January 2025

Data Protection | Partner, Intervention, and Research Policy

POLICY OWNER:	Insights Department
POLICY APPROVED BY:	Global Director, Insights
POLICY CONTACT:	Senior Manager, Measurement & Impact: Maggie Goble mgoble@water.org

Policy Contents

I. Policy Overview

Policy Statement

This policy outlines the rules and expectations related to the use of program partner, intervention, and research data.

Purpose

To keep sensitive data safe and secure that is obtained through our program partnerships, interventions, and research activities.

This policy guides employees on responsible handling, collection, storage, and sharing of sensitive personal data, ensuring confidentiality, security and compliance with data protection regulations.

Applicability

It is the responsibility of every Water.org employee who handles or has access to non-public program partner, intervention, or research information to be aware of and adhere to this data protection policy.

This includes, but is not limited to, Water.org's work with financial institutions, water supply and sanitation businesses, sector stakeholders, capital providers, WaterEquity, WaterConnect, and 3rd parties that Water.org hires to conduct any data collection activity.

Governance

The Insights department is the owner of this policy and is responsible for administering, reviewing, and making recommendations for updates or changes to this policy in alignment with business needs.

Violations

It is the expectation of Water.org that direct supervisors proactively manage their direct reports' compliance with this Policy. Non-compliance, from an employee or a direct supervisor, may result in progressive disciplinary actions consistent with the organization's established HR procedures.

II. Policy

At Water.org, we are committed to protecting sensitive information entrusted to us through our partnerships and research engagements. We recognize the importance of maintaining confidentiality and integrity of all data in our possession.

Through our program partnerships, interventions, and research activities, Water.org conducts a variety of activities that collect non-public and sensitive information about organizations and individuals.

- Examples of organizations include Water.org partners, capital investors, businesses/enterprises, and governments.
- Examples of individuals include: a person that could be a household borrower, a beneficiary, an e-Learning learner, self-help group member, and an employee.

Types of **sensitive data** include, but are not limited to the following:

- Organization: business plan, investments, loan portfolio, performance, and finances
- Individuals: personal identifiers such as names, addresses, GPS location, phone numbers, socio-economic and health information, and personal opinions.

Sensitive data that Water.org collects must be safely collected, stored, and accessed. Mishandling of this data and/or data breaches could reveal our partners' proprietary information and impact individuals' access to financial services and jeopardize their well-being. It also leaves Water.org vulnerable to reputational risk and legal repercussions.

The number of people involved in the collection, data transfer and storage of sensitive data should be limited as much as possible.

1. Requirements for handling sensitive data

Data collection preparation

- Agreements must be in place with partners and contractors before sensitive data is collected or handled through any Water.org activity.
    - Unless otherwise approved by Legal, always use the Water.org contract templates that obligate data confidentiality and security.
- When Water.org staff are directly collecting sensitive data, that person and their supervisor must plan to use all approved methods as outlined in this policy.
- New areas of research that involve surveying individuals must be checked with the policy owner in advance of the study to determine whether Institution Review Board (IRB) approval is required. This ensures that it's conducted ethically and in compliance with regulations.

Data collection

Sensitive data about an organization or individual should only be collected in the following approved tools and applications that are outlined in the table below. Any deviation from this table must be approved by the policy contact.

Tools and applications	Organizational data	Individual data
Water.org's **Microsoft email and SharePoint** systems that are password protected, and use multifactor authentication	Approved for use	Not approved for use
WaterPortal that is password protected through Water.org security systems	Approved for use	Approved for use

mWater that is password protected. If you collect sensitive data on your mobile device through the mWater app, it must be on a password protected device. The survey(s) must be uploaded to mWater and removed from your phone as soon as you have connection to the internet.	Approved for use, following removal protocol from devices	Approved for use, following removal protocol from devices
A **contracted third party's** data collection platform, in which the 3rd party has an agreement in place with Water.org and has a secure data collection system with a data privacy protocol in place.	Approved for use	Approved for use
Water.org's **eLearning platform**. The platform is password protected and allows access only to those who have been granted permission.	Approved for use	Approved for use
Paper: In rare cases, sensitive data may be collected through paper surveys or notes.	Approved for use per safe storage and destruction	Not approved for use

Data transfer and storage

Sensitive data must always be stored in a secure place, where only those with permission can access it.

Sensitive data about an organization or individual should only be transferred and stored in the following approved tools and applications that are outlined in the table below. Any deviation from this table must be approved by the policy contact.

Tools and applications	Organizational data	Individual data
Water.org's Microsoft email	Approved for use	Not approved for use
Water.org's SharePoint system that is password protected and utilizes multifactor authentication.	Approved for use	Limited use. SharePoint folders must be restricted to only staff and hired contractors that need access to that data. In cases where Water.org and the hired contractor need to transfer sensitive data to each other, Water.org should set up a secure folder on Sharepoint and give the approved consultant access to the folder. Contact IT support if you need help setting file permission that only allow certain people to access the file.
WaterPortal that is password protected through Water.org security systems	Approved for use	Approved for use with limited access based on user roles
mWater that is password protected	Approved for use	Approved for use with limited access based on user roles

Water.org's eLearning platform. The platform is password protected and access to individual learner data is restricted to only those who require access.	Approved for use	Approved for use
A **contracted third party's** secured files storage platform, in which the 3rd party has an agreement in place with Water.org and has a secure data collection system with a data privacy protocol in place.	Approved for use	Approved for use

Do not transfer or store individual personal information on a non-approved tool or application. Examples of unapproved tools and applications:

- **Email and email boxes.** If someone emails you a file containing sensitive organizational information or personal information, you must delete it from your inbox and request the sender to delete the file from their sent files.
- **Your desktop.** Data saved directly on your desktop will be at risk if laptop is stolen. It is more easily found and IT may not be able to remove files remotely.
- **A USB, hard drive, or other external storage devices**. Where case sensitive data is shared with you through these devices, immediately secure the device and transfer it to an approved platform as soon as possible. Once transferred, delete the files from the device.
- **Personal devices, such as a phone**. This includes your mWater app with surveys that you will not submit.

Sharing sensitive information internally and with direct stakeholders, including donors

Sensitive data with non-public information should only be shared with those who truly need it. Data for reporting and sharing should be aggregated where possible to increase the level of anonymity within the data.

If sensitive datasets need to be shared with an authorized person or firm, remove personal identifiers from the data set before sharing, unless absolutely needed.

The following table outlines what information staff can share internally and with our direct stakeholders. Any deviation from this table must be approved by the policy contact.

	Organizational data		Individual data	
Users	**Organizations are identifiable**	**Organizations are unidentifiable (aggregated)**	**Individuals are identifiable**	**Individuals are not identifiable (aggregated)**
Intervention lead	Access	Access	Access only to their intervention data in the WaterPortal, not in the mWater surveys	Access
Insights staff	Access	Access	Access restricted to platform admin and project leads	Access

All other staff and departments	Access, except for WaterPortal uploaded report on businesses	Access	No access	Access
WaterEquity and WaterConnect	Access, except for WaterPortal uploaded report on businesses	Access	No access	Access
Hired contract with contracted business need to access information	Access to contracted purpose	Access to contracted purpose	Access to contracted purpose	Access to contracted purpose
Donors with contracted agreements	Access to contracted purpose	Access to contracted purpose	No access	Access to contracted purpose
Donors without contract agreements	No access, without the organization's approval	Access	No access	Limited to publicly approved stats
Program partners with contract agreements	No access, without the organization's approval	Access	No access, except for their own WaterCredit reports submitted in WaterPortal	Access

Sharing data externally

Sensitive data must never be shared externally without informed consent from the organization or individual. The following table outlines what information can be shared externally. Any deviation from this table must be approved by the policy contact.

Data type	Able to share publicly?
Aggregated data where organizations and individuals are not identified (e.g. number of people reached, 90% of borrowers are women)	Yes
Names of Water.org partner organizations, with no other non-public details	Requires written partner permission
Public information regarding partners' finances and operations	Yes
Non-public information that identifies a partner with their finances, operations, workplans, monitoring & evaluations results, case studies, etc.	Requires written partner permission
Non-public sources of loan capital (e.g., banks that provide capital to partners and the terms on which it is provided)	Requires written capital provider and partners' permission
De-identified, raw, disaggregated client data (loan records without client name or ID)	No
Identifiable client data (loan records with client name and borrower ID)	No
Knowledge / learning / case studies products without partner identifiers and that context does not make the partner identifiable	Yes, with Insights approval

2. Artificial Intelligence Input Restrictions

Sensitive data and Artificial Intelligence (AI)

Please refer to Water.org's Artificial Intelligence Usage Policy before using any AI tool. With regards to the subject of this policy, please note the following:

- No confidential information, or other data to which Water.org has an obligation of non-disclosure or confidentiality, including but not limited to and no Water.org or third-party proprietary materials, may be inputed into an AI Tool unless otherwise approved by the Legal Department. Data input into an AI tool may not be kept confidential
- Do not input personally identifiable information including but not limited to (e.g., names, addresses, email, phone numbers, GPS info, biometric data of donors/partners/individuals/employees/other organizations/etc.), without written approval from the Legal Department.

Even where such information is removed, inputting Water.org's processes, system information and other confidential business information into an AI tool may be detrimental to Water.org. See Water.org's Artificial Intelligence Usage Policy.

III. Approval and Responsibility

Employee Responsibilities

The employee must follow the rules and expectations above to ensure sensitive data is protected and secured.

Direct Supervisor Responsibilities

The direct supervisor must check that their direct report is aware and is following this policy.

IV. Additional Resources

Related Policies

Specify procedures that support this policy, as well as other related policies.

Identity Security Policy
Computer and Technology Use Policy
Security and Incident Handling Policy and Procedure
Artificial Intelligence Usage Policy

V. Appendices

Appendix A | Examples of breaches or violation of this policy

Example	Why is this a breach
A partner's WaterPortal report is shared via an email attachment with a third party for surveys.	Email is not always secure. It is safer to share items via protected SharePoint files.
Water.org staff share household survey results with a partner where the individuals can be identified. This may include providing names, addresses, or even regional information where it is easy to figure out who the person is.	We promise survey respondents anonymity. By telling the financial institution information about individual responses, we are breaking the promise of anonymity and may put individuals and Water.org at risk.
In making the business case to a potential partner, an intervention lead shares non-public information about another partner, examples of this include their capital sources, loan distribution, and PAR details.	This is non-public information! Many of our partners are competitors and details such as capital source and PAR are private.
A hired contractor conducts a market assessment and emails multiple Water.org staff raw data that contains household information with personal identifiers.	Email is not always secured and likely has shared personal identifiers with a group of people who do not need that information. This action puts people at risk