



INFORMATION SECURITY POLICY

This policy outlines the rules and expectations for staff, volunteers and partners handling, storage, sharing of data and information when working in relation to Engineers Without Borders Denmark (EWB).

1. General Considerations

When working on humanitarian projects, volunteers handle sensitive information that, if exposed, can pose risks to individuals and operations.

EWB uses third party platforms for information and data storage and handling.

Data may be stored and handled on these platforms, locally on a personal computer if the data is protected by password (such as a user login). Data may be handled on an AI platform if it adheres to the AI guidelines below.

Data may not be stored outside of the above locations.

Follow the below principles for safe information and data handling and storage:

The principle of least privilege: Only access and share information necessary for your task – ask the project lead who is involved- if in doubt = check. Only give access to those who are directly involved in the project and who needs to know.

Use secure communication channels: Use end-to-end encrypted messaging apps and verified organizational tools over personal accounts or public platforms.

In group chats, the admin must clarify how the content in the chat can be used. I.e. strictly for internal use, or free to share online.

The admin must also use the tools of the app to restrict user permissions according to the project or mission considerations.

Avoid public Wi-Fi: If necessary, always use a VPN when accessing organizational systems or handling sensitive data.

EWB-DK can provide tools for internet access on missions. If using a public Wi-Fi, always use a VPN, even if the Wi-Fi is password protected.

Be mindful of metadata: Photos, documents, and files may contain embedded location or identifying information. Remove metadata before sharing.

In most of EWB-DK working locations meta-data is not a problem, but in certain areas it can be. This is briefed during mission preparation.

Report security incidents: If you suspect a data breach or unauthorized access, inform the secretariat at info@iug.dk or +45 44 40 28 28 immediately. Report using the 5WH



format: Who, What, When, Where, Why, How.

2. AI Use and Security

AI tools like ChatGPT, Copilot, and others can be helpful for general tasks but must be used responsibly.

If you are unsure whether an AI tool is safe for a specific task, consult the secretariat. When handling sensitive information, prioritize human verification and secure channels over AI automation.

Safe AI Use Practices

- *Do not share sensitive data:* Never input names, exact locations, personal details, or confidential information into AI systems without consent of the people and organizations in question.
- *Use AI for general assistance only:* AI should be limited to drafting, summarizing open-source information, or language translation—do not use it for decision-making on sensitive matters.
- *Verify all AI-generated content:* AI can produce misleading or incorrect results; always fact-check and cross-reference information.
- *Prefer AI models that comply with EU and Danish regulations:* These have stronger data protection policies and are less likely to misuse or store sensitive information.

AI Tools to Use and Avoid

- *Approved AI tools:*
 - OpenAI's ChatGPT
 - Microsoft's Copilot
 - Anthropic's Claude
- *Do not use AI tools that lack transparency or store user inputs:*
 - DeepSeek, Grok and similar models with unclear data policies
 - Public chatbots that retain and use inputted data for training
 - Any AI hosted on platforms outside EU regulatory oversight

3. Additional Precautions for Risk Areas

Volunteers working in conflict zones or politically sensitive regions should take extra care when using AI and handling data.

Do not use AI for operational security: Do not use AI to generate, store, or analyze information related to humanitarian response planning, safe zones, supply routes, or personnel movements.

Use air-gapped systems where needed: If AI assistance is required, ensure it is run in a secure offline environment.



ENGINEERS
WITHOUT BORDERS **DK**

Limit digital footprints: Be cautious when searching, communicating, or sharing information online—use encryption and VPNs when necessary.

4. Sharing and Social Media

Always get approval from all people and organizations involved before sharing information with others and on social media.

Do not share specifics of future plans, such as locations, timings etc.

Do share purpose, general area, partner, and so on.

Consult with the EWB-DK Communications Team to clarify.

Ensure consent from partners and beneficiaries before sharing photos or information of them online.

Approved by

Lasse Oszadlik
Mission Manager