



THE PROMISE FOUNDATION

For mental health, education and potential realisation

CONFIDENTIALITY POLICY

Policy brief & purpose

We designed our **confidentiality policy** to explain how we expect our employees, contractors, volunteers and partners to treat confidential information. In performing your role or providing a service you will unavoidably receive and handle personal and private information about clients, other employees, partners and about the Foundation. We want to make sure that this information is well-protected.

We must protect this information for two reasons. It may:

- Be legally binding (e.g. sensitive client data.)
- Constitute the backbone of our business, giving us a competitive advantage (e.g. research methods and business processes.)

Scope

This policy applies to employees, board members, grant agencies, partners, contractors, volunteers and any other person who may have access to confidential information.

Policy elements

Confidential and proprietary information is secret, valuable, expensive and/or easily replicated. Common examples of confidential information are:

- Unpublished financial information
- Data of Clients/Partners/Vendors
- Patents, formulas or new technologies
- Client lists (existing and prospective)
- Data entrusted to the Foundation by external parties
- Pricing/marketing and other undisclosed strategies
- Documents and processes explicitly marked as confidential
- Unpublished goals, forecasts and initiatives marked as confidential

There may be various levels of authorized access to confidential information.

What you should do:

- Lock or secure confidential information at all times
- Shred confidential documents when they're no longer needed
- Make sure you only view confidential information on secure devices
- Only disclose information when it's necessary and authorized

- Keep confidential documents inside the Foundation's premises, unless it's absolutely necessary to move them.
- Keep all confidential documents that are in digital format stored on the Foundation's secure server with appropriate encryption and password protection.

What you shouldn't do:

- Use confidential information for any personal benefit or profit
- Disclose confidential information unless authorised to do so by the Director, The Promise Foundation
- Replicate confidential documents and files and store them on insecure devices

When you stop working for the Foundation, or your assignment or contract with the Foundation concludes, you are obliged to return any confidential files and delete them from your personal devices.

Confidentiality Measures

We take measures to ensure that confidential information is well protected. These include:

- Expecting you to store and lock paper documents
- Encrypt electronic information and safeguard databases
- Ask you to sign non-compete and/or non-disclosure agreements (NDAs)
- Ask for authorization by your line manager or the Director, The Promise Foundation to allow you to access certain confidential information

Exceptions

Confidential information may occasionally have to be disclosed for legitimate reasons. Examples are:

- If a regulatory body requests it as part of an investigation or audit
- If the Foundation is engaging in a venture or partnership that requires disclosing confidential information (within legal boundaries)

In such cases, you should document the disclosure procedure and collect required authorizations. We are bound to avoid disclosing more information than needed.

Disciplinary Consequences

Failure to comply with the confidentiality policy may result in disciplinary and, possibly, legal action. Disciplinary action may include termination of employment, termination of contract or termination of engagement.

This policy is binding even after separation of employment, end of contract or end of volunteering engagement.

Gideon Arulmani, Director The Promise Foundation
Policy updated 25/7/2020

