

(FOR PUBLIC)

(Last Updated: 16 March 2026)

HFCB GROUP Plc

APPROVED BY THE BOARD OF DIRECTORS
ON: April 2024



Disclaimer

On our websites or portals, we may provide hyperlinks to other websites or third parties. When you visit these websites as redirected from our websites or portals, you shall be subject to the third party's terms and conditions and privacy policies, and we do not in any way guarantee nor will we be held responsible for the privacy of your personal data while accessing those third-party websites.

Our Rights

HFCB Group Limited or its Subsidiary Companies reserves the right to update, modify or amend this policy statement at any time and an updated copy can be obtained from the official group website.

General Statement

This Data Privacy Statement applies to HFCB GROUP PLC and its respective subsidiaries.

Copyright © 2025 HFCB GROUP LIMITED. All Rights Reserved

Table of Contents

Disclaimer	1
Our Rights	1
General Statement	1
Abbreviations	3
Definitions	4
Introduction	5
Scope	5
Individual Statements	5
1. Acknowledgement and Consent	6
2. When is personal data collected from you?	6
3. What personal data is collected from you?	6
4. Why do we need to collect and use your personal data?	7
5. Do we retain any of your personal data?	8
6. With whom will we share/disclose your personal data?	8
7. Commercial use of your personal data	9
8. Use of Behavioral Analytics & Personalization Technologies	9
9. Access to or update your personal data	11
10. Safeguarding and protecting your personal data	11
11. Handling your sensitive personal data	11
12. Transfer of your personal data outside Kenya	12
13. Your rights	12
14. Our Contacts	13
15. Data Protection Officer (DPO) Contacts	13
16. Guidelines for lodging complaints and exercising data subject rights	14
16.1. Purpose	14
16.2. Scope	14
16.3. Data Subject Rights	14
16.4. Submission Channels	14
16.5. Request submission guidelines	14
16.6. Timelines for resolution	15
16.7. Escalation and appeals	15
16.8. Record keeping	15



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
- CDD** – Customer Due Diligence
- ECDD** – Enhanced Customer Due Diligence
- KYC** – Know Your Customer
- AML** – Anti Money Laundering
- CFT** – Counter Terrorist Financing
- IPRS** – Integrated Population Registration System



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.

Customer(s), “You”, “Your” – this may mean, as the situation may apply:

- i. The person who enquires about purchases, subscribes to, enrolls onto, or consumes any of our products and/or services or accesses our websites or other HFCB Group Limited or its Subsidiary Companies’ portals.
- ii. Any visitor including contractors/service providers or any third party who gains access to any HFCB Group Limited or its Subsidiary Companies’ premises.

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

Introduction

HFCB Group Limited and its Subsidiary Companies operate in a complex, data-oriented environment that requires use of personal data to fulfil its core mandate in serving various stakeholders. This policy is our commitment to handling your personal data with the privacy it requires and in accordance with the provisions of various laws and regulations. The below outlines our key touch points with you, highlighting how we shall be handling your personal data throughout its lifecycle right from acquisition to erasure. The statement also spells out your rights and indicates the controls the organization has established to safeguard your data.

Scope

This Data Privacy statement applies to all our customers where the term customer is given meaning above.

Individual Statements

1. Acknowledgement and consent.
2. When is personal data collected from you?
3. What personal data is collected from you?
4. Why do we need to collect and use your personal data?
5. Do we retain any of your personal data?
6. With whom will we share/disclose your personal data?
7. Transfer of your information.
8. Direct marketing.
9. Access to or updating your personal data.
10. Safeguarding and protecting your personal data.
11. Handling your sensitive personal data.
12. Your rights.
13. Our Contacts.

1. Acknowledgement and Consent

By choosing to interact with us in any of the ways outlined in section 2, you will be doing so with full knowledge and consent that we will collect and process your personal data.

By consenting, you allow us to collect, process, store, disclose, transfer your data as guided in the provisions of the Data Protection Laws.

By withholding or withdrawing your consent, HFCB Group Limited and its Subsidiary Companies shall terminate any agreement with you and reject any further applications.

Please note that withholding or withdrawing your consent shall not apply to any processing done on your personal data prior to you exercising this right.

2. When is personal data collected from you?

We will collect your personal information when you: (This list is not exhaustive):

- a) Enquire about, subscribe to, enroll onto or take up any of our products or services.
- b) Visit our offices, including the head office or any of our branches or subsidiary offices.
- c) Visit our websites or any of our online portals.
- d) Call our contact center, treasury or any official bank numbers.
- e) Utilize any of our bank provided WIFI connections.
- f) Report an incident or lodge a complaint through any of our specified channels.

3. What personal data is collected from you?

Whenever you interact with us, we will collect the following information from you. (Please note that this list is not exhaustive):

- a) Information relating to enquiring about, acquiring or procuring, subscribing or onboarding/enrolling onto any of our HFCB Group Limited or its Subsidiary Companies' products or services or channels. Such information includes: your full names, identification document type(s) and number(s), phone number, email address, location, postal address, date of birth, age, gender, photograph, signature, marital status, PIN number, occupation, nationality, etc.
- b) Information that enables us to contact you and/or positively identify you in relation to enquiries made by you through our channels or portals and/or offer support for products or services that you have acquired/procured from us including account number(s), account name(s), transaction history, phone number, etc.
- c) Information that will enable us to conduct CDD/ECDD/KYC/AML/CFT validation checks as required of us by the regulators. Such information will include: your identification number, KRA details for individuals or corporates as case may be, company details and relevant incorporation documents, etc.

- d) Surveillance recordings captured by our Closed-Circuit TV (CCTV) that have been installed in strategic places in any of the HFCB Group Limited and Its Subsidiary Companies' premises to improve the security posture of the facilities.
- e) Information for safety and security purposes when you visit our premises which is recorded in an access register at the building entrance including your name, phone number(s), identification type and number, company or institution details.
- f) When you visit our websites, Internet Banking, Mobile Banking or any of our other portals, we will collect information such as your device address, location, browsing preferences.
- g) Voice recordings whenever you call our contact center, treasury or any other official numbers.
- h) When you use Bank provided WIFI, we will collect your device address, traffic information including sites visited, duration and date for the traffic.
- i) When you report an incident relating to any of your products or lodge a complaint with us, we may collect information relating to such reports including your full names, identification document type(s) and number(s) phone number, email address, location, postal address.

4. Why do we need to collect and use your personal data?

The Data Protection Law sets out the legal grounds that allow us to collect and process your personal information. These grounds include: your consent; the need to perform a contract for a product or service you have with us; compliance with legal or regulatory obligations; protection of public interests or your vital interests; and the legitimate business interests of HFCB Group Limited and its subsidiary companies.

We will use and process the information collected from you for various purposes including: (please note that this list is not exhaustive):

- a) For positive identification purposes including:
 - i. When you contact us with inquiries or service requests regarding any of the products or services, we offer you.
 - ii. For cross-refencing with various government databases e.g. IPRS, KRA etc.
- b) For communication purposes including:
 - i. Contacting you about products or services that we are offering you or that you have enquired about.
 - ii. Promotional messages for existing, new or updated products or service offerings.
 - iii. Technology systems, premises accessibility and/or account transaction updates.
 - iv. Any other general information.
- c) Satisfying our contractual obligations to you when providing the products and/or services you have procured from us.
- d) Building a dependable customer profile and provision of customized services by:
 - i. Conducting credit checks and credit scoring with various credit reference bureaus.
 - ii. Conducting CDD/ECDD/AML/CTF checks with various internal and government databases and various sanction lists.
 - iii. Establishing customer/company legitimacy/validity.
- e) Aiding investigations in the event of reported incidents or frauds.
- f) Complying with any legal, governmental or regulatory requirement or for use by our lawyers in connection with any legal proceedings e.g. responding to court orders.

5. Do we retain any of your personal data?

HFCB Group Limited or its Subsidiary Companies shall not retain your data any longer than necessary. The retention shall be determined by the purpose for which the data was collected and whether that purpose has been fulfilled unless as circumstances may dictate including:

- Applicable legal and regulatory requirements,
- Consent provided by you,
- For legitimate lawful purposes or
- For historical and reporting purposes.

6. With whom will we share/disclose your personal data?

We will not share or disclose any of your information except in accordance with applicable laws and regulations. HFCB Group Limited or its Subsidiary Companies may share or disclose your information to:

- a) Our debt recovery agencies for purposes of debt recovery.
- b) Legal, regulatory or any other statutory authorities for purposes of complying with or responding
- c) to a demand by the said authorities.
- d) Credit reference agencies/bureaus.
- e) Various government databases to comply with applicable regulatory requirements. e.g. IPRS
- f) Our subsidiaries, partners for purposes of fulfilling our obligations to you.

7. Commercial use of your personal data

We will continually introduce new products or services, upgrade existing ones and introduce new ways of serving you. In this regard, we may need to communicate such developments with you.

HFCB Group Limited or its Subsidiary Companies will however seek your consent to opt-in to receive such updates via our various communication channels.

To opt-out of these communications, you may:

- Call to place your OPT-OUT request on the phone numbers provided under Our Contacts section.
- Write an email to customer.service@hfcgroup.co.ke or mybank@hfcgroup.co.ke
- Use the opt-out options on our various channels.
- Use the request form that is available on our website, through the link: https://www.hfcgroup.co.ke/documents/data_privacy_docs

8. KYC Verification and Data Enhancement Activities

As part of our legal and regulatory obligations, we may process and verify customer information to maintain accurate and complete Know Your Customer (KYC) records and to support anti-money laundering and customer due diligence requirements.

To support these activities, we may use authorized third-party service providers and official data sources to validate or retrieve customer information where records are incomplete, outdated, or require verification.

The information processed for these purposes may include but is not limited to:

- Customer identification information;
- National identification numbers;
- Company registration information;
- KRA PIN information;
- Director and beneficial ownership information associated with corporate entities.

We only process information necessary for KYC verification, regulatory compliance, fraud prevention, and customer due diligence purposes.

Your information may be shared with carefully selected service providers acting on our instructions and subject to confidentiality and data protection obligations.

We implement safeguards to protect your information, including controlled access, contractual protection, retention limits, and secure handling procedures.

Where temporary processing by third-party providers is required, the information is retained only for the period necessary to complete the verification activity and is deleted in accordance with applicable retention and disposal requirements.

You have rights under applicable data protection laws, including the right to request access to your personal data, request correction of inaccurate information, and raise complaints regarding how your information is processed.

9. Digital Banking Disclosure

a) Introduction

This Customer Privacy Notice and Digital Banking Disclosure ("Notice") explains how the Bank collects, uses, processes, stores, and protects customer personal information in connection with digital banking services and related financial products.

The Bank is committed to safeguarding customer information and processing personal data in a lawful, secure, and transparent manner in accordance with applicable banking, data protection, anti-money laundering ("AML"), and regulatory requirements.

b) Information We Process

The Bank may collect and process the following categories of personal information:

Personal identification information

Contact information

Financial and transaction information

Device identifiers and digital access information

Card and payment information

Know Your Customer ("KYC") documentation

AML screening and compliance information

Account and transaction history

c. Sources of Information

Customer information may be obtained from:

- Information provided directly by customers
- Internal banking and operational systems
- Government and identity verification databases
- AML and sanctions screening systems
- Fraud prevention and risk management systems

d. Purpose of Processing

The Bank processes customer information for purposes including, but not limited to:

- Provision of digital banking and financial services
- Transaction processing and account management
- Customer onboarding and identity verification
- Customer authentication and access management
- Fraud detection, prevention, and investigation
- AML screening and regulatory compliance
- Protection of customer accounts and banking systems
- Service improvement and operational efficiency
- Fulfillment of legal, audit, and compliance obligations

e. Data Sharing and Processing

Customer information may be processed through authorized banking infrastructure and service platforms, including:

- Core banking systems
- Fraud management and monitoring systems
- AML and compliance screening systems
- Card management and payment processing systems
- Government verification and regulatory systems
- Approved third party vendors

All processing activities are conducted under controlled, secure, and authorized conditions and are subject to applicable confidentiality and security obligations.

f. Data Retention

Customer information is retained within secure and encrypted banking systems for as long as necessary to:

- Provide banking services
- Meet operational requirements
- Comply with legal and regulatory obligations
- Support audit, compliance, and risk management activities
- Resolve disputes and enforce contractual obligations
- Retention periods are determined in accordance with applicable laws, regulations, and internal policies.

g. Customer Rights

Subject to applicable law and regulatory requirements, customers may have the right to:

- Request access to personal information held by the Bank
- Request correction or update of inaccurate information
- Raise complaints or concerns regarding data handling
- Exercise applicable privacy and data protection rights

Customers may exercise these rights by submitting a request through the Bank's official communication channels or by contacting the Data Protection Officer ("DPO") at: Email: dpo@hfcg.co.ke

Requests may be subject to identity verification and applicable legal or regulatory limitations.

h. Security Safeguards

The Bank maintains administrative, technical, and organizational safeguards designed to protect customer information against unauthorized access, disclosure, alteration, misuse, or loss.

Security measures may include:

- Data encryption

Multi-factor authentication
Role-based access controls
Continuous system monitoring
Security assessments and testing
Fraud detection and monitoring controls

i. Regulatory Compliance

The Bank processes customer information in compliance with applicable banking regulations, AML obligations, data protection laws, and supervisory requirements.

j. Updates to This Notice

The Bank may update or amend this Notice from time to time to reflect changes in legal, regulatory, operational, or technological requirements. Updated versions may be made available through the Bank's digital channels or other appropriate communication methods.

10. Use of Behavioral Analytics & Personalization Technologies

In order to improve your experience on our channels (including our mobile applications branch channel and websites), enhance our offering and provide you with more relevant solutions, we leverage a customer engagement and analytics platform operated by a licensed third-party service provider. This platform helps us understand customer interaction with our channels (both digital and branch channels) and in turn enables us to deliver timely and personalized communication.

a) What Data do we collect through this Technology?

We may collect and process the following categories of personal data:

- Device information (such as device ID, operating system and app version).
- Usage and behavioral data (pages viewed, buttons clicked, session duration, navigation patterns).
- Event-level data (activities, transactions initiated, feature usage).
- Communication engagement data (such as whether you opened, read or interacted with messages we send).
- Optional identifiers such as email address or phone number, where you have provided these during account creation, login, or communication consent.

b) Purpose of Processing

We process the above information for the following purposes:

- To analyze how customers use our platforms.
- To improve product performance, usability and customer satisfaction.
- To segment users into relevant groups to tailor services and communications.
- To deliver personalized notifications, offers, alerts and campaigns across channels such as SMS, email, push notifications and in-app messages.
- To measure the effectiveness of our communication and service interactions.
- To enhance customer support, fraud alerts and service-related messages.
- The platform processes this data strictly according to our documented instructions as the Data Controller.

c) Use of Third-Party Data Processors

We engage reputable third-party service providers to process this data on our behalf. These providers:

- Act strictly as Data Processors, following our written instruction.
- Implement strong security measures including encryption, access controls and independently audited SOC 2 security controls.
- Do not sell, share or use your data for any purpose other than providing services to us.

d) Cross-Border Data Transfers

Some of the systems used to process your data may be hosted in secure cloud infrastructure located outside Kenya. Where this is the case, we ensure that:

- The receiving country or provider offers comparable protection to Kenyan data protection law.
- Appropriate contractual safeguards are in place.

e) Your Rights Regarding This Processing

You retain all rights granted under the Data Protection Act, including the right to:

- Access your personal data
- Request the correction or deletion
- Request for erasure of personal data
- Request for rectification of personal data
- Withdraw consent at any time
- Request restricted processing or objection to processing

To exercise these rights please utilize the data privacy documents available on our website, through the link: https://www.hfcbgroupp.co.ke/documents/data_privacy_docs

f) **Our Legal Basis for Processing Your User Data**

The legal basis for processing your data through this technology shall be based on your consent. To opt-out, please utilize the Request For Restriction, Objection Or Consent Withdrawal Form that is available on our website, through the link: https://www.hfcbgroupp.co.ke/documents/data_privacy_docs

11. Access to or update your personal data

Access to personal data shall be provided upon visit or formal request to the bank and requisite data update/modification forms provided to capture any personal data update requests. Modification of this data shall be done by the bank according to the established internal processes that aim to give assurance on integrity and accuracy of personal data.

12. Safeguarding and protecting your personal data.

HFCB Group Limited and Its Subsidiary Companies have put in place various operational and technical controls to safeguard your data from unauthorized access or modification. We are also continually enhancing our controls in line with the ever-evolving threat landscape.

13. Handling your sensitive personal data

HFCB Group Limited or Its Subsidiary Companies shall not collect or process your sensitive personal data except as necessary to carry out the activities prescribed in section 4 above.

14. Transfer of your personal data outside Kenya

HFCB Group Limited or Its Subsidiary Companies may from time to time transfer your personal data outside Kenya as circumstances may allow in fulfilment of its obligations. This shall be done with the requisite and appropriate approvals and safeguards on the data.

15. Your rights.

Your rights as spelt out in the data protection laws include the below. Please note that these are subject to legal, regulatory and contractual exceptions and we reserve a right to override exercise of your rights where there is a legitimate reason, legal or regulatory requirement to do so as may be applicable.

- a) Right to be informed of the use to which your personal data is to be put.
- b) Right to access your personal data.
- c) Right to object to the processing of all or part of your personal data.
- d) Right to correct false or misleading data about you.
- e) Right to delete false or misleading data about you.
- f) Right to erase your personal data that we are no longer authorized to retain, irrelevant, excessive or obtained unlawfully.
- g) Right to be informed that we are collecting personal data about you.
- h) Right to withdraw your consent to processing of your personal data.
- i) Right to request restricted processing of your personal data.
- j) Right to request transfer of your personal data.
- k) Right to not be subject to a decision based on automated processing; subject to such automated processing producing legal effects that affect you.
- l) Right to decline use of your personal data for commercial purposes.
- m) Right to be informed about a breach to your personal data unless your identity cannot be established in that breach.
- n) Right to lodge a complaint with the office of the Data Commissioner if you feel aggrieved by a decision made by HFCB Group Limited or any of its Subsidiary Companies using the prescribed mechanisms in the data protection laws.

16. Our Contacts

Our contact details are:

HFCB GROUP LIMITED,

Rehani House, Kenyatta Avenue / Koinange Street

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

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

OR

HFCB,

Rehani House, Kenyatta Avenue / Koinange Street

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

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

OR

HFCB BANCASSURANCE INTERMEDIARY LIMITED,

Rehani House, Kenyatta Avenue / Koinange Street

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

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

OR

HFCB DEVELOPMENT & INVESTMENT LIMITED,

Rehani House, Kenyatta Avenue / Koinange Street

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

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

17. Data Protection Officer (DPO) Contacts

Email Address: dpo@hfcbgroup.co.ke Telephone: 0709438308

18. Guidelines for lodging complaints and exercising data subject rights

18.1. 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.

18.2. 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.

18.3. Data Subject Rights

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

18.4. Submission Channels

Requests and complaints can be submitted through the following channels:

- Email: dpo@hfcbgroup.co.ke

- Postal Mail:

Data Protection Office

P.O Box 30088 – 00100, Nairobi, Kenya

- Phone: +254 709438000, 709438888
- In-person: HFCB Group Limited or Its Subsidiary Companies' Head Offices or nearest branch
- Use the request form that is available on https://www.hfcbgroup.co.ke/documents/data_privacy_docs

18.5. 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.

18.6. 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.

18.7. Escalation and appeals

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

18.8. Record keeping

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