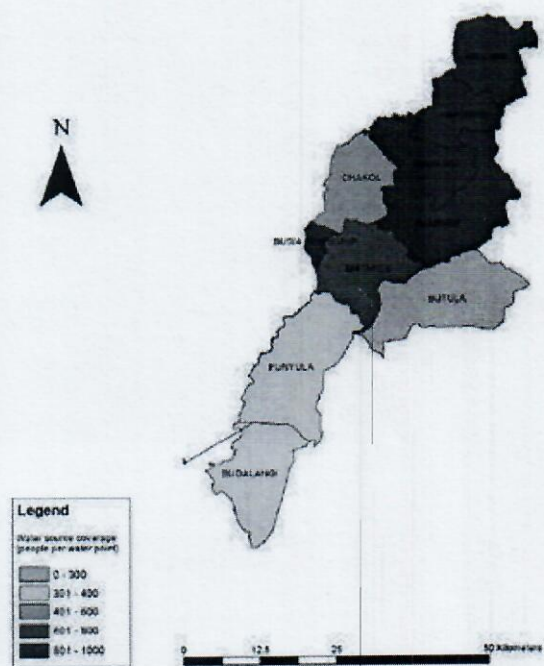


# Draft 3: DATA PROTECTION AND SECURITY POLICY



November, 2015



**PART 1 – SIGN-OFF AND APPROVALS**

**Project: COUNTY GOVERNMENT OF BUSIA DATA PROTECTION AND SECURITY POLICY**

**Sign-off: County Government of Busia Data Protection and Security Policy - Draft Three**

**County: BUSIA**

\_\_\_\_\_

**Accepted**

**Sign-Off:**

\_\_\_\_\_

Accepted with  
Modifications

\_\_\_\_\_

Not Accepted

**Signature:**

\_\_\_\_\_

**Name (Capitals):**

\_\_\_\_\_

Date \_\_\_\_\_

**Position:**

.....  
charge of ICT

In

**Signature:**

\_\_\_\_\_

**Name (Capitals):**

\_\_\_\_\_

Date \_\_\_\_\_

**Position:**

Governor

**Signature:**

\_\_\_\_\_

Date \_\_\_\_\_



## **Introduction to Data Protection**

As a public authority, the County Government of Busia (CGB) has an obligation to protect its information assets and, in particular, the information relating to its staff, stakeholders and other individuals in whatever form that information is held. The CGB is careful to ensure that personal information is properly safeguarded. The CGB and all those who process or have access to personal information must comply with the Data Protection Principles laid out at all times. Unauthorised disclosure may be a disciplinary matter and in some cases may be considered as gross misconduct.

The CGB functions require us to obtain, process and manage certain information about individuals/organisations to enable us to provide a high level of service being requested by citizens, employees and stakeholders.

All data, whether held electronically or manually, will be kept securely and not disclosed unlawfully. The CGB respects and will accommodate the right of individuals to access, check and improve the accuracy of any personal data that is being kept about them, either on computer or in a relevant filing system, as defined in legislation.

The CGB's Data Protection Policy and Guidance is available via the county website.

### **1. Objective**

The objective of this policy is to set out the CGB's commitment towards safeguarding personal data processed by or disclosed to staff or other authorised persons ensuring its confidentiality, integrity and availability by processing it in accordance with the Kenyan laws that relate to data protection. It also sets out the requirements and responsibilities of staff with access to personal data to promote understanding of confidentiality obligations.

Personal Data is defined as:

Data which relate to a living individual who can be identified –

(a) from those data, or

(b) from those data and other information which is in the possession of, or is likely to come into the possession of, the data controller

The terminology 'processing' refers to data being obtained, recorded, filed, actioned, stored, archived and disposed of.



## **2. Responsibilities of staff, stakeholders and authorised third parties**

### CGB Data Controller and Information Officer

CGB is the Data Controller i.e the County Government “determine the purposes for which and the manner in which any personal data are processed”

The Information Officer has responsibility, on behalf of the Principal:

- to ensure that the CGB maintains an up-to-date notification of its use of data with the Information Commissioner.
- Ensure the CGB is kept informed of legislative changes and that relevant amendments are implemented into the CGB processes.
- to ensure that staff, stakeholders and authorised third parties comply with the 8 Data Protection Principles, as set out in the relevant laws in Kenya and other International laws, in respect of data under their control;
- to ensure that the CGB’s Policy, guidelines and security measures are appropriate and up to date for the types of data being processed;
- train and advise staff on the interpretation of this policy and guidelines and to monitor compliance with the policy.
- be the contact point for the administration of all subject access requests relating to data held by the CGB;

### Employee Obligations.

All staff, stakeholders and authorised third parties are responsible for working in compliance with the Data Protection principles, as set out in this policy.

All CGB employees must complete mandatory training on Data Protection and they receive regular information updates on new policies and procedures as they become operational.

Throughout the course of employment, staff including agency, temporary and voluntary personnel will have access to various extracts of personal data pertaining to staff/stakeholders, depending on the nature of their role.

The format of this data will include hardcopy and electronic format e.g enrolment forms, personnel/finance forms and the other forms.

All staff are expected to behave in a responsible, professional, ethical and lawful manner when processing personal data.

Employees have a duty to safeguard any personal/sensitive data which is made known to them. This confidentiality applies to both during the term of employment and post termination.

Personal data must never be disclosed to anyone other than employees who are authorised to receive it in the course of their duties or third parties clearly associated with the provisions of the

*County Government of Busia Data Protection and Security Policy*



CGB's services authorised to receive it.

Staff must demonstrate extremely high levels of data accuracy when keying onto any database.

### Data Subject Obligations

As Data Subjects, all staff, stakeholders and authorised third parties are responsible for:

- ensuring that any personal information they provide to the CGB in connection with their employment, registration or other contractual agreement is accurate;
- informing the CGB of any changes to any personal information which they have provided, e.g. changes of address;
- responding to requests to check the accuracy of the personal information held on them and processed by the CGB, details of which will be sent out from time to time, and informing the CGB of any errors or changes to be made.

### Third party Processor Obligations

Any third party data processors will have the contractual responsibility to ensure that any processing of personal data carried out on behalf of the CGB is done in compliance with the CGB's Data Protection policy. It is the responsibility of departments and individuals contracting with third parties, with Directorate approval, to confirm that those parties treat the information in accordance with the requirements of the act.

## **3. Subject Consent to Processing**

The CGB will observe the conditions for processing personal information as laid down in legislation and in this policy. It is committed to ensuring transparency as to the reasons why certain information is required from data subjects and its subsequent destination. It will be assumed that consent has been given by the Data Subject for his/her data to be used for the purposes advised at the point of obtaining that data. Where the data is defined as sensitive personal data, explicit consent must be obtained from the Data Subject before processing can proceed.

The CGB understands "consent" to mean that the stakeholder has signified their agreement whilst being in a fit state of mind to do so and without pressure being exerted upon them. There must be active communication between the parties and consent will not be inferred assumed from non-response to a communication. Verbal consent for simple information requests should be acceptable so long as proper security checks are made to ensure that the person giving the consent *is* the stakeholder. In the case of telephone consent, the subject will be asked to confirm several separate facts that should be privy only to them (stakeholder identity number, date of birth etc). For sensitive data, explicit written consent of individuals should always be obtained unless an alternative legitimate basis for processing exists.

## **4. Privacy Notices**

A Privacy Notice is available on the CGB website to inform citizens as to the types of personal data we collect and how we will use the data which they provide to us. Citizens will also be advised of the conditions under which we may be required to disclose their data and how they can submit a Subject Access Request to the CGB.



## **5. Publication of Information**

In accordance with the Access to Information Act 2016 it is CGB policy to routinely make public a wide range of documented information surrounding CGB functions and policies.

## **6. Rights of Access to Personal Information**

The CGB respects and will accommodate the right of individuals to access, check and improve the accuracy of any personal data that is being kept about them, either on computer or in a relevant filing system, as defined in legislation.

Staff, stakeholders and others have the right to access any personal data that CGB keeps about them, either on a computer or in paper files. Any person who wishes to exercise this right should preferably complete the CGB Information Release Form, or contact the Head of ICT. The CGB will not charge any fee for access to information.

CGB aims to comply with requests for access to personal information as quickly as possible, and will ensure that it is provided within 40 calendar days unless there are mitigating factors which may cause a delay. In such cases, the reason for delay will be explained in writing to the data subject making the request.

CGB requests all Information Requests are forwarded to the following:

Chief Officer Finance and ICT  
County Government of Busia  
Private Bag  
Busia - Kenya

The CGB will acknowledge receipt of all Information Requests, collate the information which has been requested and respond officially within 40 calendar days.

There may be occasions where clarification is required to progress a request. On these occasions, the Chief Officer will communicate directly with the requester.

## **7. Disclosure**

### **Disclosing Personal Data**

Personal data will be disclosed where there is a legal or statutory obligation or on receipt of a valid subject access request in accordance with the requirements of the relevant Kenyan laws. In dealing with a subject access request CGB will be sensitive to and give proper consideration to the data subjects right of access and the right of privacy in relation to any 'third party' information contained in the response. Third party information will only be disclosed if additional conditions are met, in general this means the third party must give consent.

Sensitive personal data (racial or ethnic origin, political opinions, religious beliefs, trade union membership, health, sex life, criminal convictions) will only be disclosed where additional conditions as defined by the Kenyan law are met.

### **Informing Stakeholders of Disclosures and Obtaining Consent**

*County Government of Busia Data Protection and Security Policy*



Stakeholders will be informed of predictable disclosures (such as confirmation of stakeholders status, responding to a request for a reference) when they register with the CGB and be able to opt out of certain processing (including disclosures) on their registration form. This information will be recorded on the CGB database.

In less predictable situations the stakeholder should give their consent before any information is released.

### **Method of Disclosure**

Data will be disclosed by letter or in the preferred and permanent format as requested in the subject access request. Disclosures will not be made over the telephone. To expedite simple enquiries and where the identity of the stakeholder has been verified personal data may be emailed to the data subjects CGB email address.

### **Internal (within CGB) Disclosures by Telephone**

Stakeholder or staff personal data should only be disclosed to other CGB employees or contractors where they have a legitimate, business interest in the data concerned. Before disclosure the identity of the caller must be ascertained.

### **External (outside CGB) Disclosures by Telephone**

Stakeholder or staff personal data will not be disclosed by telephone.

### **Disclosures to the Police**

Disclosures to the Police will be made where the CGB is served with a Court Order requiring information and in other limited circumstances as defined in Kenyan laws.

If a member of staff is contacted by the Police with a request they should notify the Chief Officer Finance and ICT for advice on how to deal with the enquiry.

## **8. Retention and storage of Data**

Personal data processed for any purpose shall not be kept for longer than is necessary for those purposes or as required to comply with other legislation. Where there is good reason some forms of information will be kept for longer than others in the CGB archive.

Records will be stored securely and appropriate to their medium. Electronic records will be accessible through passwords and various permission levels.

Hard copy records will be stored in secure cabinets and drawers.

## **9. Copying and publishing data**

Backups and restoring of CGB data will be performed on a daily basis and will remain part of the Disaster Recovery Plan.

Photocopies and prints will be made when necessary and destroyed appropriately.

CGB Reports will be published and stored appropriately.

Staff are not permitted to use Personal Email accounts to transfer CGB data.



## **10. Disposal of Records (data)**

Data will be appropriately and properly disposed of when no longer needed for the effective functioning of the institution and its members. This will be in accordance to relevant to Kenyan laws.

## **11. Use of audio, photography, video and CCTV**

That will be availed upon approval by the Chief Officer on a written request.

## **12. Policy Awareness**

Access to Information Act 2016 will be a mandatory element of all staff induction. Any changed to the Act will be circulated to all staff and published on the CGB Intranet/Internet for staff, stakeholders and members of the public to view. All staff, stakeholders and authorised third parties are expected to be familiar with and comply with the policy at all times.

## **13. Reporting a Breach in Data Security**

It is the responsibility of all staff, stakeholders and any third parties authorised to access the CGB's personal data sets to ensure that those data, whether held electronically or manually, are kept securely and not disclosed unlawfully, in accordance with the Kenyan laws.

Unauthorised disclosure will usually be treated as a disciplinary matter, and could be considered as constituting gross misconduct with, in some cases, access to facilities withdrawn or even criminal prosecution.

If any individual considers that their data or that of others has been lost, damaged or has not been processed or managed in compliance with the Access to Information Act 2016.

## **14. Status of the Policy**

This policy does not form part of the formal contract of employment, but it is a condition of employment that employees will abide by the rules and policies made by the CGB from time to time. Likewise the policy is an integral part of the General Regulations for all stakeholders including employees of CGB.

Failure to comply with this policy may result in damage to CGB reputation, data loss and damage and distress to the individuals affected.

Compliance is the responsibility of all staff, stakeholders and authorised third parties. Any breach of this Data Protection Policy may lead to disciplinary action being taken, access to CGB information facilities being withdrawn, or even a criminal prosecution. Any questions or concerns about the interpretation or operation of this policy should be taken up initially with the Head of ICT.

## **The Data Protection Principles**

When processing personal information the following eight principles must be complied with and data must:

1. be obtained and processed fairly and lawfully and shall not be processed unless certain conditions are met.



2. be obtained for a specified and lawful purpose and shall not be processed in any manner incompatible with that purpose.
3. be adequate, relevant and not excessive for those purposes.
4. be accurate and kept up to date.
5. not be kept for longer than is necessary for that purpose.
6. be processed in accordance with the Data Subject's rights.
7. be kept safe from unauthorised access, accidental loss or destruction.
8. not be transferred to a country outside Kenya.

### **RESPONSIBLE OWNER**

It is the responsibility of the Chief Officer Finance and ICT to ensure this policy is implemented, adhered to and reviewed. Complaints regarding this policy or the data misuse should be forwarded to the Chief Officer Finance and ICT.

### **COMMUNICATION**

This Policy will be available for all staff in the Policies and Procedures section of the CGB intranet. It will also be made available to stakeholders via the CGB website.

### **REVIEW**

This policy will be reviewed (and if necessary updated) annually or sooner if required to reflect changes in legislation or circumstance.