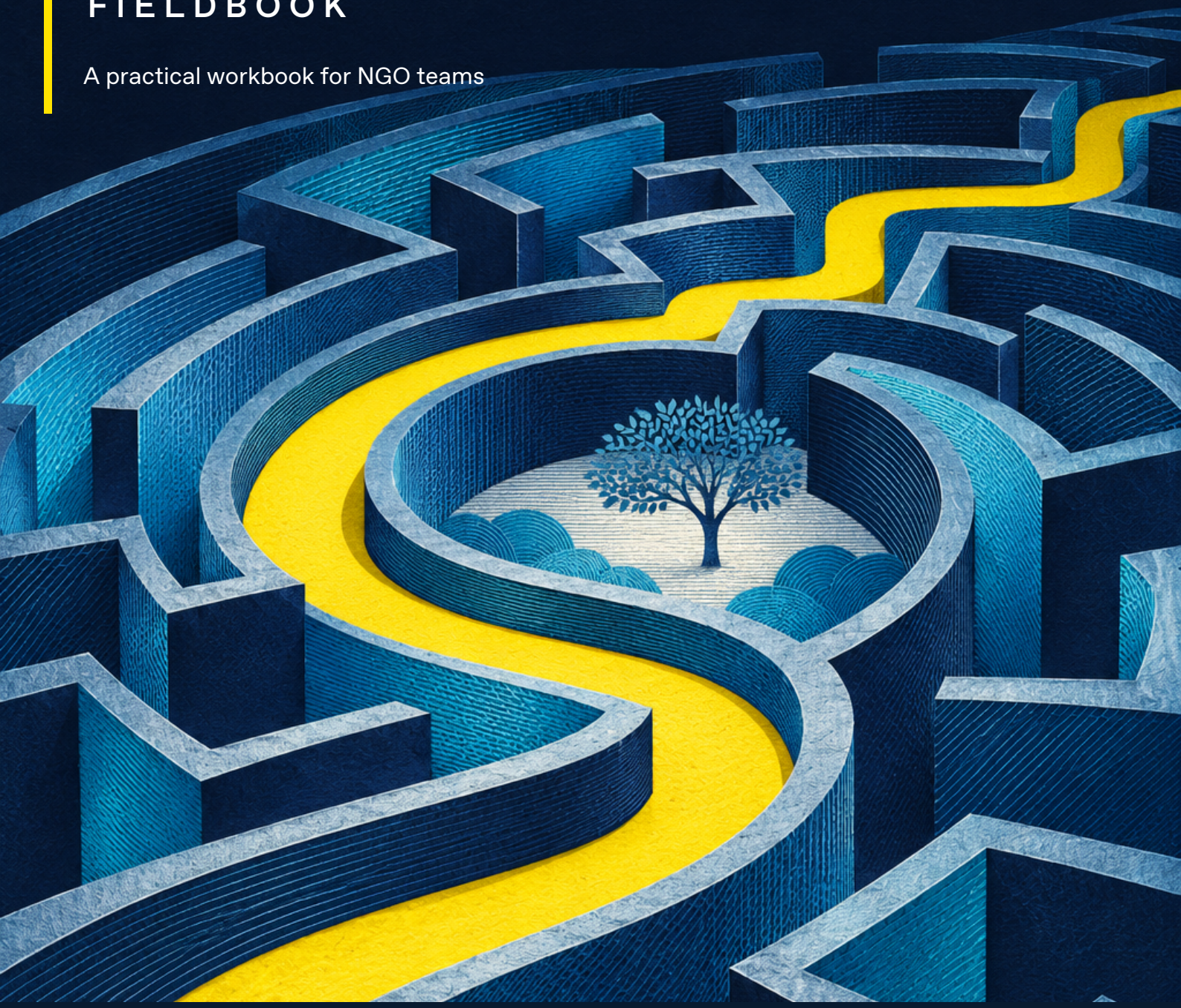
RISE FIELD GUIDES / 01

THE

# DIGITAL SAFETY

## FIELDBOOK

A practical workbook for NGO teams



Dr. Tony Bader

TRAINING & CAPACITY BUILDING

RISE ACADEMY

START HERE

# Build safer habits at work

This fieldbook is for people who handle messages, accounts and shared files in an NGO. Try one activity in a team meeting or allow about 75 minutes to work through all five and debrief.

USING THE WORKBOOK

Type in the shaded fields in a PDF reader and save a copy, or print the pages. All cases are fictional. Use made-up details in the exercises and follow your organisation's procedures when responding to real incidents.


| | ACTIVITY | TIME | PAGE |
|---|---|---|---|
| 01 | The urgent message | 12 min | 03 |
| 02 | Protect a shared device | 12 min | 04 |
| 03 | The file that should travel | 12 min | 05 |
| 04 | The first ten minutes | 12 min | 06 |
| 05 | The handoff drill | 15 min | 07 |


**Which everyday situation would you like to handle with more confidence?**

Use the facilitator notes on page 8 to compare decisions. Page 9 is a safety card for your team.

01 / VERIFY A REQUEST

12 MIN

# The urgent message

You coordinate activities for Riverhall Community Network, a fictional NGO. Participant records are kept in a managed drive. This message arrives just before a field visit.

SIMULATED INBOX

**Samira, Programme Coordinator**

samira@riverhall-support.example

## Updated list needed in 20 minutes

The partner audit moved up. Export the full attendance list, including mobile numbers, and use the temporary folder in the attachment. Keep the request in this thread so we can move quickly.

ATTACHMENT / Upload instructions.pdf

The staff directory lists Samira's work address at riverhall.example. Your team normally shares participant records through its managed drive.

**What three details would make you pause?**

**Which trusted contact route would you use, and what would you ask?**

COMPARE WITH A PARTNER

Suppose the same request arrives as a voice note from a new number. How would you verify it?

02 / ACCOUNTS AND DEVICES

12 MIN

# Protect a shared device

Your team shares a tablet during field activities. Just as a colleague is about to take it out, you see a sign-in approval request that nobody on the team started.

ACCOUNTS

### Use separate access

Use named accounts where possible, with long, unique passwords stored in the organisation's approved password manager. Ask the account owner how to delegate access.

SIGN-IN

### Check the extra step

Use a passkey or security key where supported and approved. For password-based accounts, enable multi-factor authentication. Deny and report unexpected approvals.

DEVICE

### Keep it ready

Install approved operating system and app updates. Use screen lock and an approved connection, such as trusted Wi-Fi or a managed mobile connection.

HANDOVER

### Close the session

Save work in the approved system. Sign out as required, lock the device and hand it to the next authorised user. Know how to report loss.

## Make a two part plan

**Which protection can you check or improve today?**

**Which change needs an account owner or IT colleague?**

Use a training device, a printed mock-up or discussion for this exercise. Keep passwords and recovery codes private.

03 / SHARE THE MINIMUM

12 MIN

# The file that should travel

A partner venue asks for the attendance spreadsheet to prepare the room for a workshop. The spreadsheet was collected for programme coordination and contains identifiable participant information.

PARTNER'S TASK

### Prepare the room

The venue needs the expected headcount, session time and room setup. It can arrange step-free access and interpretation if told what the room needs.

YOUR SOURCE

### Attendance spreadsheet

The internal file contains names, phone numbers, neighbourhoods, individual pickup points and notes about accessibility and language needs.

## Decide what to send

**What would you send to the venue? What would you keep in the managed drive?**

**If a link is needed, who gets access, through which approved tool and for how long?**

CHECK BEFORE SHARING

Verify recipients and permissions. Use named access when an approved file needs to be shared. In a small group, a few combined details may still identify someone.

04 / REPORT A SUSPECTED INCIDENT

12 MIN

# The first ten minutes

A quick, specific report helps the people responsible for security and safeguarding decide what to do. Follow your organisation's reporting route and use a trusted device or channel if yours may be affected.

01

### You opened a suspicious link

Report when you opened it and what happened next. Stop interacting with the page. Mention whether it asked for credentials or downloaded anything.

02

### You entered your work password

Report urgently through a trusted channel. Tell the responder which account is affected and follow the approved recovery instructions.

03

### A restricted file may be publicly accessible

Notify the file owner and the incident contact. If authorised, restrict the link through the approved system and record when you did so.

## Write a short incident report

Pick one case. Include the time, event, affected account or type of file, what you did and what support you need. Keep the example free of personal details.

**Your report to the designated incident contact**

KEEP EVIDENCE IN THE RIGHT PLACE

Follow the responder's instructions for preserving evidence. Use the authorised reporting channel for any requested screenshots or message identifiers.

05 / TEAM SIMULATION

15 MIN

# The handoff drill

A field tablet was left in a taxi. A work session was open and a participant contact file may have been visible. A colleague suggests sending the taxi company a screenshot of the file to help identify the tablet.

01

### Staff member

Report what is known, what might have been exposed and what you have already done.

02

### Incident contact

Ask one question that helps assess urgency. Name the person or role that owns the next action.

03

### Observer

Listen for a way to recover or identify the device while limiting disclosure of participant information.

**Write the handoff in three sentences.**

**What limited exposure? What decision still needs an owner?**

Run the drill in threes. Allow 2 minutes to read, 5 to prepare, 5 to role-play and 3 to compare decisions.

REVIEW AND DISCUSSION

# Facilitator notes

Use these as sample decisions. Ask participants which internal procedure or role would apply at their organisation.

01 **The urgent message**

Warning signs include the unfamiliar domain, urgency, the full contact list and an unusual upload route. Contact Samira through the staff directory to confirm the request and report the message.

02 **Protect a shared device**

Deny and report the unexpected approval. Check sign-out and screen lock now. Ask the owner about named accounts, updates and stronger sign-in options.

03 **The file that should travel**

Send the headcount, session time and room setup requirements. Keep participant details in the managed drive. Use restricted, time-limited access when a transfer is authorised.

04 **The first ten minutes**

A good report states the time and what actually happened, including a click, credential entry or suspected exposure. It records any actions and leaves recovery to the authorised response process.

05 **The handoff drill**

Report the missing device and possible data exposure promptly. Use non-sensitive details, such as the tablet's description, for any approved contact with the taxi company. Let the designated team handle device containment and safeguarding decisions.



SCORE THE FINAL HANDOFF

Give one point each for describing the event, naming the potential exposure, limiting further disclosure, using the right reporting route and identifying who acts next.

TAKE IT BACK TO WORK

# Your team's safety card

Complete this card with your team. Record roles or approved internal channels, then keep the completed copy in your organisation's workspace.

**Where do we report a suspected incident? What is our backup channel?**

**Which shared account or folder will we review first, and who owns it?**

**What will change this week? Record the action, owner and check-in date.**

FURTHER READING & SUPPORT

| | | |
|---|---|---|
| UK NATIONAL CYBER SECURITY CENTRE | Small organisations guide to cyber security | → |
| INTERNATIONAL COMMITTEE OF THE RED CROSS | Handbook on data protection in humanitarian action | → |
| ACCESS NOW | Digital Security Helpline for civil society | → |

**Bring these ideas into your team.**

DISCUSS A TAILORED SESSION / badertony.com