POPIA COMPLIANCE GUIDELINES FOR BENEFICIARIES & SERVICE PROVIDERS INVOLVED IN ED/SED PROGRAMMES

Purpose of this Document

This guideline aims to ensure all beneficiaries and service providers involved in Economic Development (ED) and Socio-Economic Development (SED) programmes, about the safe and correct handling of personal information in compliance with the Protection of Personal Information Act (POPIA). This includes the collection, processing, storage, and use of personal information of programme beneficiaries, with a particular focus on minors.

1. Obtaining Consent for the Processing of Personal Information

1.1 Important Terms/Definitions

Section 1 of POPIA defines *Personal Information* as:

Information relating to an identifiable, living, natural person, and where it is applicable, an identifiable, existing juristic person, including, but not limited to -

- Name, surname, ID number, registration number
- Contact details (email, telephone number, physical address)
- Demographic details (age, sex, gender, race, marital status, etc.)
- Biometric information
- Personal opinions, views, or preferences
- Correspondence sent by a person that is implicitly or explicitly of a private or confidential nature
- Views or opinions of another individual about the person
- Employment history

- Education information
- Financial information

Personal Information essentially covers any data that can identify a person, either directly or indirectly.

As per Section 26 of POPIA, *Special Personal Information* refers to more sensitive categories of data, which require higher levels of protection, including:

- Religious or philosophical beliefs
- Race or ethnic origin
- Trade union membership
- Political opinions
- Health or sex life
- Biometric information
- Criminal behaviour or records

This type of information may only be processed under specific conditions, such as with the data subject's explicit consent, when necessary for legal obligations (including complying with legislative provisions), or if it is in the public interest.

1.2 Individual Consent Forms

- A POPIA-compliant consent form must be completed for each programme beneficiary whose personal information is collected.
- This applies to all data collected, even where only names and surnames are recorded.
- Information without explicit consent cannot be processed under any circumstance.

1.3 Use of Personal Information

- Personal information must be used solely for the purposes of the ED or SED programme, including attendance tracking, programme reporting, and impact assessments.
- Do not use personal information for unrelated activities such as marketing, fundraising, or sharing with third parties without further consent.

1.4 Communicating the Purpose

- Clearly explain to each data subject (or their legal guardian) *why* their information is being collected, *how* it will be used, *where* it will be stored, and *who* will have access to it.
- This explanation should be given in simple, understandable language.

2. Special Considerations for Minors

2.1 Competent Person Consent

- Written consent must be obtained from a competent person (usually a parent or legal guardian) before collecting any personal information from a minor (child under 18 years of age).
- This applies to all forms of data collection, including forms, photographs, attendance records, and participation details.

2.2 Documentation

- A copy of the signed consent form must be safely stored and made available if required for audit or compliance purposes.

3. Data Minimisation Principles

- Only collect information that is necessary and relevant to the implementation of the programme.
- Avoid collecting excessive or unnecessary information such as age, gender, race, education level, etc., unless there is a clear and documented justification for needing it.
- Review data collection forms regularly to ensure they align with the principle of data minimization.

4. Ensuring Accuracy and Data Updates

- Personal information must be accurate, complete, and kept up to date.
- Operators must implement processes to allow beneficiaries to update their information.
- When a participant exits a programme or changes address or contact details, these changes must be reflected in the records as soon as possible.

5. Secure Storage and Controlled Access

- All personal information must be stored securely, whether in physical or digital format.
- Access to data must be limited to authorized personnel only.
- Implement password protection for digital files and lockable storage for physical files.
- Ensure that backup systems are in place in case of data loss, and that these backups are also secure.

6. Staff and Volunteer Training

- All staff and volunteers involved in handling personal information must receive regular training on POPIA principles. They should understand their responsibilities, the risks of non-compliance, and the importance of safeguarding data.
- Keep records of training sessions and attendance.

7. Specific Guidelines for Common Data Collection Activities

7.1 Attendance Registers

- Always include a privacy disclaimer at the top or bottom of the attendance register.

  Example:

  By signing this register, I acknowledge that I understand the purpose of collecting my information and consent to it being used solely for attendance tracking, programme monitoring, and related reporting, in line with POPIA requirements.
- Avoid circulating a single sheet where everyone can view others' names and contact details.
- Use individual sign-in slips if possible, or digital sign-in solutions.
- Ensure that participants or their guardians understand:
  - Why their information is collected
  - How it will be stored and used
  - Who will have access to it

7.2 Photographs of Beneficiaries

- Always obtain **written consent** before taking or using any photographs.
- For minors, this consent must come from a parent or legal guardian.
- Maintain a list of individuals (especially minors) who have not given photo consent.
  - Instruct staff and photographers to exclude these individuals from images or blur their faces if group photographs are taken.
- Avoid taking group photographs unless all participants have provided consent.
- Where possible, use images that obscure identity (e.g., photographs taken from behind, silhouettes, or shots without faces).
- Never publish full names alongside images unless there is specific, written permission to do so.
- Do not upload or share photographs of workshops or events involving minors to social media platforms unless explicit, written consent for that purpose has been obtained.

8. Record Keeping and Compliance Monitoring

- Maintain an audit trail of all consent forms, attendance sheets, and communications.
- Regularly review data management practices to ensure POPIA compliance.
- Address any breaches or complaints promptly and in accordance with your internal policies and POPIA.

9. Questions and Support

If you have any uncertainties about how to handle personal information, seek guidance from your programme manager [alternative: insert name and contact details] or legal advisor before proceeding.

Remember: Respecting personal information is not just a legal requirement – it is a matter of trust and integrity.

Key Do's and Don'ts for Handling Personal Information

DO's (What You Should Do):

1. **Get Consent (When needed):**
    - Obtain **informed, specific, and voluntary consent** before collecting personal information, especially sensitive or children's data.
2. **Be Transparent:**
    - Clearly explain **why** you're collecting information, **how** it will be used, **who** it will be shared with, and for **how long** it will be kept.
3. **Collect Only What's Necessary:**
    - Limit data collection to **only what is needed** for a specific, lawful purpose.
4. **Secure the Data:**
    - Implement appropriate **security safeguards** (e.g., passwords, encryption, physical security) to protect personal information from loss, damage, or unauthorized access.
5. **Keep Information Accurate and Up to Date:**
    - Take steps to ensure the data you store is **correct** and **updated** regularly.
6. **Give Access to the Data Subject:**
    - Allow individuals to **view, correct, or delete** their personal information when requested.
7. **Have a Privacy Policy:**
    - Maintain and make available a clear **Privacy Policy** that complies with POPIA principles.
8. **Train Your Team:**
    - Educate employees or service providers on POPIA responsibilities and data protection practices.

DON'Ts (What You Should Avoid):

1. **Don't Collect Data Without a Legitimate Purpose:**
    - Avoid collecting personal information **without a clear and lawful reason**.
2. **Don't Use Personal Information for a Different Purpose:**
    - Do not use data for anything **other than what was originally communicated** unless you get further consent.
3. **Don't Keep Data Longer Than Needed:**
    - Avoid storing personal information **longer than necessary** or required by law.
4. **Don't Share Data Without Consent or Legal Justification:**
    - Never give or sell personal data to third parties **without proper authorization or legal grounds**.
5. **Don't Ignore a Data Breach:**

- Failing to report a breach to the **Information Regulator** and affected individuals is a serious offense under POPIA.

6. **Don't Assume Verbal Consent is Enough:**
   - Where possible, **record consent in writing** or use clear opt-in mechanisms.
7. **Don't Leave Personal Data Unprotected:**
   - Avoid using unsecured platforms or storing physical records **without safety measures** in place.