Institution Data Protection Policy Template

1. Overview

Your Institution obtains, uses, stores, and otherwise processes personal data relating to including but not limited to staff, member institutions' staff, faculty and students, current and former workers, contractors, website users and contacts, collectively referred to in this policy as data subjects. When processing personal data, **Your Institution** is obligated to fulfill individuals' reasonable expectations of privacy by complying with the Kenya's Data Protection Act (2019), Kenya Information and Communications Act (1998), Kenya's Access to Information Act (2016), Kenya's Government ICT Standards (2019), EU General Data Protection Regulation (2018) and other relevant data protection legislation (data protection law)

2. Purpose

2.1 This policy applies to all personal data processed by **Your Institution**.

2.2 The appointed Data Protection Officer is responsible for the Organization's ongoing compliance with this policy.

2.3 Implementation is immediate, and this Policy shall stay in force until any alterations are formally agreed.

3. Scope

This policy refers to all parties (employees, job candidates, customers, suppliers etc.) who provide any amount of information to **Your Institution**.

This policy therefore seeks to ensure that **Your Institution**:

3.1 Is clear about how personal data must be processed and the expectations of all those who process personal data on behalf of **Your Institution**.

3.2 Will comply with the data protection laws and good practice thus protect **Your Institution** reputation by ensuring the personal data entrusted to us is processed in accordance with data subjects' rights

3.3 Is protected from risks of personal data breaches and is compliant with the relevant data protection laws

4. Policy

4.1 Definition of terms

4.1.1 **Processing of information** – how information is stored and managed.

4.1.2 **Data Subject** – refers to an individual or entity about whom data is held.

4.1.3 **D**ata **Controller** – is the entity with overall responsibility of data collection and management. In this policy, **Your Institution** is the Data Controller.

4.1.4 **Data Processor** – an individual handling or processing data on behalf of the Data Controller.

4.1.5 **Personal data** – any information which enables a person to be identified

4.1.6 **Sensitive Personal Data**: refers to data revealing a person's race, health status, ethnic, social origin, conscience, belief, genetic data, biometric data, property details, marital status, family details - names of children, parents, spouse, gender, or sexual orientation of a data subject

4.1.7 **Data Protection officer**- Person appointed by **Your Institution** to ensure that the organization processes the personal data of data subjects in compliance with the applicable data protection laws.

4.2 Data Protection Principles

Your Institution is committed to processing data in accordance with the Data Protection Act 2019.As the data controller, **Your Institution** is required to comply with the principles of good information handling.

These principles require **Your Institution** to**:**

4.2.1 Process personal data fairly, lawfully and in a transparent manner.

4.2.2 Ensure the right to privacy of the data subject when processing and handling personal data.

4.2.3 Obtain personal data only for one or more specified and lawful purposes and to ensure that such data is not processed in a manner that is incompatible with the purpose or purposes for which it was obtained.

4.2.4 Ensure that personal data is adequate, relevant and not excessive for the purpose or purposes for which it is held.

4.2.5 Ensure that personal data is accurate and, where necessary, kept up to date.

4.2.6 Ensure that personal data is not kept for any longer than is necessary for the purpose for which it was obtained.

4.2.7 Ensure that personal data is kept secure.

4.2.8 Ensure that personal data is not transferred to a country outside Kenya unless there is proof of adequate data protection safeguards or consent from the data subject.

4.2.9 Adhere to registration requirements by the Office of the Data Protection Commissioner of Kenya

4.3 Consent

Your Institution must record data subjects' explicit consent to storing certain information (known as 'personal data' or 'special categories of personal data') on file.

Personal and special categories of personal data cover information relating to, but not limited to: -

4.3.1 The racial or ethnic origin of the Data Subject,

4.3.2 His/her political opinions.

4.3.3 His/her religious beliefs or other beliefs of a similar nature.

4.3.4 Whether he/she is a member of a trade union.

4.3.5 His/her physical or mental health or condition.

4.3.6 His/her sexual orientation.

4.3.7 The commission or alleged commission by him/her of any offence

4.3.8 Name and contact details

4.3.9 Genetic and/or biometric data which can be used to identify an individual

Consent is not required to store information that is not classified as special category of personal data, if only accurate data that is necessary for a service to be provided is recorded.

As a rule, **Your Institution** will always seek consent where personal or special categories of personal information is to be collected.

It should also be noted that where it is not possible or reasonable to obtain consent at the time when data is first recorded and the case remains open, retrospective consent should be sought at the earliest appropriate opportunity.

If personal and/or special categories of personal data need to be recorded for the purpose of service provision and the service user refuses consent, the case should be referred to the Executive Director for advice.

4.4 Obtaining Consent

Consent may be obtained in several ways and must be recorded on or maintained with the case records.

Your Institution will obtain consent from data subjects through:

4.4.1 Face-to-face

4.4.2 Written

4.4.3 Telephone

4.4.4 Email

4.4.5 Online messaging and/or SMS

4.4.6 Video and/or audio recording

4.4.7 Filled and signed form

4.4.8 Disclaimer notices on webpage

Consent obtained for one purpose cannot automatically be applied to all uses e.g., where consent has been obtained from a service user in relation to information needed for the provision of that service, separate consent would be required.

Preliminary verbal consent should be sought at the point of initial contact as personal and/or special categories of personal data will need to be recorded either on email or a computerized record. The verbal consent is to be recorded in the appropriate fields on computer record or stated on email for future reference. Although written consent is the optimum, verbal consent is the minimum requirement that will be documented through creation of a support ticket and the ticket number shared with the data subject. If the subject is less than 18 years (legal minor) of age then parental/guardian consent should be sought.

Specific consent for use of any photographs and/or videos taken should be obtained in writing. Such media could be used for, but not limited to, publicity material, press releases, social media, and websites. Consent should also indicate whether agreement has been given to their name being published in any associated publicity.

Individuals have a right to withdraw consent at any time in writing.

4.5 Security

Your Institution shall ensure that personal data is stored securely using appropriate ICT infrastructure that is kept-up to date.

4.5.1 Access to personal data shall be limited to personnel who need access and appropriate security shall be in place to avoid unauthorized sharing of information. Destruction or deletion of personal data/records, either print or electronic should be that the records are rendered irrecoverable even using forensic data recovery techniques, for the electronic data**.** Appropriate back-up and disaster recovery solutions shall be in place.

4.5.2 **Your Institution** staff, students, researchers are bound by a Non-Disclosure Agreement, and it is an offence to disclose personal information 'knowingly and recklessly' to third parties.

4.5.3 Personal information shall only be communicated within **Your Institution** staff on a strict need to know basis. Care shall be taken that conversations containing personal or special categories of personal information may not be overheard by people who should not have access to such information.

4.5.4 Where **Your Institution** needs to use the services of an external data processor (such as suppliers and service providers), **Your Institution** shall opt for a data processor who provides sufficient guarantee of data protection; and **Your Institution** and the data processor shall enter into a formal agreement which shall provide that the data processor shall act only on instructions received from **Your Institution** and shall be bound by **Your Institution's** obligations.

4.5.5 Additional information Security Awareness Training may be required by all employees, students, researchers at other intervals when the IT infrastructure environment changes.

4.5.6 All newly hired employees are required to sign an acceptable use policy (AUP) stipulating constraints and practices' that the employee will agree to for access the institutional network, Internet or other resources

4.6 Use of Files, Books and Paper Records

YourInstitution uses paper records in certain instances and to prevent unauthorized access or accidental loss or damage to personal information, **Your_Institution** will ensure that:

- Paper records shall be kept in locked cabinets/drawers overnight and care should be taken to ensure safety of special categories of personal information without leaving the records unattended and in clear view during the working day.
- Any paperwork kept away from the office shall be treated as confidential and stored securely as if it were held held in the office. Documents should not be kept in open view (e.g., on a desktop) but kept in a file in a drawer or filing cabinet as examples, the minimum optimum requirement being a locked cabinet safely out of sight for unauthorized personnel.
- When carrying paper files or documents **Your_Institution** staff shall ensure the documents are in a locked briefcase or in a folder or bag which can be securely closed or zipped up. The briefcase/folder/bag should contain **Your Institution's** contact details.
- Staff members leave an institution/supplier/contractor with the correct number of documents and that they have not inadvertently left any necessary document behind.
- No valuable institutional documents shall be left in an unsecured car. When transporting documents, they should be carried out of sight.

4.7 Disposal of Scrap Paper, Printing or Photocopying Overruns

Your Institution will ensure that any scrap paper, printing, or photocopying overruns are appropriately disposed of: