



DATA PRIVACY STATEMENT FOR EMPLOYEES, CONTRACT STAFF AND INTERNS

CONTENTS

Abbreviations	3
Definitions	3
Introduction	4
Scope	4
1 Acknowledgement and Consent	4
2 When is personal data collected from you?	4
3 What personal data is collected from you?	5
4 Why do we need to collect and use your personal data?	7
5 Do we retain any of your personal data?	7
6 With whom will we share/disclose your personal data?	8
7 Commercial use of your personal data	8
8 Access to or updating your personal data	8
9 Safeguarding and protecting your personal data.	9
10 Employee Activity Monitoring	9
11 Transfer of your personal data outside Kenya	10
12 Automated Processing and Your Rights	10
13 Our Contacts	10
14 Data Protection Officer (DPO) Contacts	11
15 Guidelines for lodging complaints and exercising data subject rights	11
15.1 Purpose	11
15.2 Scope	11
15.3 Data Subject Rights	11
15.4 Submission Channels	11
15.5 Request submission guidelines	11
15.6 Acknowledgement and verification	12
15.7 Timelines for resolution	12
15.8 Escalation and appeals	12
15.9 Record keeping	12

ABBREVIATIONS

CCTV	Closed Circuit Television
DCI	Directorate of Criminal Investigations
NSSF	National Social Security Fund
NHIF	National Hospital Insurance Fund
KRA	Kenya Revenue Authority
PIN	Personal Identification Number
ID	Identity
CBK	Central Bank of Kenya
HELB	Higher Education Loans Board

DEFINITIONS

Personal data, Sensitive personal data, identifiable natural person – as given meaning in the Kenya Data Protection Act, 2019.

Processing – as given meaning in the Kenya Data Protection Act, 2019.

“You”, “Your” – this may mean, as the situation may apply:

- I. Job Applicant** – A person who applies for a job at HFCB through our online recruitment portal or submits their Curriculum Vitae and/or application materials to HFCB through email or any other approved recruitment channel.
- II. Employee** – A person who is employed by HFCB under an executed employment contract with the Bank.
- III. Intern** – A person who has been offered and accepted an internship opportunity at HFCB for a defined period to gain practical work experience.
- IV. Contract Staff** – A person employed by a third-party organisation and assigned to HFCB to provide services to the Bank under a contractual arrangement between HFCB and the third party.
- V. Consultant** – An individual or firm engaged by HFCB under a consultancy agreement to provide specialised professional, technical, advisory, or project-related services for a defined scope and duration.
- VI. Team-as-a-Service (TaaS) Personnel / Secondees** – Individuals assigned to HFCB by a service provider, partner organisation, or affiliate entity as part of a Team-as-a-Service, staff augmentation, secondment, or similar resource arrangement to perform agreed functions on behalf of or for the benefit of HFCB.
- VII. Temporary Staff** – A person engaged by HFCB directly or through a third party on a temporary, casual, fixed-term, seasonal, or short-term basis to perform specific duties for a defined period.

“Organization”, “Us”, “We”, “Our” – HFCB, including the Bank, and all its subsidiaries as listed on the official group website.

INTRODUCTION

HFCB operates in a complex and data-driven environment that requires the collection and use of personal data in order to fulfil its obligations as an employer and as a regulated financial institution. We are committed to handling personal data lawfully, fairly, transparently and securely in accordance with applicable data protection, banking, employment and other relevant laws and regulations.

This Statement explains how HFCB collects, uses, shares, stores and protects personal data relating to employees, contract staff, interns and job applicants. It also outlines your rights and the controls established by HFCB to safeguard personal data.

SCOPE

This Data Privacy Statement applies to:

- Employees;
- Contract staff;
- Interns;
- Temporary staff;
- Consultants engaged directly by HFCB;
- Personnel seconded to HFCB by third parties; and
- Job applicants.

1. ACKNOWLEDGEMENT AND CONSENT

By applying for a position, accepting employment, providing personal data to HFCB or otherwise engaging with HFCB in any of the ways described in this Statement, you acknowledge that HFCB may collect and process your personal data for the purposes outlined herein.

Where consent is required by law, HFCB shall seek such consent before processing your personal data. Withdrawal of consent shall not affect the lawfulness of processing undertaken prior to such withdrawal. In certain cases, withdrawal of consent may limit HFCB's ability to maintain or continue an employment or contractual relationship where processing is necessary to fulfil legal, contractual, business or regulatory obligations.

2. WHEN IS PERSONAL DATA COLLECTED FROM YOU?

HFCB may collect personal data from you in various circumstances including, but not limited to:

- a) During recruitment and job application processes.
- b) During employee onboarding and establishment of employment records.
- c) In the course of employment when updating employee records, administering benefits, managing performance, facilitating training or undertaking workforce administration activities.
- d) When you visit HFCB premises, branches or facilities, including through visitor management systems, security systems and CCTV installations.

- e) When you use HFCB information technology resources, devices, communication systems, applications, networks, cloud-hosted services, collaboration platforms, business systems or digital channels.
- f) During investigations, audits, compliance reviews, disciplinary processes, grievance handling, whistleblowing programmes or regulatory engagements.
- g) During emergency response, business continuity management, health and safety activities or employee welfare programmes.
- h) Through third parties authorised or required to provide information relating to your employment, qualifications, professional certifications, references, background checks or legal and regulatory obligations.

3. WHAT PERSONAL DATA IS COLLECTED FROM YOU?

HFCB may collect and process personal data including, but not limited to:

a) Personal identification information

- Full names
- National ID, Passport or Alien ID information
- Date of birth
- Gender
- Nationality
- Marital status
- Postal and physical address
- Contact information
- Photographs

b) Employment and Professional Information

- Curriculum vitae and employment history
- Academic qualifications
- Professional certifications
- Reference and background verification information
- Performance and competency records
- Training and development records
- Employment contracts and related documentation



c) Financial and Benefits Information

- Payroll information
- Bank account details
- Tax information
- Pension and social security information
- Medical insurance information
- Staff lending and credit product information

d) Sensitive Personal Data

Where necessary and legally permissible, HFCB may process sensitive personal data including:

- Health and medical information
- Biometric information used for authorised access control and security purposes
- Information required to comply with legal and regulatory obligations

e) Technology, Security and Activity Information

HFCB may collect information generated through the use of its systems and services including:

- User account information
- System access records
- Device information
- Network activity logs
- Email and communication metadata
- Document and file access records
- Collaboration platform activity records
- Security alerts and audit logs
- Authentication and access management records
- System, application and service telemetry

f) Investigation and Compliance Information

Where necessary, HFCB may process information relating to:

- Internal investigations
- Fraud prevention activities
- Disciplinary matters
- Grievances and complaints

- Security incidents
- Legal proceedings
- Regulatory reviews and inspections

4. WHY DO WE NEED TO COLLECT AND USE YOUR PERSONAL DATA?

HFCB processes personal data based on lawful grounds including consent, contractual necessity, legal obligations, legitimate interests, public interest and other lawful bases recognised under applicable law.

Your personal data may be used for purposes including:

- Recruitment and hiring activities.
- Employee onboarding and administration.
- Payroll and benefits administration.
- Employee welfare, health and safety management.
- Training, development and certification management.
- Workforce planning and resource management.
- Performance management and career development.
- Administration of employee loan facilities and credit products.
- Verification of identity, qualifications and employment history.
- Compliance with legal, regulatory and contractual obligations.
- Fraud prevention, financial crime management and risk management activities.
- Protection of HFCB information assets, customers, employees and systems.
- Monitoring, managing and securing HFCB information technology resources, communication systems, networks, applications and cloud-based services.
- Detecting, investigating and responding to cyber security threats, security incidents, misuse of systems, policy violations, fraud, misconduct or unlawful activity.
- Conducting audits, investigations, reviews and compliance assessments.
- Business continuity, disaster recovery and crisis management activities.
- Defending, establishing or exercising legal rights.

5. DO WE RETAIN ANY OF YOUR PERSONAL DATA?

HFCB shall retain personal data only for as long as necessary to fulfil the purpose for which it was collected and processed.

Retention periods may vary depending on:

- Employment requirements;

- Legal obligations;
- Regulatory requirements;
- Business needs;
- Security requirements;
- Investigation requirements;
- Audit requirements; or
- Record management obligations.

Different categories of records shall be retained in accordance with HFCB's applicable Records Retention Schedule and relevant legal and regulatory requirements.

6. WITH WHOM WILL WE SHARE OR DISCLOSE YOUR PERSONAL DATA?

HFCB may share personal data where necessary and lawful with:

- HFCB subsidiaries and affiliated entities.
- Regulatory, supervisory, law enforcement and government authorities.
- External auditors and professional advisers.
- Pension, insurance and employee welfare providers.
- Background screening and verification service providers.
- Technology service providers, software vendors, cloud-hosted service providers and managed service providers supporting HFCB operations.
- Security service providers.
- Training and professional development institutions.
- Third parties where disclosure is necessary to fulfil legal, contractual or regulatory obligations.

All such disclosures shall be subject to appropriate contractual, technical and organisational safeguards.

7. COMMERCIAL USE OF PERSONAL DATA

HFCB shall not use employee personal data for commercial marketing purposes except where permitted by law or where appropriate consent has been obtained.

8. ACCESS TO OR UPDATING YOUR PERSONAL DATA

Employees may request access to personal data held by HFCB and may request correction or updating of inaccurate or incomplete information in accordance with established internal procedures and applicable law.

9. SAFEGUARDING AND PROTECTING YOUR PERSONAL DATA

HFCB has implemented appropriate technical, organisational and administrative safeguards to protect personal data against unauthorised access, disclosure, alteration, loss, misuse or destruction.

These safeguards may include:

- Access controls
- Encryption technologies
- Monitoring and audit controls
- Data loss prevention controls
- Security assessments
- Incident management procedures
- Physical security measures
- Employee awareness programmes

10. EMPLOYEE ACTIVITY MONITORING

As part of the management, security and protection of HFCB information, systems and technology resources, HFCB may monitor activities conducted on or through systems, devices, networks, applications, communication platforms and services provided, authorised or managed by HFCB.

Monitoring may include the collection and review of system access records, user activity logs, communication metadata, file access information, security events, audit records, device information and other operational or technical information generated through the use of HFCB resources.

Such monitoring may be undertaken for legitimate business, security, compliance, legal, regulatory, operational, audit and investigative purposes including:

- Managing cyber security risks;
- Detecting and responding to threats;
- Preventing fraud and misconduct;
- Protecting customers, employees and information assets;
- Investigating suspected policy violations;
- Ensuring compliance with applicable legal and regulatory obligations.

Employees should use HFCB systems primarily for authorised business purposes and should not expect absolute privacy when using HFCB-owned, managed or authorised systems, devices, networks or services.

Access to monitoring information shall be limited to authorised persons on a need-to-know basis and shall be handled in accordance with applicable policies, procedures and legal requirements.

11. TRANSFER OF PERSONAL DATA OUTSIDE KENYA

HFCB may transfer personal data outside Kenya where necessary to fulfil legitimate business, technical, legal, regulatory or operational requirements.

This may include the use of international service providers, technology vendors, software platforms, cloud-hosted services, outsourced service providers and affiliated entities.

Where personal data is transferred outside Kenya, HFCB shall implement appropriate safeguards and transfer mechanisms in accordance with applicable legal and regulatory requirements to ensure the security and protection of personal data.

12. AUTOMATED PROCESSING AND YOUR RIGHTS

Certain HFCB systems may utilise automated technologies to support employee administration, access management, security monitoring, fraud detection, risk management, workflow processing and other operational activities.

Where required by law, HFCB shall implement appropriate safeguards and human oversight in relation to automated processing activities.

Employees have the rights provided under applicable data protection laws including:

- Right to be informed;
- Right of access;
- Right to correction;
- Right to deletion where applicable;
- Right to object to processing where applicable;
- Right to restrict processing;
- Right to data portability where applicable;
- Right to withdraw consent;
- Right not to be subject to unlawful automated decision making;
- Right to lodge a complaint with the Office of the Data Protection Commissioner.

13. OUR CONTACTS

Our contact details are:

HFCB

Rehani House, Kenyatta Avenue / Koinange Street

P.O. Box 30088-00100, Nairobi Telephone: 0709 438 000 & 0709 438 888

Website: <https://www.hfcb.co.ke/>

14. DATA PROTECTION OFFICER (DPO) CONTACTS

Email Address: dpo@hfcfb.co.ke

15. GUIDELINES FOR LODGING COMPLAINTS AND EXERCISING DATA SUBJECT RIGHTS

15.1 Purpose

This guideline outlines how data subjects can exercise their rights under the Kenya Data Protection Act, 2019. It ensures that all requests and complaints are handled transparently, accessibly, and within the stipulated legal timeframes.

15.2 Scope

This guideline applies to all data subjects whose personal data is processed by HFCB Group and its subsidiaries, including employees, customers, partners, and other stakeholders.

15.3 Data Subject Rights

Under the Kenya Data Protection Act, data subjects have been accorded data subject rights as outlined in section 12 above.

15.4 Submission Channels

Requests and complaints can be submitted through the following channels:

- Email: dpo@hfcfb.co.ke
- Postal Mail:
Data Protection Office
P.O Box 30088 – 00100, Nairobi, Kenya
- Phone: +254 709438000, 709438888
- In-person: HFCB Head Offices or nearest branch

15.5 Request submission guidelines

To process a request, the data subject must provide:

- Full name
- Contact information (email or phone)
- Description of the request or complaint
- Proof of identity (for verification)

Requests lacking sufficient information may result in processing delays.

15.6 Acknowledgement and verification

All valid requests will be acknowledged within 5 business days. Identity verification shall be conducted prior to processing requests involving both personal or sensitive data. All requests shall be acknowledged within 5 business days of identity verification. The request shall thereafter be complied within the provisions of the law.

15.7 Timelines for resolution

Resolution timelines for all complaints and for exercising data subject rights will be as per the Kenya Data Protection Act.

If additional time is required for complex cases, the data subject will be informed within the initial period with an estimated resolution date.

15.8 Escalation and appeals

If the data subject is dissatisfied with the resolution, they may escalate to the Data Protection Officer via dpo@hfcg.co.ke or lodge a complaint directly with the Office of the Data Protection Commissioner (ODPC) at www.odpc.go.ke.

15.9 Record keeping

All requests, complaints, and related correspondence will be securely logged and retained in accordance with our data retention and protection policies.

