PRIVACY POLICY

NABFOUNDATION

PRIVACY POLICY

1. Purpose and Scope

NABFOUNDATION is committed to protecting the privacy and confidentiality of staff, vendors, and organization in the way information is collected, stored and used in a secure manner. This policy provides a guidance on NABFOUDATION's legal obligations and ethical expectations in relation to privacy and confidentiality.

Confidentiality applies to the relationship of confidence. Confidentiality ensures that information is accessible only to those authorised to have access, and is protected throughout its lifecycle. Confidential information may be marked as such or deemed confidential by its nature, e.g. it is information that is not available in the public domain.

2. Definitions

Data protection in India is currently governed by the Information Technology (Reasonable security practices and procedures and sensitive personal data or information) Rules, 2011 ("Data Protection Rules") notified under the Information Technology Act, 2000 ("IT Act").

The Data Protection Rules impose certain obligations and compliance requirements on organizations that collect, process, store and transfer sensitive personal data or information2 of individuals such as obtaining consent, publishing a privacy policy, responding to requests from individuals, disclosure and transfer restrictions

Consent: means voluntary agreement to some act, practice or purpose. Consent has two elements: knowledge of the matter agreed to and voluntary agreement.

Individual: means any person such as a partner, vendor, staff member, Board member, contractor or a member of the public.

Organizational information includes publicly available, and some confidential information about organizations.

Personal information means information or an opinion (including information or an opinion forming part of a database) about an individual. It may include information such as names, addresses, bank account details and health conditions.

The public domain in relation to confidentiality is "common knowledge," i.e. information that can be accessed by the general public.

3. Principles

NABFOUDATION is committed to ensuring that information is used in an ethical and responsible manner.

NABFOUDATION recognizes the need to be consistent, cautious and thorough in the way that information about clients, stakeholders, staff and Board members is recorded, stored and managed.

All individuals including vendors, stakeholders, and staff and have legislated rights to privacy of personal information. In circumstances where the right to privacy may be overridden by other considerations, staff acts in accordance with the relevant policy and/or legal framework.

All staff and Board members are to have an appropriate level of understanding about how to meet the organisation's legal and ethical obligations to ensure privacy and confidentiality.

4. Outcomes

NABFOUDATION maintains data in which information is collected, stored, used and disclosed in an appropriate manner complying with both legislative requirements and ethical obligations.

All staff understand their privacy and confidentiality responsibilities in relation to personal information and organisational information about NABFOUDATION, its partner, staff and stakeholders. This understanding is demonstrated in all work practices.

6. Risk Management

NABFOUDATION ensures mechanisms are in place to demonstrate that decisions and actions relating to privacy and confidentiality comply Data Protection Rules and Information Technology Act, 2000 ("IT Act").

All staffs are provided with ongoing support and information to assist them to establish and maintain privacy and confidentiality.

7. Policy Implementation

This policy is developed in consultation with all staff and approved by the Board of Directors. This policy is to be part of all staff orientation processes and all employees are responsible for understanding and adhering to this policy.

This policy should be referenced in relevant policies, procedures and other supporting documents to ensure that it is familiar to all staff and actively used.

This policy will be reviewed in line with NABFOUDATION 'quality improvement program and/or relevant legislative changes.

8. Policy Detail

Data protection in India is currently governed by the Information Technology (Reasonable security practices and procedures and sensitive personal data or information) Rules, 2011 ("Data Protection Rules") notified under the Information Technology Act, 2000 ("IT Act"). The Data Protection Rules impose certain obligations and compliance requirements on organizations that collect, process, store and transfer sensitive personal data or information2 of individuals such as obtaining consent, publishing a privacy policy, responding to requests from individuals, disclosure and transfer restrictions.

8.1 Collection of Information

Information collected by NABFOUDATION is only for purposes which are directly related to the functions or activities of the organisation.

8.2 Use and Disclosure

NABFOUDATION only uses information for the purposes for which it was given, or for purposes which are directly related to one of the functions or activities of the organization. It may be provided to government agencies, other organizations or individuals if:

– The individual has consented

– It is required or authorised by law

– It will prevent or lessen a serious and imminent threat to somebody's life or health.

8.3 Data Quality

NABFOUDATION takes steps to ensure that the information collected is accurate, up-to- date and complete. These steps include maintaining and updating information when we are advised by individuals that it has changed (and at other times as necessary), and checking that information provided about an individual by another person is correct.

8.4 Data Security

NABFOUDATION takes steps to protect the information held against loss, unauthorized access, modification or disclosure and against other misuse. These steps include reasonable physical, technical and administrative security safeguards for electronic and hard copy of paper records as identified below.

Reasonable physical safeguards include:

– Locking filing cabinets and unattended storage areas

– Physically securing the areas in which the information is stored

– Not storing information in public areas

– Positioning computer terminals and fax machines so that they cannot be seen or accessed by unauthorised people or members of the public.

Reasonable technical safeguards include:

– Using passwords to restrict computer access, and requiring regular changes to passwords

– Establishing different access levels so that not all staff can view all information

– Ensuring information is transferred securely

– Installing virus protections and firewalls.

Reasonable administrative safeguards include not only the existence of policies and procedures for guidance but also training to ensure staff are competent in this area.

8.5 Access and Correction

Individuals may request access to personal information held about them. Access will be provided unless there is a sound reason under the Privacy Act or other relevant law. Other situations in which access to information may be withheld include:

– Access to information creates and unreasonable impact on the privacy of others

– The request is clearly frivolous or vexatious or access to the information has been granted previously

– There is existing or anticipated legal dispute resolution proceedings

– Denial of access is required by legislation or law enforcement agencies.

Amendments may be made to information to ensure it is accurate, relevant, up-to-date, complete and not misleading, taking into account the purpose for which the information is collected and used. If the request to amend information does not meet these criteria, NABFOUDATION may refuse the request.

If the requested changes to information is not made, the individual may make a statement about the requested changes which will be attached this to the record.

HR is responsible for responding to queries and requests for access/amendment to information.

8.6 Anonymity and Identifiers

Wherever it is lawful and practicable, individuals will have the option of not identifying themselves or requesting that NABFOUDATION does not store any of their information.

8.7 Collection use and disclosure of confidential information

Other information held by NABFOUDATION may be regarded as confidential, pertaining either to an individual or an organization. The most important factor to consider when determining whether information is confidential is whether the information can be accessed by the general public.

Staff members are to refer to the CEO before transferring or providing information to an external source if they are unsure if the information is sensitive or confidential to NABFOUDATION or staff and stakeholders.

9.Organizational Information

All staff, partners, and vendors agree to adhere to the NABFOUDATION Code of Conduct when commencing employment, involvement or a placement. The Code of Conduct outlines the responsibilities to the organization related to the use of information obtained through their employment/ involvement/ placement.

The Code of Conduct states that individuals will:

"Use information obtained through their involvement, employment or placement only for the purposes of carrying out their duties, and not for financial or other benefit, or to take advantage of another person or organization."

10. Staff Information

The Human Resources Policy details how the organization handles staff records to manage privacy and confidentiality responsibilities, including the storage of and access to staff personnel files and the storage of unsuccessful position applicants' information.

Stakeholder Information:

NABFOUDATION works with a variety of stakeholders including private consultants, government agencies, organizations and foundation. The organization may collect confidential or sensitive information about its stakeholders as part of a working relationship. Staff at NABFOUNDATION will not disclose information about its stakeholders that is not already in the public domain without stakeholder consent.

The manner in which staff members manage stakeholder information will be clearly articulated in any contractual agreements that the organization enters into with a third party.

NABFOUNDATION fully ensures their employees are aware of their responsibilities regarding the protection of data and information as per the privacy policy. In addition to the forgoing, if employees become aware of a theft or loss of data, they are required to immediately report to Human Resources or concerned person/department.

In the event their HRM is not available, they are to immediately report the theft or loss to the Information Technology-Support department.

11. Breach of Privacy or Confidentiality

If employees are dissatisfied with the conduct of a colleague with regards to privacy and confidentiality of information, the matter should be raised with the staff member's direct supervisor. Staff members who are deemed to have breached privacy and confidentiality standards set out in this policy may be subject to disciplinary action.