

Terms and Conditions for using UNICEF Data Systems by Volunteers

As a volunteer who is granted access to UNICEF data systems (such as UNICEF TeamPass, AG Intranet, GK-Net, UNICEF Campus, etc.), you must adhere to specific rules.

Not everyone is permitted access to these systems because they contain confidential and personal information.

Access is determined by responsible administrators or group leaders, who decide who can use the systems and what specific functions are available to each user. These administrators verify new volunteers, review their UNICEF group accounts to ensure that all necessary consents are obtained and that a valid extended certificate of good conduct is on file. They also handle account updates, profile assignments, and can deactivate accounts if needed.

As a user, you have the ability to create your own account, update your information, and delete your account when necessary.

What should you keep in mind?

To access and use our systems, you must be familiar with, accept, and comply with the following Terms of Use, especially regarding data protection requirements:

1. Data Protection - What is it?

Data protection refers to the safeguarding of an individual's personal information. The primary aim is to protect the fundamental right to informational self-determination, which is the right to control how one's own data is used.

Personal Data includes e.g., an individual's name, address, date of birth, telephone number, occupation, hobbies, photographs and video recordings. Such data may only be processed if there is a distinct purpose for such processing, e.g., to organize and carry out your voluntary service.

2. Data Secrecy – Your personal obligation

Data Secrecy means: You are **not allowed to disclose** any personal data you encounter during your volunteer service **with external parties without authorization or use this data for any other purposes**. This obligation continues even **after your voluntary service ends**.

3. Confidentiality – Handling of sensitive information

Confidentiality refers to: All internal information – including non-personal data (such as organizational processes and plans, meeting content or minutes, campaign and promotional concepts, statistics, and analyses, and similar information) – must be **kept secure and safeguarded**. Access to this information is restricted to authorized individuals only.

External Digital Communication Systems

Additionally, various digital communication systems are utilized for interaction between UNICEF and volunteers, as well as among the volunteers themselves. Please note that UNICEF does not have administrative access to these systems.

The obligations outlined above pertaining to data protection, data secrecy, and confidentiality also apply to these systems.

Such systems include, but are not limited to:

- **WhatsApp** (Meta):

A communication channel for young people, college student groups, and work teams to connect with one another and UNICEF staff through individual or group chats.

- **Facebook & Instagram** (Meta):

Communication channels for public relations activities maintained by volunteers.

- **Hochschulgruppen (college student groups) Instagram Fanpage** (Meta):

A page supported by UNICEF for college student groups.

- **CoreMedia:**

Program used by UNICEF for managing UNICEF groups' websites. UNICEF offers training on the use of this platform.

- **Zoom**

This platform is used for participating in UNICEF webinars and digital networking meetings among volunteers, both within their group and cross-regionally.

- **Various email programs** (for example, MS Office, MS 365, Thunderbird or other providers)

Your Consent – What you are confirming

By accepting these Terms and Conditions, you confirm the following:

- You will treat all internal information **as confidential at all times**.
- You agree **not to disclose any personal data of other volunteers, full-time UNICEF employees, donors, greeting card purchasers, or any other individuals associated with UNICEF** to external third parties. You will use such data **solely for purposes related to your volunteer service**.
- You comply with all applicable legal **data protection requirements** (such as the General Data Protection Regulation (GDPR) and the German Federal Data Protection Act (BDSG)).
- You are fully aware that violations of these laws may lead to **legal ramifications**.
- You securely store **data carriers and printouts**, such as in a locked cabinet.
- You **never share your passwords and keep your access data confidential**.
- You dispose of data that is no longer needed **securely and permanently**. Such data includes printouts, data carriers, emails, files, and contact information.
- You take measures to ensure that unauthorized individuals do not gain access to confidential documents or notes.
- You report any data breaches or accidental disclosures of data to your group leader immediately.

Technical notes when using UNICEF internal systems:

- When you use the systems, your personal data will be stored.
- Your activity within the system will only be **tracked on an individual basis** if there is a specific suspicion of a rule violation.
- If such a situation arises, you will be informed **personally and without undue delay**.

Where can I find the rules?

You can refer to these Terms and Conditions anytime in the UNICEF TeamPass.

You can consent to these Terms and Conditions **online by checking the box**; no signature is required.