THE PROMISE FOUNDATION

For mental health, education and potential realisation

RECORDS RETENTION POLICY

Policy brief & purpose
The Promise Foundation (the Foundation) Records Retention Policy describes our guidelines for creating, preserving and accession the Foundation's records. To ensure that our records are accurate and secure, we ask our employees to adhere to this policy.

Scope
This policy applies to employees, board members, contractors, volunteers and any other person who create, access and manage records.

In this policy, a "record" is any type of electronic or paper file (document, spreadsheet, database entries) that we store in our systems. This includes files that both employees and external sources create. All legal and business documents, as well as formal internal and external communications, fall under this policy's purview.

Policy elements

Creating records

We place high value on our records. By storing information, we are able to:

- Make better decisions
- Support our day-to-day operations
- Forecast and prepare for the future
- Learn from past mistakes
- Preserve and defend the Foundation's legal position
- Evaluate our operations and employee productivity over time
- Develop plans to improve and grow the Foundation

What records do employees need to create?
Creating and storing certain types of records are mandatory. Employees should keep records that:

- Are mandated by law (e.g. record keeping requirements of the Income Tax Act)
- Are necessary for them or other employees to perform their jobs
- Indicate internal or external changes that affect our operations, employees, donors, partners or clients
- Include decisions, reports, data and activities that are important to our business
- Describe business plans, communication with regulatory bodies or the public

You may keep other records if they decide they're useful to their jobs.

We have a few general guidelines for creating records. Employees should:

- Ensure that information is accurate and complete
- Store records in appropriate mediums (OneDrive, servers, hard copy)
- Name, categorize and share records properly
- Mark appropriate records as confidential
- Clarify who's authorized to access records

Authorization
Records may have different levels of authorization that limit their accessibility. The authorization level is usually determined by those who create the records, the Foundation's official policy or the law (the law always take precedence.) The following records are strictly confidential and require authorization by the Director:

All *Employment records*

- Terms of service
- Employee salary and bonus
- Employee performance review
- Employee data (date of birth, academic records, medical, etc)

Unpublished financial data

- Budgets
- Forecasts
- Estimates
- Costs projections
- Cash flow

Intellectual property

- *Tests*
- *Standards*
- *Research*

[*Client/ student/ vendor/ partner/ job applicant information and contracts*]

Access to these records are restricted to employees who directly manage the information. Other types of records, like performance metrics and internal policies, may be accessible by all permanent employees. Employees must not disclose records to people outside of the Foundation, unless authorized.

Our confidentiality and data protection policies always apply to all relevant records.

Retaining records

Our employees must protect our records, whether marked as confidential or not.

Physical records

Printed records must be stored safely in filing cabinets or closed offices. Important, confidential files must not be left in open office areas.

When employees need to carry physical records out of our offices, they must prevent them from being damaged, lost or stolen. We advise our employees to avoid relocating records as much as possible.

Electronic records

Electronic records will be protected by passwords, firewalls and other security settings. Employees are responsible for keeping these records intact. For example, if an employee shares a spreadsheet, they must decide whether to give colleagues permission to edit, view or comment. Employees should not grant editing privileges unless necessary.
Also, when employees access electronic, confidential records outside of our offices, they should ensure that both their devices and networks are secure. They should not leave their screens and devices unattended while logged in to the Foundation's accounts.

Data retention period

As a general rule, we will keep all records for a minimum of [two years.] The law may oblige us to retain certain records for a longer period. In this case, we will abide by the law. Also, the following records must be preserved indefinitely:

- *Tax returns*
- *Internal policies*
- *Employment contracts*
- *Partnership and contracts*
- *Financial statements and annual reports*
- *Results of audits and legal investigations*
- *Board Resolutions*
- *Board Minutes*

Discarding records

After the data retention period has passed, authorized employees may choose to discard records for a specific reason. They will usually do this either by shredding physical documents or deleting data from a database or computer. Printed copies of electronic files should be shredded, too.

Records may also be discarded upon request from a stakeholder. For example, a client or partner may ask us to delete their information from our databases. In this case, the Director or Assistant Director will authorize employees to discard relevant records.

Gideon Arulmani,
Director,
The Promise Foundation.
Policy updated 22/4/2021