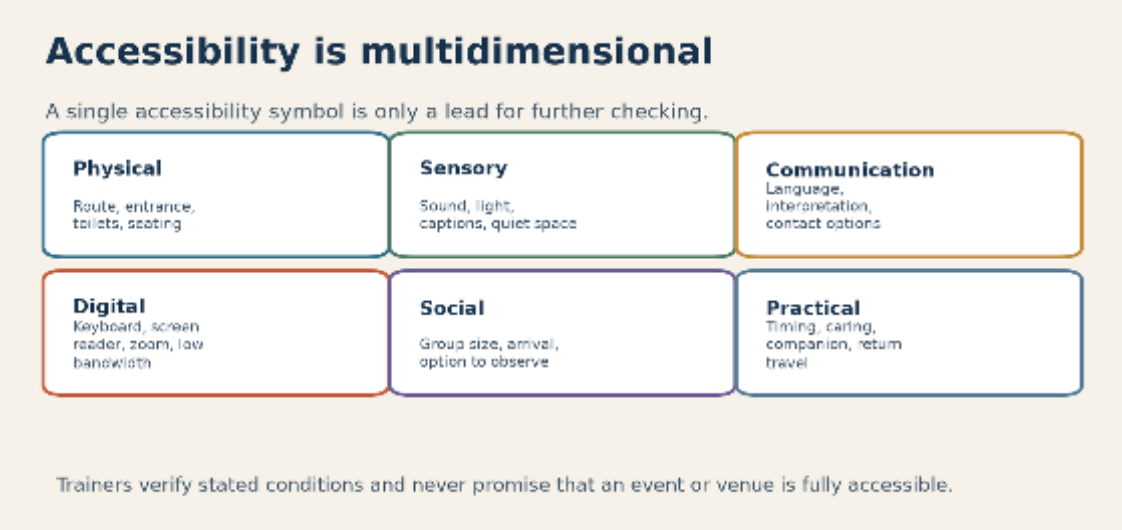
Accessibility as an information-quality issue

Accessibility is broader than step-free entry. Examine what the listing states and how a person can confirm:

- **Physical:** route, entrance, lifts, toilets, seating, rest space, parking, support-person policy, and mobility-device access.
- **Sensory:** lighting, sound level, quiet space, hearing support, captions, audio description, and sensory warnings.
- **Communication:** plain language, interpretation, contact methods, response times, and alternatives to telephone-only contact.

- **Digital:** keyboard operation, screen-reader structure, zoom and reflow, contrast, captions, accessible forms, low-bandwidth access, and no-app route.
- **Social:** group size, arrival process, option to observe, peer or companion choice, women-only or family conditions where stated, and a clear way to leave.

An accessibility symbol is a useful lead, not complete evidence. Trainers should never diagnose needs, promise accommodation, or describe a venue as fully accessible without current, specific information.



Six dimensions of event accessibility: physical, sensory, communication, digital, social, and practical.

Autonomy, culture, and social anxiety

- Finding, checking, comparing, saving, printing, or rejecting an event are valid outcomes.
- Do not register anyone, create an account, buy a ticket, or set attendance as a course requirement or evidence of integration.
- Do not assume that participants want family, migrant-specific, women-only, faith-based, free, mainstream, or heritage events.
- Do not treat a name, language, clothing, nationality, religion, family role, or migration history as a cultural preference.
- Do not ask anyone to explain why an event, mixed group, journey, venue, or social situation feels unsuitable.
- Social anxiety may affect searching, contacting, arriving, joining, or leaving. Offer observation, fictional scenarios, pair or solo work, a pause, and a no-explanation opt-out.
- A participant leads the final choice, including the choice to take no further action. Trainer enthusiasm must not become attendance pressure.



Registration privacy and data minimization

Apply GDPR principles whether or not the trainer is the data controller: purpose limitation, data minimization, accuracy, storage limitation, security, transparency, and accountability.

- Separate information that is required for a booking from optional marketing, profile, demographic, photo, or location data.
- Question requests for identity documents, immigration status, full date of birth, gender, contacts, or precise location when they are not evidently necessary.
- Check who collects the data, for what purpose, on what basis, for how long, with whom it is shared, and how rights or cancellation requests can be exercised.
- Do not complete forms, accept cookies, enable location, upload documents, or change a participant's device permissions as a demonstration.
- Prefer a public web, telephone, in-person, or paper route when an app asks for unrelated contacts, photos, microphone, or continuous location access.
- Obtain separate, specific consent for training photographs or recordings. Refusal must not reduce participation. Never publish a live location or infer consent from attendance.


Username
1234
Next
1234

3. Non-sensitive needs analysis and safer practice

Needs analysis without personal disclosure

Collect only information needed to adapt delivery. Ask about preferred learning conditions, not the reason behind them.

Suitable prompts for course planning include:

- preferred language and format;
- phone, shared-device, computer, print, or no-device access;
- internet reliability and need for an offline route;
- preferred pace, group size, and option to work alone or with a peer;
- requirements for captions, audio, large print, keyboard access, plain language, breaks, or seating; and
- whether an anonymous question route or private conversation with an authorized staff member is useful.

Do not collect immigration status, diagnosis, income, childcare circumstances, literacy label, religion, address, live location, or history of harassment to sort people into activities. Make responses optional, explain their use, restrict access, set a deletion date, and provide broadly useful adaptations without requiring proof.



Safer delivery and safeguarding boundaries

Safety is a process, not a promise. A trainer can teach risk checks and follow organizational duties but cannot certify an event, organizer, neighborhood, route, platform, or person as safe.

- Use fictional profiles, prepared screenshots, public listings, and dummy forms. Remove names, booking codes, QR codes, contact details, and device notifications from examples.
- Consider outward and return travel, service disruption, lighting, accessibility, venue entry, dependency or caring arrangements, and what to do if plans change.
- Offer general planning options without asking participants to disclose routines, addresses, immigration status, or who they live with.
- Do not require buddying, location sharing, emergency-contact disclosure, or trainer accompaniment. Present available options and preserve autonomy.
- Know the organization's safeguarding, incident, harassment, disclosure, and emergency procedures and the limits of trainer confidentiality.
- If a safeguarding concern arises, listen without investigating, avoid promises of secrecy or safety, record only what policy requires, and use the designated referral or emergency route.
- If a suspected scam has caused loss or exposure, preserve relevant evidence only with consent and policy authority, stop further contact, and refer to verified reporting and support routes.



4. Guided event-source evaluation

Purpose and materials

Use two plausible event sources and one contrasting listing, such as an outdated entry, sponsored aggregator result, or fictional scam ticket page.

Validation procedure

For each resource, create a short validation record containing:

1. **Identity and scope:** URL, provider, owner, contact, purpose, and commercial or sponsored status.
2. **Currency:** date checked, visible update date, working links, current sample event, and evidence from the organizer or venue.
3. **Event chain:** calendar provider, organizer, venue, registration or ticket controller, payment seller, and any unresolved mismatch.
4. **Information completeness:** date and year, start and finish, location, language, eligibility, total cost, registration, cancellation, physical and sensory access, communication route, and digital requirements.
5. **Privacy and risk:** account requirement, data fields, privacy notice, cookies or tracking, app permissions, photo or location practice, scam indicators, and safer alternatives.
6. **Format access:** mobile behavior, keyboard and zoom check, plain-language burden, translation quality, print result, low-bandwidth route, offline contact, and support-person information.
7. **Decision:** `use`, `use with a stated limitation`, `hold for confirmation`, or `do not use`, with reasons and evidence links.

Evaluation standard

A sound review:

- compares important claims across at least two appropriate sources rather than counting links;
- marks absent or conflicting details instead of inferring them;
- traces a ticket or registration link without entering data or payment information;
- records total likely cost and at least one travel, access, and cancellation consideration;
- identifies the minimum data apparently needed and any disproportionate request or permission;
- tests a mobile and non-digital route; and
- uses a current screenshot or excerpt with personal data removed and a visible check date.

Do not retain copied listings longer than needed. Preserve the source URL and validation notes so future trainers can recheck rather than assume that the evidence remains current.



5. Inclusive facilitation and adaptation

Participant-led choice

Design facilitated practice around fictional preference cards or trainer-prepared listings. Participants should be able to select criteria, change a criterion, compare without choosing, observe without searching, or stop without explanation. Avoid public rounds asking what each person wants to attend.

Model neutral language:

- say `This source states...` rather than `This event is safe`;
- say `not stated` rather than filling a gap;
- say `one available option` rather than `the right event for you`;
- say `Would another format help?` rather than asking for a diagnosis; and
- say `No next action is required` before discussing registration or attendance.

Use peer work only as an option. Set roles that do not require personal disclosure, such as source checker, detail finder, access checker, or question recorder. A confident participant should not take control of another person's device, form, account, or decision.

Mobile, multilingual, print, and offline design

Mobile

- Use short, numbered steps and one task per screen.
- Test portrait view, zoom, keyboard access, link labels, pop-ups, cookie controls, map alternatives, and data consumption.
- Avoid mandatory downloads, account creation, QR-only access, and demonstrations on personal accounts.

Multilingual and literacy-responsive

- Pre-check translated search terms, dates, times, costs, venue names, registration conditions, and culturally specific terms with a competent reviewer.
- Keep the original listing available because machine translation can alter dates, negation, eligibility, and accessibility details.
- Use plain language, short chunks, spoken explanation, labelled icons, audio, demonstration, repetition, and teach-back without testing reading speed.
- Support right-to-left scripts and allow responses by pointing, speaking, ordering cards, or using a scribe.

Print and offline

- Print the source, URL, contact, date checked, and warning that details can change; do not rely on a QR code alone.
- Provide large-print and high-contrast versions and ensure images have an equivalent text description.
- Identify verified library, municipality, venue, community-center, telephone, or in-person routes. Check opening hours, language support, call costs, and physical access.
- Recheck printed examples immediately before use and withdraw obsolete copies.



Troubleshooting guide

Situation	Trainer response
Search results show an old event	Use it to model date and year checks, then locate a current organizer or venue update. Do not present it as available.
Sources disagree	Compare publication times and responsible actors; mark the conflict and contact a verified source or choose a clearer example.

Situation	Trainer response
The event is changed, cancelled, or sold out	Check the official notice, refund or waiting-list route, and data handling. Do not use unofficial ticket offers.
Access, language, or cost is missing	Record `not stated`; use a verified contact or select a listing with better information.
An app requires broad permissions	Do not install it for practice. Use a browser, print, telephone, or in-person alternative and document the limitation.
Translation changes an important detail	Compare with the original and confirm through a competent person or the organizer before teaching it.
Internet or device access fails	Continue with dated print extracts, screenshots, sorting cards, and verified offline contacts.
A participant discloses distress, harassment, or loss	Pause the activity, protect privacy, avoid investigation, and follow the organization's support and safeguarding route.

6. Model workshop for trainer analysis

This 75-minute example applies the module's verification, privacy, accessibility, and participant-choice principles.

Illustrative purpose: Practise extracting, checking, and comparing event information through fictional preferences and public or simulated listings, with no registration, payment, location sharing, or attendance.

Prepared materials: Two current verified listings, one contrasting or incomplete listing, fictional preference cards, a dated print version, a phone-sized version, a plain-language event-check sheet, and verified offline contact information.

Exemplar flow for trainer analysis

1. **Choice and boundaries, 10 minutes:** The trainer states that observation, comparison, rejection, and stopping are valid; no personal need or intended attendance is requested.
2. **Modelled verification, 15 minutes:** Using a fictional profile, the trainer distinguishes provider, organizer, venue, and ticket source; checks the date; and records missing information without registering.
3. **Optional pair or solo comparison, 20 minutes:** Participants use fictional criteria to compare two prepared listings. Roles and observation are optional, and no one uses a personal account.
4. **Feasibility and access check, 15 minutes:** The trainer elicits stated total cost, travel, timing, language, access, data, and cancellation information, while preventing assumptions about individual circumstances.
5. **Participant-led decision, 10 minutes:** Each person may identify which listing is better evidenced, request another format, record uncertainty, reject both, or give no decision.
6. **Close, 5 minutes:** The trainer reinforces that the demonstrated skill is verification and comparison, while registration and attendance remain optional and outside the activity.

Trainer analysis prompts

- Where does the exemplar visibly separate information checking from attendance?
- Which statements could accidentally imply that an official source or event is safe?
- What evidence is required before the two listings can be used?
- How would the flow change for one shared phone, no internet, low literacy, screen-reader use, translated delivery, or high social anxiety?
- Which step gives participants meaningful control, including rejection or observation?
- What would count as observable information-literacy performance without collecting personal data?



7. Trainer quiz

1. A municipality calendar and a community social page list the same event, but the start times differ. Which source strategy should the trainer model?
    - A. Use the municipality time because public providers are always current.
    - B. Compare update dates and confirm the time on the organizer's or venue's current page before using the example.
    - C. Use the social-page time because community pages update faster.
    - D. Average the two times and tell participants to arrive early.
2. A search result shows a well-written festival listing from last year with no current-year organizer page. What should the trainer do?
    - A. Use it if the annual festival usually occurs in the same month.
    - B. Present it as current but ask the group to verify it after the session.
    - C. Remove the year from the screenshot and use it to practise event selection.
    - D. Treat it only as an outdated-information example unless a responsible current source confirms a new event.
3. A sold-out event is followed by a direct message offering cheaper tickets through an urgent bank transfer. What is the best training decision?
    - A. Model stopping, avoiding the link and payment, and checking only the organizer's official resale or waiting-list route.
    - B. Compare the seller's profile age and proceed if it has a long history.
    - C. Ask the seller for an identity document before deciding.
    - D. Make a small transfer from a trainer account to demonstrate the risk.
4. A local event app requests contacts, photos, microphone, and continuous location access before showing listings. What should the trainer do?
    - A. Install it on participants' phones and switch off permissions after practice.
    - B. Approve the permissions because local recommendations depend on personalization.
    - C. Use a public browser, print, telephone, or in-person route and document the app as unsuitable for the activity.
    - D. Ask participants to decide together which permissions everyone should grant.
5. A free library activity asks registrants for an identity document, immigration status, full date of birth, and marketing consent. What should the trainer model?
    - A. Complete the form with fictional data to see whether all fields are enforced.
    - B. Pause, verify the purpose and controller through an official contact, check for a less intrusive route, and avoid submission meanwhile.
    - C. Recommend the form because a public venue would not request unnecessary data.

- D. Submit only the document and decline the other fields.

6. A trainer assumes women in the group will prefer a women-only cultural event connected to their countries of origin. Which redesign is best?
    - A. Keep the event but let participants explain publicly if it is unsuitable.
    - B. Select a mainstream event instead so culture does not affect the session.
    - C. Ask a community representative to choose one culturally appropriate event for everyone.
    - D. Offer varied fictional criteria and formats, allow private or no selection, and avoid inferring preferences from identity.
7. A translated event-search example was created several months ago. Before reusing it, what is the most important check?
    - A. Recheck the sources, language, currency, total cost, travel, access contacts, registration rules, and cancellation arrangements.
    - B. Keep the original details because translation review also confirms that the example is current.
    - C. Add more event platforms so every possible interest is represented.
    - D. Keep the screenshots unchanged because consistency is more important than currency.
8. A group includes emerging readers, screen-reader users, and people with limited data. Which design is strongest?
    - A. Provide a simplified app and ask peers to read difficult sections aloud.
    - B. Use icon-only mobile instructions because text and print create literacy barriers.
    - C. Provide short plain-language steps, labelled visuals, structured digital text, audio or spoken support, large print, and an equivalent offline route.
    - D. Demonstrate once on a projector and provide the link for later independent review.
9. A venue asks the trainer to post group photos and tag the live location as evidence of community engagement. What should the trainer do?
    - A. Announce the photo in advance and treat continued attendance as consent.
    - B. Decline live-location sharing and use separate informed opt-in consent, a fully equivalent no-photo option, and clear use and deletion information.
    - C. Photograph the room from behind so individual consent is unnecessary.
    - D. Ask participants to remove tags later if they become uncomfortable.
10. Which activity best supports this module's information-literacy goal?
    - A. Use a fictional simulation in which participants can find, verify, compare, mark uncertainty, and choose a proportionate next step or no action.
    - B. Count how many participants create accounts and save an event.

- C. Ask participants to report whether they attended a local event within one month.
- D. Score a written definition test about calendars, organizers, and tickets.

References

- Council of Europe. (2022). *Literacy and Second Language Learning for the Linguistic Integration of Adult Migrants (LASLLIAM): Reference Guide*. Council of Europe LASLLIAM.
- European Parliament and Council of the European Union. (2016). *Regulation (EU) 2016/679 (General Data Protection Regulation)*, especially Articles 5, 12, 13, and 25. EUR-Lex.
- Redecker, C. (2017). *European Framework for the Digital Competence of Educators: DigCompEdu*. Punie, Y. (Ed.). Publications Office of the European Union. https://doi.org/10.2760/159770.
- Vuorikari, R., Kluzer, S., and Punie, Y. (2022). *DigComp 2.2: The Digital Competence Framework for Citizens, with new examples of knowledge, skills and attitudes*. Publications Office of the European Union. https://doi.org/10.2760/115376.
- World Wide Web Consortium. (2023). *Web Content Accessibility Guidelines (WCAG) 2.2*, W3C Recommendation. https://www.w3.org/TR/WCAG22/.



LINK UP: Digital Empowerment and Community Engagement for Third-Country National Women

2025-1-DE02-KA220-ADU-000350564

WP2: Public Service Awareness Modules

Module 5: Local initiatives and community news

Module 5: Local initiatives and community news

Module overview

Field	Details
Audience	Trainers, educators, social workers, and facilitators working with TCN women
Duration	3-5 hours
Delivery method	Face-to-face / Online / Blended
Scope	Local information classification, source evaluation, privacy, safety, referral, and inclusive facilitation
Lead partner(s)	Institute TREND-PRIMA, Maribor (Slovenia)

Purpose

Local information can open routes to support, civic participation, volunteering, and timely public information. The same ecosystem can circulate outdated notices, disguised advertising, false grants, harassment, unsafe recruitment, and rapidly translated rumours. Trainers therefore need more than a list of websites: they need a repeatable process for validating resources, explaining uncertainty, protecting privacy, and referring concerns without shame or unnecessary data collection.

Core principles are:

- start with one or two clear, verified sources rather than many platforms;
- distinguish the information type before deciding how to verify or act;
- compare source, date, purpose, and corroboration;
- use public pages, fictional profiles, prepared screenshots, and offline alternatives;
- never require a real account, post, direct message, document upload, or live location in training; and
- review live examples before delivery and on a defined maintenance cycle.



Trainer competencies

By completing this module, the trainer can:

1. **Classify** local examples accurately as initiatives, services, volunteering, public notices, news, opinion, advertising, or events, and explain the Module 4 boundary.
2. **Map** a local information item by originator, source, owner, editorial or moderation process, sponsor, distribution channel, and intended purpose.
3. **Verify** a consequential local claim with S-D-P-C, lateral reading, and proportionate triangulation, while explaining why ranking and popularity are not evidence.
4. **Design** privacy-preserving responses to misinformation, unsafe messaging, exploitative volunteering, crisis alerts, harassment, and safeguarding concerns.
5. **Evaluate sources** for ownership, access, inclusion, risk, currency, and offline alternatives.
6. **Plan inclusive facilitation** using accessible, multilingual, mobile-first verification and psychologically safe, non-shaming methods.

1. Scope and information taxonomy

Correct classification matters because each type has a different authority, purpose, risk, and verification route.

Local initiative

An organized project or collective action intended to change or improve a local condition. It may be time-limited or continuing and may be led by residents, an association, a public body, or a partnership.

Trainer check: identify the organizer, objective, governance, funding, area served, participation conditions, and evidence of current activity. A good intention or many followers does not establish legitimacy.

Service

An ongoing or recurring provision of practical, social, legal, health, educational, or administrative support. A service should state who provides it, eligibility, scope, contact route, cost, opening arrangements, and data required.

Trainer check: distinguish the provider from a directory that merely lists it. Confirm high-consequence details with the responsible provider.

Volunteering

Freely chosen, unpaid activity intended to benefit others or the community, usually with a defined organizer and role. Reimbursement of agreed expenses is not pay.

Trainer check: volunteering is not automatically safe, lawful, inclusive, or free from exploitation. Apply the due-diligence process in Section 4.

Public notice

An official operational or regulatory communication from the body responsible for a rule, closure, deadline, public-health measure, consultation, emergency, or service change.

Trainer check: confirm the issuing authority, jurisdiction, publication time, effective period, update or cancellation status, and original page. A screenshot of a notice is not the notice itself.

News

Reported information about recent matters of public or community relevance. News normally involves selection, verification, editing, correction, and publication, although standards vary across outlets.

Trainer check: identify the named outlet and journalist where available, evidence cited, editorial standards, corrections route, ownership, date, and distinction between reporting and commentary.

Opinion

Interpretation, judgement, advocacy, or personal viewpoint. It can be informed and valuable but should not be presented as verified fact or official instruction.

Trainer check: look for labels such as commentary, editorial, letter, column, or personal post, then separate factual claims from conclusions.

Advertising and sponsored content

Paid or commercially motivated communication intended to promote a product, service, opportunity, organization, or action. Sponsored content may resemble news or a community recommendation.

Trainer check: locate the advertising or sponsorship label, payer, beneficiary, claims, fees, data requests, and conflict of interest. Payment does not make content automatically false, and visual similarity to news does not make it editorially independent.

Events

Time-bound gatherings such as meetings, cultural activities, workshops, or festivals. An event may be organized by an initiative or service, but the event remains a distinct information type.



2. The local information ecosystem

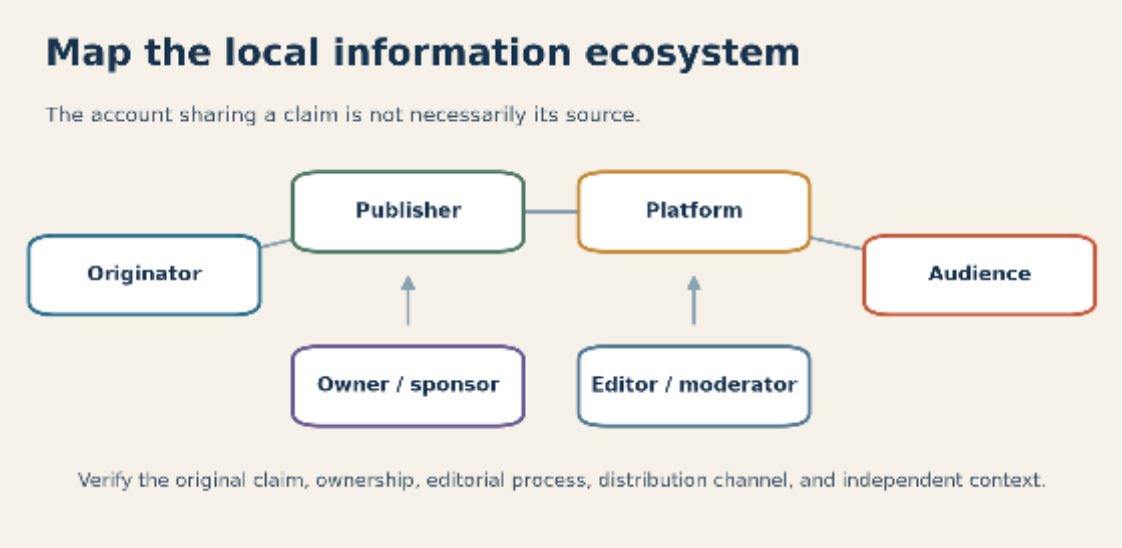
Map the whole route

A local claim moves through several roles. One organization may hold more than one role.

- **Originator:** creates the underlying decision, service, project, evidence, or observation.
- **Publisher or source:** makes the specific item available and takes responsibility for it.
- **Owner:** legally or financially controls the outlet, page, organization, or platform.
- **Editorial process:** selects, verifies, frames, corrects, and updates published material.
- **Moderator:** manages membership and conduct in a forum or group; moderation is not fact-checking unless explicitly designed as such.
- **Sponsor or advertiser:** pays for visibility or association and may have an interest in the response.
- **Platform or channel:** distributes or hosts the item, such as search, social media, messaging, a newsletter, radio, print, or a noticeboard.
- **Amplifier:** recirculates the item, often without adding evidence, through reposts, screenshots, influencers, or community chats.
- **Human access point:** provides clarification or offline help through a municipality desk, library, community centre, volunteer centre, recognized organization, or helpline.

The account sharing a claim is not necessarily its source. Ten sites repeating one press release are not ten independent confirmations. A private group may have active moderators but unclear ownership. An official source may be authoritative for its own rule yet poor at explaining community impact. Independent journalism and recognized community organizations can add scrutiny and access context.





Local information ecosystem connecting the originator, publisher, platform, audience, owner or sponsor, and editor or moderator.

Questions for trainer analysis

- Where did the claim originate, and where did the trainer encounter it?
- Who can correct or update it?
- What editorial or moderation process is visible rather than assumed?
- Who owns or funds the channel, and is sponsorship labelled?
- Which source is authoritative for the specific claim, and which independent source can test or contextualize it?
- What human or offline route remains if the digital channel fails?



3. Verification foundation

S-D-P-C

Use S-D-P-C as a visible, memorable first pass.

1. **Source:** Who published the item? Is the original source identifiable? Are ownership, contact, editorial standards, and correction routes visible?
2. **Date:** When was it published, updated, or effective? Does it use a different calendar, time zone, or an old screenshot? Has it been superseded or cancelled?
3. **Purpose:** Is it reporting, an official instruction, opinion, recruitment, fundraising, advertising, advocacy, entertainment, or provocation? Who benefits from action?
4. **Check:** Can the consequential claim be traced to original evidence and corroborated through an appropriate independent route?

S-D-P-C is not a mechanical trust score. A current date cannot repair anonymous ownership, and an official logo cannot establish that a copied page is genuine. The trainer models a reasoned decision: **use, use with a limitation, pause and verify, or do not use**.



S-D-P-C verification method: check source, date, purpose, and corroboration before deciding whether to use information.

Triangulation and lateral reading

For a consequential claim, move away from the page and inspect the wider evidence environment.

- Trace a quote, policy, alert, grant, or service change to the responsible originator.
- Compare with a credible independent report or recognized organization that has its own verification process.
- Confirm operational details through a published human contact when uncertainty remains and contact is safe.
- Search the outlet or organization name with terms such as `owner`, `about`, `correction`, `scam`, or the local-language equivalent.
- Check whether apparently separate reports copy the same text, image, or unnamed source.
- Record disagreement and uncertainty rather than forcing a false consensus.

Triangulation should be proportionate. A high-consequence claim about legal status, health, money, safety, or crisis action needs stronger confirmation than a low-risk community-interest item. During an immediate official emergency alert, follow the authorized instruction first; do not delay protective action to complete a classroom-style source comparison.



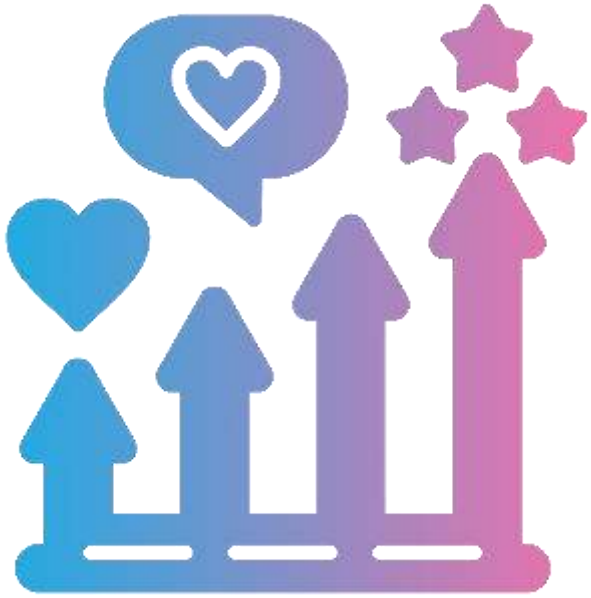
Search ranking, algorithms, and popularity

Search and social platforms rank content using changing combinations of relevance, location, language, freshness, personalization, prior behaviour, engagement, advertising, and search-engine optimization. The first result may be paid, popular, nearby, or tailored; it is not automatically the most authoritative.

Trainers should demonstrate these distinctions:

- **rank** means placement by a system;
- **reach** means how many accounts may have received content;
- **engagement** means interactions such as views, shares, or comments;
- **popularity** means attention or approval; and
- **evidence** supports whether a claim is accurate.

High engagement can result from fear, outrage, novelty, coordinated promotion, or repeated correction. Search snippets can omit dates and qualifiers. Personalization means two people may see different results. Sponsored placement must be identified before comparison.



Multilingual misinformation

Misinformation can change as it crosses languages and formats. Common patterns include:

- an accurate old notice translated and recirculated as current;
- a policy condition or negation lost in translation;
- a voice note with no traceable source;
- a real image paired with a false local caption;
- a place or organization with several transliterations;
- copied text that changes dates, currencies, eligibility, or jurisdiction;
- machine translation that makes an uncertain claim sound definite; and
- rumours moving rapidly through trusted family or community networks.

Trainer verification should:

1. preserve and inspect the original-language item where lawful and safe;
2. identify the exact claim, place, date, and action rather than translating only keywords;
3. compare an official version and a competent human or recognized bilingual explanation when available;
4. label machine translation and check critical words with a second route;
5. avoid asking a participant to interpret sensitive material for the group; and
6. explain uncertainty in plain language without implying that a language or community is the problem.

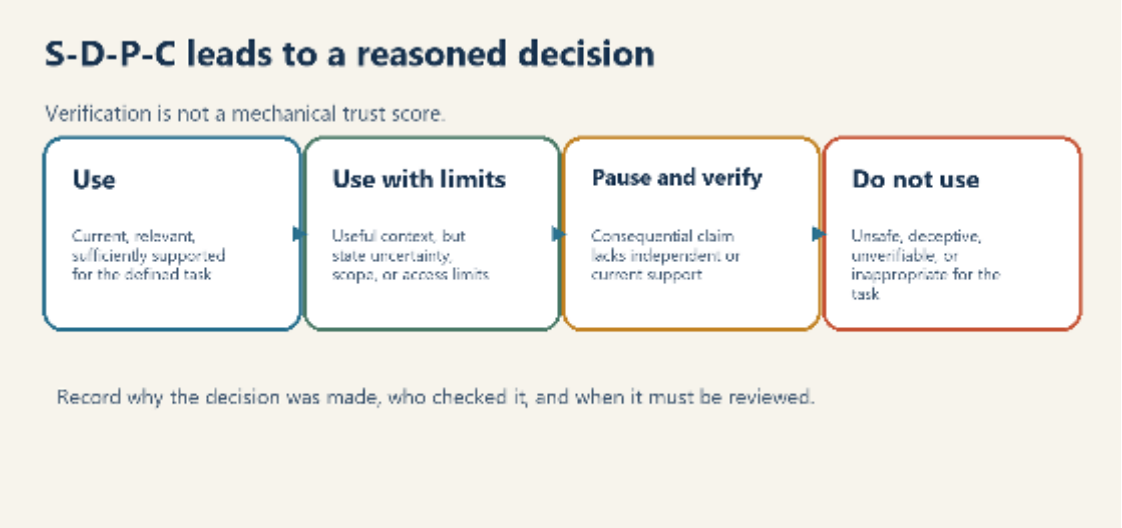


Non-shaming correction

Public humiliation makes correction less likely to be heard and can expose the person who shared a rumour. The trainer should:

1. pause further circulation;
2. acknowledge the concern or helpful intent without affirming the false claim;
3. state the corrected fact briefly and identify the current evidence;
4. avoid repeating a harmful falsehood more than necessary;
5. provide a concrete safe next action and an offline route;
6. correct in the same channel when appropriate, without naming or exposing the original sharer; and
7. revisit the resource pack if the training example itself caused confusion.

Useful trainer wording is: “The issue matters, and this version is not confirmed. The responsible source currently states X. Before anyone acts or shares, use this current route or contact this verified service.”



Four possible verification decisions: use, use with limits, pause and verify, or do not use.

4. Safety, privacy, and safeguarding

Training boundaries

For all demonstrations and facilitated practice:

- do not ask for an address, immigration status, family situation, support need, identity document, account name, or current location;
- do not require joining a social network, private group, newsletter, volunteer activity, or messaging channel;
- do not post, comment, accept requests, send a direct message, or share live location from a real account;
- do not open suspicious links, scan unknown QR codes, or download unexpected files;
- use fictional profiles, redacted screenshots, prepared comparisons, and public pages; and
- make observation and a non-digital route valid ways to participate.

Public groups, private groups, and direct messages

- **Public group:** posts and member details may be visible, searchable, copied, or archived beyond the intended audience.
- **Private group:** access is restricted but members can still copy content; the label `private` does not establish confidentiality, good moderation, or trustworthy ownership.
- **Direct message:** less visible than a public post but still recordable, forwardable, impersonated, and subject to platform access or account compromise.

Before presenting a community channel, check its owner, moderators, rules, membership questions, complaint route, visible member data, commercial interests, and history of updates. Do not present an unmoderated group or commercial platform as an official or universally safe route.



Location and privacy

Demonstrate with prepared screens rather than changing real settings. Explain that posts, photos, file metadata, check-ins, map links, background landmarks, and repeated routines can reveal location. A disappearing message or temporary location can still be captured.

Apply GDPR Article 5 principles to all trainer-controlled information:

- **lawfulness, fairness, and transparency:** state what is collected and why;
- **purpose limitation:** do not reuse workshop data or stories for publicity;
- **data minimisation:** collect only what delivery genuinely requires;
- **accuracy:** correct resource and contact records;
- **storage limitation:** set deletion and review periods; and
- **integrity and confidentiality:** restrict access and use approved storage.

The trainer should also follow the organization's lawful basis, consent, security, breach, and data-subject procedures. Consent is not the automatic lawful basis for every training record.



Harassment, threats, blocking, reporting, and evidence

When a scenario includes harassment or hate speech, the trainer should stop the harmful interaction, restate the conduct boundary, support the targeted person without forcing disclosure, and use the approved escalation route. Do not turn a person's identity or lived experience into debate material.

Blocking can stop direct contact but may remove access to content needed for a report. Where policy and safety permit, preserve the minimum necessary evidence first: the account identifier, date and time, message or URL, and brief context. Redact unrelated personal data, store evidence only in an approved location, and do not recirculate it in

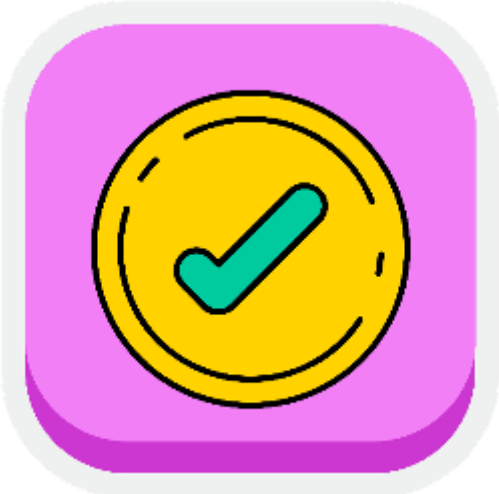
class. Platform reporting does not replace emergency, police, specialist, or organizational safeguarding routes where those are required.



Story and image consent

A useful story is not automatically safe to publish. Consent for a story, photo, quote, or recording must be freely given, specific, informed, understandable, and capable of being withdrawn for future use. Refusal must have no effect on access to the workshop or support. Explain the audience, channel, editing, retention, and limits of withdrawal after publication.

Anonymization may fail when a place, image, role, family detail, or rare experience identifies a person. Prefer fictional or composite examples. Never use a disclosure as a success story.



Volunteer due diligence and exploitation

Before recommending a volunteer route, validate:

- the organizer's legal or recognized community identity and named contact;
- the role, hours, location, supervision, induction, and right to stop;
- accessibility, safeguarding, complaints, insurance, and health-and-safety arrangements;
- reimbursement, equipment, training, and any genuine costs;
- what personal data or checks are required, by whom, at what stage, and why; and
- whether local rules affect the role, especially regulated work or immigration conditions. Refer legal questions to a competent official or specialist service.

Warning signs include a fee to secure a place, requests for passports or banking credentials by direct message, vague duties, unpaid substitution for a normal job, excessive or changing hours, isolated accommodation or transport, pressure to recruit others, withholding documents, threats, sexualized expectations, and no safe way to leave or complain.

Do not confront a suspected exploiter during training. Preserve minimal evidence if safe, stop the referral, and use the approved safeguarding, labour-rights, anti-trafficking, police, or specialist route according to the situation and local protocol.



Fake grants and financial opportunities

Treat unsolicited grants, prizes, hardship funds, and investment-style community schemes as high consequence. Verify the programme on the named funder's own domain and through an independently published contact. A legitimate logo, testimonial, or sponsored placement is not enough. Do not pay a release or processing fee, share credentials, or send identity documents through an unverified message channel.



Crisis alerts

Before delivery, identify the official alert channels, emergency number, accessible alert alternatives, and local-language routes for each delivery location. For an alert, check:

- issuing authority and original channel;
- exact location, date, time, time zone, and affected period;
- required action and whether an update or all-clear supersedes it; and
- an accessible fallback such as official radio, SMS, telephone, or a staffed public point.

Do not ask people to post their location, route, health status, or household details. Do not use crowd reactions as confirmation. If there is immediate danger, prioritize the authorized emergency instruction and emergency services over teaching the verification method.



Safeguarding and referrals

The trainer must know the organization's safeguarding lead, immediate-danger procedure, mandatory-reporting duties, confidential recording system, and current specialist referrals before delivery.

If a concern or disclosure arises:

1. listen calmly and do not investigate or ask for a detailed account;
2. explain the limits of confidentiality and the next required step;
3. check immediate safety without requesting unnecessary case details in the group;
4. involve the designated safeguarding lead and emergency services where the protocol requires;
5. seek the person's informed involvement in a referral where safe and legally possible;
6. record only necessary facts in the approved system; and
7. do not promise confidentiality, eligibility, a service outcome, or personal follow-up outside the trainer's role.

Keep a verified, discreet route for domestic abuse, sexual violence, trafficking, hate crime, labour exploitation, child and adult safeguarding, legal advice, and urgent mental-health support where relevant. A resource list is not a referral protocol; trainers need role boundaries and a named escalation route.



5. Non-sensitive needs analysis

Conduct needs analysis to adapt delivery, not to identify or document personal cases. Explain that responses are optional, may be skipped, and do not affect access.

Collect only planning information such as:

- preferred workshop and support languages;
- broad familiarity with phone, browser, search, and messaging interfaces;
- device sharing, data cost, connectivity, and offline access in aggregate;
- preferred visual, audio, print, large-text, caption, or assistive-technology formats;
- whether examples should focus broadly on services, public notices, news, initiatives, or volunteering; and
- practical timing, breaks, childcare-access arrangements, and anonymous accessibility requests.

Do not ask why a person needs a service, their status, address, diagnosis, case history, experience of abuse, political belief, or membership of a community group. Avoid linking individual names to digital-confidence or support responses. Use anonymous counts, private optional contact with an authorized support role, and a clear deletion date.

Translate the delivery design from the findings:

- reduce platforms and steps when digital familiarity or data access is low;
- provide screenshots and printed source packs when accounts or connectivity are barriers;
- plan qualified language support rather than relying on participants;
- separate general information from private referral pathways; and
- retain multiple ways to observe, speak, point, annotate, or pause.



6. Guided source-evaluation practice

Purpose and output

Review a small set of prepared sources without browsing through a participant account or submitting personal details.

For each candidate source, consider:

- resource title, information type, URL, and offline address or telephone route;
- responsible organization, owner, sponsor, and contact;
- editorial standards, corrections route, or group moderation rules where relevant;
- geographic scope, audience, eligibility, cost, and account requirement;
- languages, reading demand, mobile behaviour, accessibility features, and print option;
- publication or update date for the item being used;
- personal data requested and privacy notice;
- S-D-P-C findings and independent corroboration;
- known limitation or risk;
- date checked and current status; and
- safe replacement route if the resource becomes unavailable.

Practice method - 40 minutes

1. **Select - 5 minutes:** choose three candidates: one responsible official source, one recognized community or journalistic source, and one offline or human-help route.
2. **Inspect - 10 minutes:** inspect ownership, purpose, dates, sponsorship, language, accessibility, contact, data requests, and corrections or moderation.
3. **Triangulate - 10 minutes:** trace one important claim to its origin and compare it with at least one genuinely independent source.
4. **Test access - 5 minutes:** test on a narrow mobile viewport and check whether the key information remains usable without an account, high bandwidth, audio, colour alone, or a pointer device.
5. **Record and decide - 5 minutes:** label each candidate `suitable for the example`, `conditional - explain limitation`, or `do not use`.
6. **Challenge assumptions - 5 minutes:** question the authority, independence, privacy, and fallback assumptions, and revise any unsupported conclusion.

Evaluation is specific to a claim, audience, and date. It is not a permanent endorsement of an organization or platform.



7. Inclusive facilitation design

Mobile and low-bandwidth

- Demonstrate one short route at a time on a phone-sized view.
- Use stable public URLs and prepared screenshots with visible publisher and date.
- Avoid QR-only access, app installation, account creation, autoplay, and large downloads.
- Provide a low-bandwidth document and a telephone, desk, library, or community-centre alternative.
- Allow shared-device observation without exposing browser history, notifications, or accounts.

Visual and accessible

- Apply WCAG 2.2 principles: perceivable content, operable controls, understandable instructions, and robust formats.
- Use meaningful headings, descriptive links, readable spacing, strong contrast, captions, transcripts, and text alternatives.
- Do not rely on colour, icons, screenshots, audio, or fine motor control alone.
- Describe the evidence visible in an image and provide the original text source where possible.
- Keep printed layouts linear, uncluttered, and legible in grayscale.

Multilingual, literacy-aware, and LASLLIAM-aligned

- Pre-teach a small set of functional terms such as `source`, `date`, `official`, `sponsored`, `report`, and `block` in relevant languages.
- Pair plain language with the official label or organization name shown in the source.
- Read critical text aloud without putting a participant on the spot.

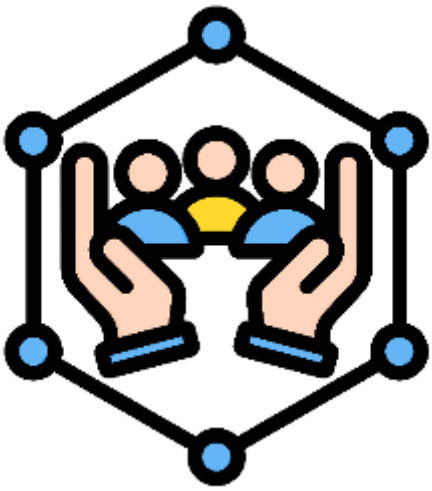
- Use modelling, repeated routines, images with text alternatives, and oral or pointing options.
- Check concepts rather than accent, spelling, speed, or recall of specialist vocabulary.
- Do not assume literacy in a first language or familiarity with Latin script.

Print and offline

- Print dated source extracts with the URL, publisher, and `training copy` label.
- Include a blank field where the trainer can write a current telephone or staffed access route.
- Never imply that a printout remains current indefinitely; add `checked on` and `check again by` dates.
- Prepare an offline facilitation version that can run without search, log-in, video, or personal devices.

Psychologically safe discussion

- State that no one must disclose a personal need, harmful message, migration experience, or group membership.
- Use fictional and composite scenarios; allow pass, pause, observation, or private support routes.
- Discuss why a claim is unsupported, not why a person was foolish to believe it.
- Interrupt stereotypes, hate speech, victim blaming, and demands that a targeted person educate the group.
- Avoid asking for consensus on a person's rights, safety, or identity.
- Close uncertainty with a safe next step rather than pressure to decide publicly.



8. Facilitation troubleshooting

A live page has changed or disappeared

Stop the demonstration. Use the dated training copy, identify the change as a maintenance issue, and model the fallback source. Do not improvise a new recommendation without validation.

Search results differ across devices or languages

Use the difference to explain personalization, location, language, and sponsored ranking. Return to a known responsible domain and compare claims, not result positions.

Two credible sources disagree

Compare publication and effective dates, jurisdiction, definitions, and proximity to the original decision. Contact the responsible body through a published route if action depends on the answer. State unresolved uncertainty.

Translation is uncertain

Do not guess a consequential term. Mark it for checking, use the original text, and consult an approved competent language route. Machine translation may support orientation but not settle high-consequence meaning.

A real disclosure replaces the fictional discussion

Pause the activity, do not gather details in the group, restate confidentiality limits, and activate the approved safeguarding or referral process.

A hostile or hateful contribution occurs

Interrupt it, name the breached boundary, support the person targeted, preserve evidence only if required, and decide whether a safe continuation is possible. Do not convert hate speech into an open debate.

Connectivity fails

Move to the printed comparison and offline contact map. The verification reasoning, not successful browsing, is the instructional priority.



9. Model workshop for trainer analysis

This 90-minute example applies the module's classification, verification, privacy, safety, and inclusion principles.

Model purpose

The trainer models how to classify a local information item, verify a current local-news claim, and select a safe action without using personal accounts or disclosing private circumstances.

Prepared materials

- one fictional viral post about a local service or policy;
- one current original notice from the responsible body, captured and dated for training;
- one independent local-news or recognized community explanation;
- one redacted messaging screenshot showing a privacy or scam warning sign;
- S-D-P-C cards or a one-page sheet;
- an offline contact route and safeguarding route; and
- accessible phone-size, large-text, translated-keyword, and print versions.

Facilitation sequence

0-10 minutes - Boundary and information map

The trainer states the no-disclosure and no-real-account boundaries, introduces the eight information types, and places the prepared example inside Module 5 rather than event-planning work from Module 4.

10-25 minutes - Taxonomy exemplar

Workshop participants sort prepared fictional cards by information type and may pass or observe. The trainer asks for evidence in the card, not personal experience, and clarifies ambiguous combinations such as an initiative advertising an event.

25-45 minutes - S-D-P-C demonstration

The trainer models a phone-first trace from the viral post to the original current notice. Think-aloud language distinguishes the sharing channel from the source and the top search result from evidence.

45-65 minutes - Source-comparison exemplar

Pairs compare the prepared official and independent sources. They annotate agreement, difference, missing evidence, sponsorship, update date, and the safest source for the specific action. No browsing, joining, or messaging is required.

65-80 minutes - Safe-action exemplar

Small groups choose a response to a fictional message: pause, verify, use an offline contact, block, report, preserve minimal evidence, or refer. The trainer corrects a planted rumour with non-shaming language and keeps safeguarding decisions within role boundaries.

80-90 minutes - Consolidation and routes

The trainer restates the verification routine, names current offline and urgent-help routes, and collects only anonymous feedback about access to the workshop format.

Trainer analysis prompts

- Where does the sequence distinguish source, channel, ownership, editorial process, moderation, and sponsorship?
- Is each example necessary, current, relevant, and safe to display?
- Where could a prompt invite personal disclosure, and how will the trainer rewrite it?
- Which step could fail on a shared phone, in low bandwidth, in print, or across languages?
- Does the correction protect dignity while making the accurate action unmistakable?
- Are the offline, crisis, harassment, and safeguarding routes current and role-appropriate?
- What should be shortened or extended for a facilitated group without crossing into Module 4?



10. Trainer quiz

1. A viral post says a local residency-related policy changes tomorrow, but it links only to another social post. What should the trainer do before using it in a workshop?

- A. Include it with a prominent `unverified` label so the group can decide whether it sounds credible.
- B. Pause use, trace the claim to the responsible authority's current dated publication, and seek independent corroboration appropriate to the consequence.
- C. Use it as a ranking example because the trainer is not personally advising anyone to act.
- D. Replace it with a highly shared news summary that gives the same date.

2. An official service notice and a recognized community summary give different start dates. The summary is clearer and translated. What is the best trainer decision?

- A. Prefer the summary because accessible language is the strongest indicator of practical reliability.
- B. Present both dates without choosing, because disagreement proves that neither can guide action.
- C. Combine the clearest parts of both items into one simplified date statement.
- D. Check jurisdiction, publication and effective dates on the responsible body's current notice, contact it if needed, and use the community source for independent context rather than authority it does not hold.

3. During a facilitated exemplar, a peer repeats a false rumour that was shared to help the community. How should the trainer respond?

- A. Acknowledge the concern or helpful intent, state the verified correction without exposing the sharer, and provide a concrete safe route before further sharing.
- B. Ask the peer to explain publicly why the source was trusted, then let the group identify the mistake.
- C. Avoid correction during the session and send the accurate link privately afterward to preserve comfort.
- D. Repeat the rumour in full, label every false part, and name the account that circulated it.

4. A sponsored post offers a new community grant but requires a processing fee and passport image by direct message. What should the trainer model?

- A. Contact the advertiser by direct message without attachments and judge the response before deciding.
- B. Ask the stated sponsor whether the fee can be paid only after approval.
- C. Do not engage or send data; verify the grant on the funder's own domain and independent contact, preserve minimal evidence if safe, and use the appropriate fraud or support route.

- D. Share a redacted version in a large local group to gather community experience before reporting it.

5. A trainer wants to demonstrate privacy in a private messaging group. Which design is best?

- A. Create a temporary real group with minimal profiles and delete it immediately after the demonstration.
- B. Use fictional, redacted screenshots without joining or messaging; explain that private is not confidential and model data minimisation, evidence, block, and report options.
- C. Ask a trusted moderator to show the group from their account while hiding the member list.
- D. Let trainers use new accounts so their established profiles and contacts are not exposed.

6. A local newsletter asks the trainer for a participant success story and photo after a workshop. What is the best decision?

- A. Provide an anonymized story and cropped photo because removal of the name makes new consent unnecessary.
- B. Ask for general verbal consent in front of the group and omit sensitive details.
- C. Reuse the workshop registration consent if the newsletter promotes the same programme.
- D. Decline unless there is freely given, specific, informed, understandable, and revocable consent with no service consequence, and use only the minimum safe data.

7. Which source-review note best supports later checking?

- A. Resource name, category, homepage URL, and a note that it appeared active during the last check.
- B. Resource name, search rank, follower count, star rating, and the most recent positive comment.
- C. Owner and contact, scope, language and accessibility, data and account requirements, sponsorship, offline route, evidence checked, known limitation, reviewer, last-checked date, and next review date.
- D. A screenshot, translated summary, general trust label, and the name of the trainer who recommended it.

8. A workshop discussion includes hostile hate speech aimed at a represented community. What should the trainer do first and next?

- A. Interrupt the speech, name the conduct boundary, support those targeted, preserve or report minimal evidence under procedure, and decide whether safe continuation or referral is appropriate.
- B. Allow a short evidence-based debate so inaccurate stereotypes can be corrected by the group.

- C. Invite someone from the targeted community to explain the impact before deciding whether to stop the discussion.
- D. Remove the visible comment, remind everyone to be respectful, and continue the planned activity without further attention.

9. A highly shared local post conflicts with a current original notice. Which explanation should the trainer model?

- A. Widespread sharing is useful community corroboration when no financial sponsor is visible.
- B. The safest estimate is the detail on which the popular post and official notice most nearly agree.
- C. Ranking systems usually move corrected information upward, so the trainer should wait for search order to stabilize.
- D. Popularity and ranking measure distribution or engagement, not truth; verify the original current source and use genuinely independent evidence for corroboration or context.

10. A recognized organization advertises a volunteer role, but the description omits supervision, complaint routes, costs, and the right to stop. What should the trainer do?

- A. Recommend it because the organizer's recognized status makes the missing details low risk.
- B. Pause the recommendation and verify the missing role, safeguarding, cost, complaint, and withdrawal details through the organization's official contact.
- C. Ask interested participants to join first and report whether the role is well managed.
- D. Treat the opportunity as suitable if it does not request a fee or identity document.

References

1. Redecker, C. (2017). *European Framework for the Digital Competence of Educators: DigCompEdu*. Punie, Y. (Ed.). Publications Office of the European Union, EUR 28775 EN. https://doi.org/10.2760/159770. Relevant areas include digital resources, teaching and learning, assessment, empowering learners, and facilitating digital competence.
2. Vuorikari, R., Kluzer, S., and Punie, Y. (2022). *DigComp 2.2: The Digital Competence Framework for Citizens - With new examples of knowledge, skills and attitudes*. Publications Office of the European Union, EUR 31006 EN, JRC128415. https://doi.org/10.2760/115376. Relevant areas include information and data literacy, communication, safety, and problem solving.
3. European Union. (2016). *Regulation (EU) 2016/679 (General Data Protection Regulation)*, especially Article 5 principles relating to personal-data processing. https://eur-lex.europa.eu/eli/reg/2016/679/oj. Trainers must also follow applicable national law and organizational policy.
4. UNESCO. (2021). *Media and Information Literate Citizens: Think Critically, Click Wisely! Media and Information Literacy Curriculum for Educators and Learners*. UNESCO. https://unesdoc.unesco.org/ark:/48223/pf0000377068.
5. World Wide Web Consortium. (2023). *Web Content Accessibility Guidelines (WCAG) 2.2*, W3C Recommendation. https://www.w3.org/TR/WCAG22/.
6. Minuz, F., Kurvers, J., Schramm, K., Rocca, L., and Naeb, R. (2022). *Literacy and Second Language Learning for the Linguistic Integration of Adult Migrants (LASLLIAM): Reference Guide*. Council of Europe. https://www.coe.int/en/web/language-policy/laslliam.

Link Up

MAP MÜNCHENER AKADEMIKER PLATTFORM

Edu Change Network

FDI Future Development Initiative

BALKAN BRIDGE

netwerkpro
Waar vrouwen de toekomst vormen

Co-funded by the European Union

2025-1-DE02-KA220-ADU-000350564