

**Stichting BRAC International (BRAC International)**

<b>Policy No :02</b>	<b>BRAC International Data Protection Policy</b>	
<b>Staff Covered</b>	<b>All staff in BRAC International Countries and Head Office</b>	
<b>Version/Review History</b>	<b>Department /person Responsible</b>	<b>Approval</b>
Second Approved Version	BRAC International HRD	December 2018 by Supervisory Board, BRAC International
First Approved Version	Rehana Amin Murshed, Jessica Merton	February 2013 by Dr. Mahabub Hossain, Executive Director BRAC and BRAC International

Signed at 6 December 2018 on behalf of Management Board by:



Faruque Ahmed  
Executive Director  
BRAC International

## **BRAC INTERNATIONAL-DATA PROTECTION POLICY**

### **1. Introduction**

BRAC International is committed to complying with the internationally recognised data protection protocol and will ensure that all personal data collected is processed fairly and lawfully, that all statutory requirements are complied with, and that the rights of those whose data is held are protected.

This policy applies equally to directors, management, staff, volunteers, consultants and customers.

### **2. The Data Protection Principles**

BRAC International will implement and comply with the following data protection principles:

- i. Personal data shall be processed and analysed fairly and lawfully
- ii. Personal data shall be obtained for one or more specified and lawful purposes, and shall not be further processed in any manner incompatible with that purpose or those purposes.
- iii. Personal data shall be adequate, relevant and not excessive in relation to the purpose or purposes for which they are processed.
- iv. Personal data shall be accurate, and where necessary, kept up to date.
- v. Personal data processed for any purpose or purposes shall not be kept for longer than is necessary for that purpose or those purposes.
- vi. Personal data shall be processed in accordance with Personal data shall be processed in accordance with the rights of data subjects under the relevant local laws.
- vii. Appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data.
- viii. Personal data shall not be transferred to a country or territory outside the country in which it is collected unless that country or territory ensures an adequate level of protection for the rights of data subjects in relation to the processing of personal data.
- ix. Strict confidentiality must be maintained when collecting, processing and analysing personal data.

### **3. Good Practice Guidelines**

#### Collecting data

Those collecting data must comply with this policy. They should tell data subjects the purpose(s) for which the data is being collected, also details of any other person to whom the data may be disclosed. If sensitive personal data i.e. on race or ethnic origin, political opinions and trade union membership, religious or other beliefs, physical or mental health or condition, sexual life, criminal activities, both committed and alleged, is being collected explicit consent is mandatory. No more data should be collected than is necessary for the purpose(s) declared.

#### Holding data

Data must be securely stored with password protection, encryption or coding where possible. Personnel files must be s in locked filing cabinets with access by authorised staff only. Adequate measures must be taken to ensure no unauthorised access, loss or destruction.

#### Destruction of data

Appropriate approval must be taken for removing any personal data, report/documents in the system. Appropriate measures must be taken to ensure that data earmarked for destruction cannot be reconstructed.

### **4. Data Subjects' Right of Access**

BRAC International is fully committed to facilitating access on request by data subjects to their personal data, while bearing in mind the need to protect other individuals' rights to privacy.

### **5. Responsibilities of Directors, Country Representatives, Supervisors, Staff, Volunteers and Consultants**

Compliance with this policy is the responsibility of all directors, management, staff, volunteers and consultants.

The Country Representative in the countries and Executive Director, BRAC International, will regularly review data protection procedures and practices within the organisation.

By signing contracts of employment, staff consents to personal data being held about them. Agreement to BRAC International's processing of personal data is a condition of staff employment. This includes explicit consent to BRAC on sensitive personal data of the staff e.g. sickness records, health needs, child adaption, etc.

Accessing another employee's personnel records without authority or disclosing personal information in breach of this policy will lead to disciplinary action. Directors, staff, volunteers and consultants can be criminally liable if they disclose personal data in breach of this policy.

## **6. Procedure**

- Any staff member who breaches this policy will be subject to BRAC's disciplinary procedure of respective HRPP. In serious cases such behaviour will be deemed to constitute gross misconduct and, as such, may result in summary dismissal.
- If you have any queries relating to compliance with this policy, please contact respective Head of the Country HRD or Country Representative or if this is not appropriate or feasible, the Regional Director or Executive Director of BRAC International directly.



## **Annex – Data protection Consent**

BRAC will keep data provided to us in a secure personal file. BRAC will only use the information in personal file for:

- Routine record keeping , monitoring and audit
- Process of record in event of an emergency
- BRAC`s and its donors research purposes to promote the objects of their organizations.

I agree to BRAC recording and processing this information about me. I understand that this information will be used only for the purpose(s) set out in the statement above.

### **To be filled up by the employee:**

Name:.....

Signature: .....

PIN: .....

Role:.....

Job Station: .....

Date:.....

### **To be filled up by the office:**

Information verified by (Signature): .....

Date:.....

Name (Block capitals): .....