



中国电信(肯尼亚)有限公司
China Telecom (Kenya) Limited

CHINA TELECOM (KENYA) LIMITED
Privacy Policy

Table of Contents

1. Introduction	3
2. Definitions.....	3
3. Scope of the Policy	4
4. Policy Statement	4
5. Processing of Personal Data	4
6. Data Subject Rights	7
7. Principles for lawful processing.....	9
8. Direct Marketing	13
9. Data Protection Impact Assessment.....	13
10. Personal Data Breaches	13
11. Automated Individual Decision Making	14
12. Child's Privacy	14
13. Implementation and Enforcement Guidelines	14
14. Review Frequency.....	15

1. INTRODUCTION

China Telecom (Kenya) Limited (“We”, “Us”, “Our”, “CTK”) is committed to manage all Personal Data that we hold in a fair, responsible, secure and sensible way and in accordance with the applicable data protection laws and regulations. We carefully use and safeguard all Personal Data which belongs to our Data Subjects.

We aim to strike a fair balance between the rights of Data Subjects and the ability of organisations we contract with to handle Personal Data for their legitimate purpose concerning their business activities. We take steps to ensure that our business processing and operations are designed with privacy requirements in mind: we closely observe any restrictions and standards concerning the security, use and disclosure of all Personal Data.

This Policy establishes our approach to protect and manage Personal Data when we Process Personal Data for our own purposes and/or on behalf of our customers. The requirements within this Policy are primarily based upon the DPA (as defined below), a key piece of legislation covering security and privacy of Personal Data in Kenya.

1.1. **Contact Details**

China Telecom (Kenya) Limited

Registered address: The Atrium, 1st Floor, Office No. 06, Junction of Chaka and Lenana Road, Kilimani, Nairobi, Kenya

Contact person 1: **Joyce Mbithe Kinyanjui**

Telephone Number: +254 (0) 726415263

Email address: ctmealegal@chinatelecomglobal.com

Contact person 2: **Priya Ratanjee**

Telephone Number: **+27 (0)11 656 3196**

Email address: ctmealegal@chinatelecomglobal.com

2. DEFINITIONS

2.1. “**Consent**” means the voluntary, specific and informed expression of will in terms of which permission is given for the processing of Personal Data;

2.2. “**Data Subject**” means a natural person who can be identified directly or indirectly by reference to an identifier such as name, identification number, location data, an online identifier or one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity. (In this policy referred to as “**You**” or “**Your**”)

2.3. “**Direct Marketing**” means approaching a Data Subject either in person or by mail or electronic communication, for the direct or indirect purpose of promoting, or selling them a product or service, of requesting a donation;

2.4. “**DPA**” means the Data Protection Act, No. 24 of 2019, Laws of Kenya;

2.5. “**DPGR**” means the Data Protection (General) Regulations, 2021 (Legal Notice NO. 263) Laws of Kenya “

2.6. “**Personal Data**” means any information relating to an identified or identifiable natural person;

- 2.7. **“Processing, Process”** means an operation or activity, whether by manual or automatic means, concerning Personal Data;
- 2.8. **“Services”** means services offered by China Telecom (Kenya) Limited within its nature and conduct of its business; and
- 2.9 **“Sensitive Personal Data”** means all information relating to a natural person's conscience, religious or philosophical beliefs, genetic data, property details, race, social or ethnic origin, trade union membership, political persuasion, health or sex life, sexual orientation, marital status, family details including names of the person's children, parents, spouse or spouses, biometric information or criminal behaviour.

3. SCOPE OF THE POLICY

The Policy applies to all employees and directors of CTK affiliates, contractors and business partners. The provisions of the Policy are applicable to both on and off-site Processing of Personal Data

4. POLICY STATEMENT

We collect and use Personal Data of Data Subjects, including but not limited to Personal Data pertaining to prospective and current customers, vendors, and independent contractors to operate and carry out our business effectively.

The purpose of this Policy, therefore, is to set out a framework to satisfy the standards contained in DPA and to provide an adequate level of protection for the usage of all Personal Data that we use and collect in Kenya, as well as for Personal Data that we transfer out from Kenya to other countries.

CTK regards that the lawful and appropriate Processing of all Personal Data to be crucial to the success of our service delivery and essential for maintaining confidence between CTK and those individuals and entities we deal with. CTK therefore fully endorses and adheres to the principles of DPA.

5. PROCESSING OF PERSONAL DATA

5.1. Purpose of Processing

CTK uses Personal Information we hold only for the following purpose:

- a. Keeping of accounts and records for the operation of our business and legal and statutory obligations;
- b. Complying with legal and regulatory requirements;
- c. Providing services to customers or business partners;
- d. Provide customers with services offered and requested;
- e. Providing prospects and customers with CTK related marketing material due to their past interaction and use of CTK's services;
- f. Office management and physical security of premises;
- g. For statistical, historical and/or reporting purposes;
- h. For Cybersecurity Measures;



- i. For business transfers: We may use Your Personal Data to evaluate or conduct a merger, divestiture, restructuring, reorganization, dissolution, or other sale or transfer of some or all of Our assets, whether as a going concern or as part of insolvency or similar proceeding, in which Personal Data held by Us is among the assets transferred.

CTK will always ask Data Subjects for their permission before using any Personal Data for other purposes that has not been previously disclosed (see above clause 5.1 (a-i)) and/or such other purpose is unrelated to the operations/services/use in the ordinary course of business of CTK and/or consent was not given for such other purpose and/or there is no other legal basis for such Processing.

5.2. Types of Information Collected by CTK

- a) CTK collects Personal Data about subscribers of China Telecom services or users connected through the enterprise network services in a manner through Supplier and Customer Profile Forms, Contracts/Agreements, email signatures etc., such methods are not exclusive (collectively to be referred to as “**Manner**”). This information includes, inter alia, subscribers' registration and contact details (including the **person's name, business email address, business address and telephone number**).
- b) CTK collects contact details of those that work for or represent our enterprise customers (customers that use CTK's enterprise network services) in such Manner. This information includes, inter alia, **a person's name, email address, telephone number, company and job title**.
- c) CTK collects contact details of those that work for or represent our wholesale customers (customers that use CTK's wholesale network services) in such Manner. This information includes, inter alia, **a person's name, email address, telephone number, company and job title**.
- d) CTK collects business contact information of those that work for or represent other companies with whom CTK has a relationship, such as vendors and business partners in such Manner. This information includes, inter alia, **names of contact persons; name of legal entity; physical and postal address and contact details; email address, financial information; registration number; founding documents; tax related information; authorised signatories; beneficiaries; ultimate beneficial owners; shareholding information;** CTK collects biometric information, marital and family status of its employees and health data strictly relating to Covid-19 in the interests of lessening or preventing serious threat to life, health or safety of a Data Subject, or to public health and safety.

5.3 Sources of Personal Data

We obtain Personal Data directly from You unless where:

- a. the data is contained in a public record;
- b. You have deliberately made the Personal Data public;
- c. You have consented to the collection from another source;
- d. The Data Subject has an incapacity and the guardian appointed has consented to the collection from another source;
- e. The collection from another source will not prejudice Your interests;

- f. The collection of the Personal Data from another source is necessary for prevention, detection, investigation, prosecution and punishment of a crime, for enforcement of law that imposes a pecuniary penalty or for the protection of the interests of the Data Subject or another person.

Where Personal Data is collected indirectly as per paragraph (a) to (f) above, We shall inform you within fourteen (14) days of such collection.

In so far as is practicable and before collection of Your Personal Data We will notify You:

- a. of Your data subjects' rights;
- b. that Your data is being collected;
- c. the purpose for which the Personal Data is being collected;
- d. the third parties with whom the Personal Data shall be shared with including the safeguards adopted;
- e. the contacts of data controller/data processor;
- f. description of technical and organizational security measures adopted to ensure the safety of the data;
- g. the data being collected pursuant to any law and whether such collection is voluntary or mandatory; and
- h. consequences, if any where You fail to provide the data.

5.4. Categories of Recipients for Processing the Personal Data

The Personal Data collected is used only by CTK and our employees for our organisational purposes and services. We will only share Personal Data to recipients outside of CTK in instances where it is necessary to fulfil an obligation or service. CTK may supply the Personal Data to any party to whom CTK may have assigned or transferred any of its rights or obligations under any agreement, and/or to service providers ("**Service Providers**") who render the following services:

- a. Capturing and organising of data;
- b. Storing of data;
- c. Sending of emails and other correspondence to customers;
- d. Conducting due diligence or background checks; or
- e. More generally, performing any services, under the instructions of CTK, where processing the Personal Data is necessary to perform such service.

Such Service Providers may include, inter alia, Auditors, Legal Partners / Law Firms, Human Resource agency, Marketers and Information Technology contractors.

5.5. Actual or Planned Transborder Flows of Personal Data

Personal Data may be transmitted trans-border to CTK'S authorised dealers, its suppliers in other countries, or our affiliated companies. Personal Data may be stored in data servers hosted in a third country outside Kenya.

CTK will take necessary steps in such circumstances to ensure that services providers and third-party operators are bound by applicable laws or binding agreements that provide a level of protection and uphold principles for reasonable and lawful Processing of Personal Data as contemplated by DPA.

CTK shall not transfer any Sensitive Personal Data in its possession without the prior consent of the Data Subject.

CTK undertakes to ensure that where there is transborder flow/transfer of Personal Data there is compliance with the appropriate standards of data protection as set in the DPA in order to ensure the security of Data Subjects' Personal Data. The foundational requirement is for CTK to secure integrity and confidentiality of Personal Data in our possession and control by taking all appropriate, reasonable technical and organizational measures.

5.6. Retention of Personal Data Records

- a. Personal Data will only be retained for as long as necessary for CTK to carry out the function, legal obligation or services. Personal Data no longer required for the purposes of complying with a legal obligation, performing a contractual relationship or rendering services or after completion of services, will be destroyed. Personal Data will be retained and destroyed in accordance with the terms of CTK Data Retention and Destruction Policy.
- b. CTK however may maintain de-identified information for statistical purposes.

5.7. General Description of Information Security Measures

CTK employs up-to-date technology to ensure the confidentiality, integrity and availability of the Personal Data under its care. Measures include, inter alia:

- a. Firewalls
- b. Virus protection software and update protocols
- c. Logical and physical access control;
- d. Secure setup of hardware and software making up the IT infrastructure;
- e. Outsourced service providers who process Personal Data on behalf of CTK are contracted to implement security controls.

6. DATA SUBJECT RIGHTS

Data Subjects have the right to:

- **Request access to Personal Data.** Once We receive and confirm Your request, We will disclose to You:
 - The categories of Personal Data We collected about You.
 - The purpose of processing the Personal Data.
 - The categories of third parties with whom We share the Personal Data.
 - Categories of sources of collection of the Personal data.
 - The period within which the Personal Data may be stored or the criteria of determining that period.

- **Request correction of the Personal Data** that We hold about You. You have the right to have any incomplete or inaccurate information We hold about You corrected.
- **The right to say no to the commercial use of the Personal Data (opt-out).** You have the right to direct Us to not process Your Personal Data for commercial use.
- **Object to processing of Your Personal Data.** This right exists where We are relying on a legitimate interest as the legal basis for Our processing and if there is something about Your particular situation, which makes You want to object to our processing of Your Personal Data on this ground, You also have the right to object where We are processing Your Personal Data for direct marketing purposes.
- **Restrict the Processing of Your Personal Data.** You have a right to request the restriction in the processing of Your Personal Data.
- **Request erasure of Your Personal Data.** You have the right to ask Us to delete or remove Personal Data when there is no good reason for Us to continue processing it. We may deny Your deletion request if retaining the information is necessary for Us
 - To exercise the right of freedom of expression and information;
 - To comply with a legal obligation;
 - For performance of a task carried out in the public interest or in exercise of official authority;
 - For achieving purposes in the public interest, scientific research, historical research or statistical purposes where erasure is likely to render impossible or seriously impair the achievement of that processing; or
 - For the establishment, defence or exercise of a legal claim.
- **Request the transfer of Your Personal Data.** We will provide to You, or to a third-party You have chosen, Your Personal Data in a structured, commonly used, machine-readable format.
- **Withdraw Your consent.** You have the right to withdraw Your consent on using your Personal Data.
- **The right to notice.** You have the right to be notified of which categories of Personal Data are being collected and the purposes for which the Personal Data is being used.
- **The right not to be discriminated against.** You have the right not to be discriminated against for exercising any of Your rights.

6.1 EXERCISE OF DATA SUBJECT'S RIGHTS

You may exercise Your rights of access, rectification, deletion, opposition, restriction and data portability by contacting the Information Officer or the Deputy Information Officer through the prescribed forms under the DPGR. Please note that we may ask You to verify Your identity before responding to such requests.

If You make a request, We will try our best to respond to You as soon as possible and where your request is denied we will give reasons for such refusal and/or denial. CTK will respond within seven (7) days to a request of access to data, within fourteen (14) days to the requests for the erasure or rectification of data, objection or restriction to the processing of data and within thirty (30) days to a request for data portability.

No fees will be required to be paid to Us in exercise of Your rights except in the exercise of the right to transfer your Personal Data or data portability where a reasonable fee will be charged taking into account the costs for actualizing the request.

7. PRINCIPLES FOR LAWFUL PROCESSING

DPA is implemented by abiding to certain principles for lawful processing (“**Principles**”). CTK shall abide by these Principles in all its Processing activities.

- **Accountability**
- **Lawful Grounds of Processing Personal Data**
- **Lawful, transparency and fairness**
- **Purpose Limitation**
- **Accuracy**
- **Integrity, confidentiality and availability**
- **Storage Limitation**
- **Data Minimization**

Further information of the Principles is detailed as follows:

7.1. Accountability

CTK shall ensure that all Personal Data is processed according to its the purpose and means under the required consent or legal basis. CTK shall remain liable, even if it has outsourced its Processing activities to a third party.

7.2. Lawful grounds of Processing Personal Data

The Processing of Personal Data is only lawful if the information is adequate, relevant and not excessive to justify its purpose. CTK may only process Personal Data if one of the following grounds of lawful Processing exists:

- a. **Consent:** The Data Subject consents to the Processing.
- b. **Performance of a contract:** Processing is necessary for the conclusion or performance of a contract with the Data Subject.
- c. **Legal Obligation:** Processing complies with a legal responsibility imposed on CTK.
- d. **Vital interest of the Data Subject:** Processing protects a vital interest of the Data Subject or of another natural person.
- e. **Legitimate Interest of CTK or Third Party:** Processing is necessary for pursuance of a legitimate interest of CTK, or a third party to whom the information is supplied.
- f. **Public interests:** Processing Personal Data is related to a task that is carried out in the public interest or in the exercise of official authority vested in the CTK.
- g. For the purpose of historical, statistical, journalistic, literature and art or scientific research.

CTK may only process Sensitive Personal Data under the following circumstances:

- a. the Data Subject has consented to such Processing.
- b. the processing is necessary in protecting vital interests of the data subject or another person where the data subject is unable to give consent.
- c. the processing is for purpose of protecting public interests in the area of public health.
- d. processing is necessary for carrying out the obligations and exercising specific rights of the CTK or data subject.
- e. the S Sensitive Personal Data was deliberately made public by the Data Subject.
- f. processing is necessary for the establishment of a right or defence in law.

7.3 Lawfulness, transparency and fairness

CTK shall obtain Personal Data fairly and shall not mislead or deceive persons as to how their Personal Data will be used. CTK shall be transparent about the way in which Personal Data is collected and used. When collecting a Data Subject's Personal Data, CTK shall notify that Data Subject, explaining the key aspects of the ways in which Personal Data is handled.

CTK shall take reasonable steps to ensure that the Data Subject is made aware of:

- a. What Personal Data is collected, and the source of the information;
- b. The purpose of collection and Processing;
- c. Whether the provision of Personal Data is voluntary or mandatory, and the consequences of failure to provide such information;
- d. Whether collection of Personal Data is required by law; and
- e. Whether the Personal Data shall be shared with any third party.

7.4. Purpose Limitation

CTK shall only process Personal Data for the specific purposes as set out and defined above at clause 5.1.

CTK will specify the purpose of Processing at the time of data collection. Any subsequent Processing of such information collected shall be limited to the fulfilment of those specified purposes only.

Personal Data must only be obtained and stored in accordance with the purposes specified in privacy notices/Consents, which include, inter alia:

- Staff Administration (for example payroll, provision of benefits, performance reviews, training);
- Advertising, Marketing & Public Relations (for example, keeping customers and candidates informed about CTK's services);
- Service delivery (for example, account details, invoices and call records); and
- Accounts & Records (for example staff planning and resource allocation across CTK and keeping records of dealings with customers).

If Personal Data is processed for any additional purposes which may not fall within the terms of a privacy notice, such additional purposes should first be reported to the Deputy Information Officer, subject to approval before any Processing occurs.

Further processing of Personal Data will be compatible with the original purpose of collection.

7.5. Accuracy

CTK shall take reasonable steps to ensure that Personal Data is complete, accurate, not misleading and updated. CTK shall periodically review Data Subject records to ensure that the Personal Data is still valid and correct.

Employees of CTK should as far as reasonably practicable follow the guidance below when collecting Personal Data

- a. Personal Data should be dated when received;
- b. A record should be kept of where the Personal Data was obtained;
- c. Changed to information records should be dated;
- d. Irrelevant or unneeded Personal Data should be deleted or destroyed; and
- e. Personal Data should be stored securely, either on a secure electronic database or in a secure physical filing system.

7.6 Integrity, Confidentiality and Availability

7.6.1 Security Safeguards

Personal Data shall be protected by reasonable security safeguards against such risks as loss or unauthorised access, destruction, use, modification or disclosure of data

CTK shall ensure that the integrity and confidentiality of all Personal Data in its possession, by taking reasonable steps to:

- a. Identify all reasonably foreseeable risks to information security; and
- b. Establish and maintain appropriate technical and organizational safeguards against such risks.

7.6.1.1 Written records

- a. Personal Data records shall be kept in locked cabinets, or safes;
- b. When not in use, Personal Data records shall not be left unattended in areas where non-staff members may access them;
- c. CTK shall implement and maintain a “Clean Desk Policy” where all employees shall be required to clear their desks of all Personal Data when leaving their desks for any length of time and at the end of the day;
- d. Personal Data which is no longer required shall be disposed of by shredding; and
- e. Any loss or theft of, or unauthorised access to, Personal Data shall be immediately reported to the Information Officer.

7.6.1.2 Electronic Records

- a. All electronically held Personal Data shall be saved in a secure database;
- b. As far as reasonably practicable, no Personal Data shall be saved on individual computers, laptops or hand-held devices;
- c. All computers, laptops and hand-held devices shall be protected with a password or fingerprint scan, with the password being of reasonable complexity and changed frequently; CTK shall implement and maintain a “Clean Screen Policy” for all employees, where the Computer workstations, Laptops, tablets and other hardware devices must be locked with a password for password protection when the desk is unoccupied for any length of time and to log off at the end of the day;
- d. Electronic Personal Data which is no longer required shall be deleted from the individual laptop or computer and the relevant database. The employees of CTK shall ensure that the information has been completely deleted and is not recoverable; and

- e. Any loss or theft of computers, laptops or other devices which may contain Personal Data shall be immediately reported to the Information Officer, who shall notify the IT department, who shall take all necessary steps to remotely delete the information, if possible.

7.7 Storage Limitation

CTK will retain Your Personal Data only for as long as is necessary for the purposes set out in this Privacy Policy. We will retain and use Your Personal Data to the extent necessary to comply with our legal obligations (for example, if we are required to retain your data to comply with applicable laws), resolve disputes, and enforce our legal agreements and policies.

Where Personal Data is no longer necessary CTK shall ensure the deletion and destruction of such data.

Documents may be destroyed after the termination of the retention period specified in the Retention Schedule, or as determined by CTK from time to time.

Each department is responsible for attending to the destruction of its documents and electronic records, which must be done on a regular basis as per the Retention Schedule. Files must be checked to make sure that they may be destroyed and to ascertain if there are important original documents in the file. Original documents must be returned to the holder thereof, failing which, they should be retained by CTK pending such return.

The documents must be made available for collection by the Shred-It, or other approved document disposal company.

Deletion of electronic records must be done in consultation with the IT Department, to ensure that deleted information is incapable of being reconstructed and/or recovered.

7.8 Data Minimization

CTK will only collect Personal Data necessary for the relevant purposes and will anonymize or delete data that is no longer necessary for the purpose.

8. DIRECT MARKETING

All Direct Marketing communications shall contain CTK's details, and an address or method for the Data Subject to opt-out of receiving further marketing communication.

8.1.1. Existing Customers

Direct Marketing by electronic means to existing customers is only permitted:

- a. If the customer's details were obtained in the context of a sale or service; and
- b. For the purpose of marketing the same or similar products;
- c. The customer must be given the opportunity to opt-out of receiving Direct Marketing on each occasion of Direct Marketing and how to opt-out anytime thereafter.

8.1.2. Consent

CTK may send electronic Direct Marketing communication to Data Subjects who have consented to receiving it. CTK may send a reconfirmation of consent email to the Data Subject within that email to

allow two or more reminders before no contact is made to the Data Subject. CTK will remind the Data Subject of his/her/its right to withdraw consent to receive anytime.

8.1.3. Consent Record Keeping

CTK shall keep record of:

- a. Date of Consent
- b. Wording of the Consent
- c. Who obtained the Consent
- d. Proof of opportunity to opt-out on each marketing contact
- e. Record of opt-outs

8.1.4 At no time shall CTK use any Sensitive Personal Data within its possession for purpose of direct marketing.

9. DATA PROTECTION IMPACT ASSESSMENT

Data Protection Impact Assessment (DPIA) means assessment of the impact of the envisaged processing operations on protection of Personal Data.

CTK acknowledges that under the DPA it has an obligation to conduct a DPIA where the processing operations of Personal Data are likely to result to high risk to the rights and freedoms of Data Subjects, that is it has a responsibility to assess the risks that may arise from the conduct of the processing operations and devise measures to mitigate the risks.

CTK shall ensure to conduct a Data Protection Impact Assessment where the processing operations of Personal Data are likely to result to high risk to the rights and freedoms of the Data Subjects.

CTK will conduct Data Protection Impact Assessment where the processing operations involve:

- a. automated individual decision making activities
- b. Processing biometric or genetic data;
- c. processing sensitive Personal Data; or
- d. large scale processing of Personal Data

10. PERSONAL DATA BREACHES

A personal data breach is a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed.

CTK has a response plan to address any personal data breaches that exposes a real risk of harm to the Data Subject.

11. AUTOMATED INDIVIDUAL DECISION MAKING

Automated Individual Decision Making is any decision made by automated means without any human involvement.

Profiling is a form of automated processing of Personal Data consisting of the use of Personal Data to evaluate certain personal aspects relating to a natural person, in particular to analyse or predict aspects concerning that natural person's race, sex, pregnancy, marital status, health status, ethnic social origin, colour, age, disability, religion, conscience, belief, culture, dress, language or birth; personal preferences, interests, behaviour, location or movements.

CTK does not subject Data to Automated Decision Making and Profiling, but will where subjecting Personal Data to Automated Individual Decision Making and Profiling ensure that:

- a. the Data Subject is duly informed;
- b. it provides meaningful information about the logic involved;
- c. transparency, fairness and that the rights for a Data Subject to oppose to the profiling and specifically the profiling for marketing are present;
- d. the conduct of a Data Protection Impact Assessment in relation to the automated individual decision making and profiling;
- e. it explains the significance and envisaged consequences of the processing;
- f. there's prevention of errors;
- g. It uses appropriate mathematical or statistical procedures;
- h. It puts appropriate technical and organisational measures in place to correct inaccuracies and minimise the risk of errors;
- i. It processes personal data in a way that eliminates discriminatory effects and bias; and
- j. that a Data Subject can obtain human intervention and express their point of view.

12. CHILD'S PRIVACY

Our Services do not address any minor. We **do not** knowingly collect personally identifiable information from any minor. If You are a parent or guardian and You are aware that Your child has provided Us with Personal Data, please contact Us. If We become aware that We have collected Personal Data from any minor without verification of parental consent, We take steps to remove that information from Our servers.

13. IMPLEMENTATION AND ENFORCEMENT GUIDELINES

13.1. Training & Dissemination of Information

This Policy has been put in place throughout CTK and communicated to its employees and directors, vendors and partners. Training on the Policy and DPA will take place with all affected employees.

All new employees will be made aware at induction, or through training programmes, of their responsibilities under the terms of this Policy and DPA.

Modifications and updates to data protection and information sharing policies, legislation, or guidelines will be brought to the attention of all staff.

13.2 Enforcement

CTK relies on all its employees, contractors and partners to comply with all applicable data protection laws and regulations. Failure to comply with this Policy or any of the supporting and complementing policies, contracts, and/or procedures must be construed as misconduct and may result in one or more of the actions mentioned below:

- (a) The restriction, suspension or termination of access to the network, information, information assets and facilities, including immediate suspension of his or her or its access or rights pending further investigations;
- (a) The institution of legal proceedings by CTK, including but not limited to criminal prosecution under applicable laws that may prevail in Kenya from time to time; and
- (b) The taking of disciplinary steps against the user, which may lead to suspension or dismissal.

14. REVIEW FREQUENCY

This Policy will be subject to a regular review which will take place annually.