MORINGA

Discover · Grow · Transform

Data Protection Policy

Introduction

This Policy sets out the obligations of MORINGA SCHOOL LIMITED ('Moringa'), a company registered in Kenya, whose registered office is at **Ngong Lane, Ngong Lane Plaza, 1st Floor, Nairobi, Kenya** ("the Company") regarding data protection and the rights of customers, employees, suppliers, visitors and any other individuals whose personal data is processed by **Moringa** ("data subjects") in respect of their personal data under Data Protection Law. "Data Protection Law" means all legislation and regulations in force from time to time regulating the use of personal data including, but not limited to, the Kenya Data Protection Act, 2019 (the Act), The Data Protection General Regulations 2021, The Data Protection (Registration of Data Controllers and Data Processors) 2021, The Data Protection (Complaints Handling and Enforcement Procedures) Regulations 2021 (collectively, "the Regulations). The Act and the Regulations are collectively, the Data Protection Law, and any other regulations made under the Act.

This Policy is in compliance with **Regulation 23(1) of The Data Protection General Regulations 2021** and sets the Company's obligations regarding the collection, processing, transfer, storage, and disposal of personal data. The procedures and principles set out herein must be followed at all times by the Company, its employees, agents, contractors, or other parties working on behalf of the Company.

Definitions

“consent”	means the consent of the data subject which must be a voluntarily be given, specific, informed, and unambiguous indication of the data subject’s wishes by which they, by a statement or by a clear affirmative action, signify their agreement to the processing of personal data relating to them;
“data controller”	" means a natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purpose and means of processing of personal data. For the purposes of this Policy, the Company is the data controller of all personal data relating to customers, employees, suppliers, visitors used in our business for our commercial purposes.
“data processor”	means a natural or legal person or organisation which processes personal data on behalf of a data controller
“data subject”	means an identified or identifiable natural person who is the subject of personal data.
“personal data”	means any information relating to an identified or identifiable natural person such as a name, identification number, location data, an online identifier, or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural, or social identity of that data subject.
“personal data breach”	means 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.

“processing”	means any operation or set of operations performed on personal data or sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction
“pseudonymisation”	means the processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organisational measures to ensure that the personal data is not attributed to an identified or identifiable natural person.
“sensitive personal data”	means data revealing the natural person's race, health status, ethnic social origin, conscience, belief, genetic data, biometric data, property details, marital status, family details including names of the person's children, parents, spouse or spouses, sex or the sexual orientation of the data subject

Scope

The Company is committed not only to the letter of the law, but also to the spirit of the law and places high importance on the correct, lawful, and fair handling of all personal data, respecting the legal rights, privacy, and trust of all individuals with whom it deals. The Data Protection Officer is responsible for administering this Policy and for developing and implementing any applicable related policies, procedures, and/or guidelines.

All managers, department heads and supervisors are responsible for ensuring that all employees, agents, contractors, or other parties working on behalf of the Company comply with this Policy and, where applicable, must implement such practices, processes, controls, and training as are reasonably necessary to ensure such compliance.

Any questions relating to this Policy or to Data Protection Law should be referred to the Data Protection Officer. In particular, the Data Protection Officer should always be consulted in the following cases:

i) if there is any uncertainty relating to the lawful basis on which personal data is to be collected, held, and/or processed;
ii) if consent is being relied upon in order to collect, hold, and/or process personal data;
iii) if there is any uncertainty relating to the retention period for any particular type(s) of personal data;
iv) if any new or amended privacy notices or similar privacy-related documentation are required;
v) if any assistance is required in dealing with the exercise of a data subject's rights (including, but not limited to, the handling of subject access requests);
vi) if a personal data breach (suspected or actual) has occurred;
vii) if there is any uncertainty relating to security measures (whether technical or organisational) required to protect personal data;
viii) if personal data is to be shared with third parties (whether such third parties are acting as data controllers or data processors);

ix) if personal data is to be transferred outside of the REPUBLIC OF KENYA and there are questions relating to the legal basis on which to do so;

x) when any significant new processing activity is to be carried out, or significant changes are to be made to existing processing activities, which will require a Data Protection Impact Assessment;

xi) when personal data is to be used for purposes different to those for which it was originally collected;

xii) if any automated processing, including profiling or automated decision-making, is to be carried out; or

xiii) if any assistance is required in complying with the law applicable to direct marketing or commercial use of personal data.

The Data Protection Principles (Section 25 of the Act)

This Policy aims to ensure compliance with Data Protection Law. Section 25 of the Act sets out the following principles with which any party handling personal data must comply. Data controllers are responsible for, and must be able to demonstrate, such compliance. All personal data must be:

a. processed in accordance with the right to privacy of the data subject
b. processed lawfully, fairly, and in a transparent manner in relation to the data subject;
c. collected for specified, explicit, and legitimate purposes and not further processed in a manner that is incompatible with those purposes. Further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be considered to be incompatible with the initial purposes;
d. adequate, relevant, and limited to what is necessary in relation to the purposes for which it is processed;
e. accurate and, where necessary, kept up to date. Every reasonable step must be taken to ensure that personal data that is inaccurate, having regard to the purposes for which it is processed, is erased, or rectified without delay;
f. kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data is processed. Personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes, or statistical purposes, subject to implementation of the appropriate technical and organisational measures required by the Act in order to safeguard the rights and freedoms of the data subject;
g. not transferred outside Kenya, unless there is proof of adequate data protection safeguards or consent from the data subject.

The Rights of Data Subjects (Section 25 of the Act)

The Act sets out the following key rights applicable to data subjects:

a. the right to be informed;
b. the right of access;
c. the right to rectification;
d. the right to deletion;
e. the right to restrict processing;
f. the right to data portability;
g. the right to object; and
h. rights with respect to automated decision-making and profiling.

Lawful, Fair, and Transparent Data Processing (Section 30 of the Act)

Data Protection Law seeks to ensure that personal data is processed lawfully, fairly, and transparently, without adversely affecting the rights of the data subject. Specifically, the processing of personal data shall be lawful if at least one of the following applies:

a) the data subject has given consent to the processing of their personal data for one or more specific purposes;
b) the processing is necessary for the performance of a contract to which the data subject is a party, or in order to take steps at the request of the data subject prior to entering into a contract;
c) the processing is necessary for compliance with a legal obligation to which the data controller is subject;
d) the processing is necessary to protect the vital interests of the data subject or of another natural person;
e) the processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the data controller; or

f) the processing is necessary for the purposes of the legitimate interests pursued by the data controller or by a third party, except where such interests are overridden by the fundamental rights and freedoms of the data subject which require protection of personal data;
g) for the purpose of historical, statistical, journalistic, literature and art or scientific research.

If the personal data in question is special category personal data (also known as "sensitive personal data"), at least one of the following conditions must be met:

a) the processing is necessary for the purpose of carrying out the obligations and exercising specific rights of the controller or of the data subject;
b) the processing is necessary to protect the vital interests of the data subject or of another natural person where the data subject is physically or legally incapable of giving consent;
c) the data subject has given their explicit consent to the processing of such data for transfer of personal data outside of the Republic of Kenya (unless the law prohibits them from doing so)
d) the data controller is a foundation, association, or other non-profit body with a political, philosophical, religious, or trade union aim, and the processing is carried out in the course of its legitimate activities, provided that the processing relates solely to the members or former members of that body or to persons who have regular contact with it in connection with its purposes and that the personal data is not disclosed outside the body without the consent of the data subjects;
e) the processing relates to personal data which is manifestly made public by the data subject;
f) the processing is necessary for the conduct of legal claims or whenever courts are acting in their judicial capacity;
g) the processing is necessary for substantial public interest reasons, on the basis of law which shall be proportionate to the aim pursued, shall respect the essence of the right

to data protection, and shall provide for suitable and specific measures to safeguard the fundamental rights and interests of the data subject;

h) the processing is necessary for public interest reasons in the area of public health, for example, protecting against serious cross-border threats to health or ensuring high standards of quality and safety of health care and of medicinal products or medical devices, on the basis of law which provides for suitable and specific measures to safeguard the rights and freedoms of the data subject (in particular, professional secrecy).

Consent (Section 32 of the Act)

If consent is relied upon as the lawful basis for collecting, holding, and/or processing personal data, the following shall apply:

a. Consent is a clear indication by the data subject that they agree to the processing of their personal data. Such a clear indication may take the form of a statement or a positive action. Silence, pre-ticked boxes, or inactivity are unlikely to amount to consent.
b. Where consent is given in a document which includes other matters, the section dealing with consent must be kept clearly separate from such other matters.
c. Data subjects are free to withdraw consent at any time and it must be made easy for them to do so. If a data subject withdraws consent, their request must be honoured promptly.
d. If personal data is to be processed for a different purpose that is incompatible with the purpose or purposes for which that personal data was originally collected that was not disclosed to the data subject when they first provided their consent, consent to the new purpose or purposes may need to be obtained from the data subject.
e. Except for where sensitive personal data is transferred outside of Kenya, if sensitive personal data is processed in all other cases, the Company shall normally rely on a lawful basis other than explicit consent. If explicit consent is relied upon, the data subject in question must be issued with a suitable privacy notice in order to capture their consent.

f. In all cases where consent is relied upon as the lawful basis for collecting, holding, and/or processing personal data, records must be kept of all consents obtained in order to ensure that the Company can demonstrate its compliance with consent requirements.

Specified, Explicit, and Legitimate Purposes (Section 25(c) of the Act)

The Company collects and processes the personal data set out in Part 22 of this Policy. This includes:

a) personal data collected directly from data subjects.

b) The Company only collects, processes, and holds personal data for the specific purposes set out in Part 22 of this Policy (or for other purposes expressly permitted by Data Protection Law).

c) Data subjects must be kept informed at all times of the purpose or purposes for which the Company uses their personal data. Please refer to Part 15 for more information on keeping data subjects informed.

Adequate, Relevant, and Limited Data Processing (Section 25(d) of the Act)

The Company will only collect and process personal data for and to the extent necessary for the specific purpose or purposes of which data subjects have been informed (or will be informed) as under Part 8, above, and as set out in Part 22, below.

a. Employees, agents, contractors, or other parties working on behalf of the Company may collect personal data only to the extent required for the performance of their job duties and only in accordance with this Policy. Excessive personal data must not be collected.

b. Employees, agents, contractors, or other parties working on behalf of the Company may process personal data only when the performance of their job duties requires it. Personal data held by the Company cannot be processed for any unrelated reasons.

Accuracy of Data and Keeping Data Up-to-Date (Section 25(f) of the Act)

a. The Company shall ensure that all personal data collected, processed, and held by it is kept accurate and up-to-date. This includes, but is not limited to, the rectification of personal data at the request of a data subject, as set out in Part 17, below.
b. The accuracy of personal data shall be checked when it is collected and at regular intervals thereafter. If any personal data is found to be inaccurate or out-of-date, all reasonable steps will be taken without delay to amend or erase that data, as appropriate.

Data Retention (Section 39 of the Act)

a. The Company shall not keep personal data for any longer than is necessary in light of the purpose or purposes for which that personal data was originally collected, held, and processed.

b. When personal data is no longer required, all reasonable steps will be taken to erase or otherwise dispose of it without delay.
For full details of the Company's approach to data retention, including retention periods for specific personal data types held by the Company, please refer to our Data Retention Policy.

Secure Processing (Section 29(f) of the Act)

a. The Company shall ensure that all personal data collected, held, and processed is kept secure and protected against unauthorised or unlawful processing and against accidental loss, destruction, or damage. Further details of the technical and organisational measures which shall be taken are provided in Parts 25 to 30 of this Policy.

b. All technical and organisational measures taken to protect personal data shall be regularly reviewed and evaluated to ensure their ongoing effectiveness and the continued security of personal data.

c. Data security must be maintained at all times by protecting the confidentiality, integrity, and availability of all personal data as follows:

d. only those with a genuine need to access and use personal data and who are authorised to do so may access and use it;

e. personal data must be accurate and suitable for the purpose or purposes for which it is collected, held, and processed; and

f. authorised users must always be able to access the personal data as required for the authorised purpose or purposes.

Accountability and Record-Keeping

a. The Data Protection Officer is responsible for administering this Policy and for developing and implementing any applicable related policies, procedures, and/or guidelines.

b. The Company shall follow a privacy by design approach at all times when collecting, holding, and processing personal data. Data Protection Impact Assessments shall be conducted if any processing presents a significant risk to the rights and freedoms of data subjects (please refer to Part 14 for further information).

c. All employees, agents, contractors, or other parties working on behalf of the Company shall be given appropriate training in data protection and privacy, addressing the relevant aspects of Data Protection Law, this Policy, and all other applicable Company policies.

d. The Company's data protection compliance shall be regularly reviewed and evaluated by means of Data Protection Audits.

e. The Company shall keep written internal records of all personal data collection, holding, and processing, which shall incorporate the following information:

    i) the name and details of the Company, its Data Protection Officer, and any applicable third-party data transfers (including data processors and other data controllers with whom personal data is shared);

    ii) the purposes for which the Company collects, holds, and processes personal data;

    iii) the Company's legal basis or bases (including, but not limited to, consent, the mechanism(s) for obtaining such consent, and records of such consent) for collecting, holding, and processing personal data;

    iv) details of the categories of personal data collected, held, and processed by the Company, and the categories of data subject to which that personal data relates;

    v) details of any transfers of personal data to countries outside the Republic of Kenya including all mechanisms and security safeguards;

vi) details of how long personal data will be retained by the Company (please refer to the Company's Data Retention Policy);

vii) details of personal data storage, including location(s);

viii) detailed descriptions of all technical and organisational measures taken by the Company to ensure the security of personal data

Data Protection Impact Assessments and Privacy by Design (Section 31 of the Act)

a. In accordance with the privacy by design principles, the Company shall carry out Data Protection Impact Assessments for any and all new projects and/or new uses of personal data which involve the use of new technologies and where the processing involved is likely to result in a high risk to the rights and freedoms of data subjects.

b. The principles of privacy by design should be followed at all times when collecting, holding, and processing personal data. The following factors should be taken into consideration:

   i) the nature, scope, context, and purpose or purposes of the collection, holding, and processing;

   ii) the state of the art of all relevant technical and organisational measures to be taken;

   iii) the cost of implementing such measures; and

   iv) the risks posed to data subjects and to the Company, including their likelihood and severity.

Data Protection Impact Assessments shall be overseen by the Data Protection Officer and shall address the following:

a) the type(s) of personal data that will be collected, held, and processed;

b) the purpose(s) for which personal data is to be used;

c) the Company's objectives;

d) how personal data is to be used;

e) the parties (internal and/or external) who are to be consulted;

f) the necessity and proportionality of the data processing with respect to the purpose(s) for which it is being processed;
g) risks posed to data subjects;
h) risks posed both within and to the Company; and
i) proposed measures to minimise and handle identified risks.

Keeping Data Subjects Informed (Section 26(a) of the Act)

The Company shall provide the information set out in Part 15.2 to every data subject:

a) where personal data is collected directly from data subjects, those data subjects will be informed of its purpose at the time of collection; and
b) where personal data is obtained from a third party, the relevant data subjects will be informed of its purpose:
    i. if the personal data is used to communicate with the data subject, when the first communication is made; or
    ii. if the personal data is to be transferred to another party, before that transfer is made; or
    iii. as soon as reasonably possible and in any event not more than one month after the personal data is obtained.

The following information shall be provided in the form of a privacy notice:

a) details of the Company including, but not limited to, contact details, and the names and contact details of any applicable representatives and its Data Protection Officer;
b) the purpose(s) for which the personal data is being collected and will be processed (as detailed in Part 22 of this Policy) and the lawful basis justifying that collection and processing;
c) where applicable, the legitimate interests upon which the Company is justifying its collection and processing of the personal data;
d) where the personal data is not obtained directly from the data subject, the categories of personal data collected and processed;

e) where the personal data is to be transferred to one or more third parties, details of those parties;

f) where the personal data is to be transferred to a third party that is located outside of the Republic of Kenya, details of that transfer, including but not limited to the safeguards in place;

g) details of applicable data retention periods;

h) details of the data subject's rights under the Act;

i) details of the data subject's right to withdraw their consent to the Company's processing of their personal data at any time;

j) details of the data subject's right to complain to the Office of the Data Protection Commissioner;

k) where the personal data is not obtained directly from the data subject, details about the source of that personal data;

l) where applicable, details of any legal or contractual requirement or obligation necessitating the collection and processing of the personal data and details of any consequences of failing to provide it; and

m) details of any automated decision-making or profiling that will take place using the personal data, including information on how decisions will be made, the significance of those decisions, and any consequences.

Data Subject Access (Section 26(b) of the Act)

a. Data subjects may make subject access requests ("SARs") at any time to find out more about the personal data which the Company holds about them, what it is doing with that personal data, and why.
b. Employees wishing to make a SAR should do using a Subject Access Request Form, sending the form to the Company's Data Protection Officer at info@moringa.co.ke
c. Responses to SARs must normally be made within **seven days** of receipt.
d. All SARs received shall be handled by the Company's Data Protection Officer
e. The Company does not charge a fee for the handling of normal SARs. The Company reserves the right to charge reasonable fees for additional copies of information that has already been supplied to a data subject, and for requests that are manifestly unfounded or excessive, particularly where such requests are repetitive.

Rectification of Personal Data (Section 40(1)(a) of the Act)

a. Data subjects have the right to require the Company to rectify any of their personal data that is inaccurate or incomplete.
b. The Company shall, where satisfied that a rectification is necessary, rectify the personal data in question, and inform the data subject of that rectification, within **fourteen days** month of the data subject informing the Company of the issue. Where a request for rectification is declined, the Company, in writing, notify a data subject of that refusal within **seven days** and shall provide reasons for refusal.
c. In the event that any affected personal data has been disclosed to third parties, those parties shall be informed of any rectification that must be made to that personal data.
d. The Company does not charge a fee for the handling of normal requests for rectification of data.

Erasure of Personal Data (Section 40(1)(b) of the Act)

Data subjects have the right to request that the Company erases the personal data it holds about them in the following circumstances:

a) it is no longer necessary for the Company to hold that personal data with respect to the purpose(s) for which it was originally collected or processed;

b) the data subject wishes to withdraw their consent to the Company holding and processing their personal data;

c) the data subject objects to the Company holding and processing their personal data (and there is no overriding legitimate interest to allow the Company to continue doing so) (see Part 21 of this Policy for further details concerning the right to object);

d) the personal data has been processed unlawfully; OR

e) the personal data needs to be erased in order for the Company to comply with a particular legal obligation.

f) The Company shall respond to a request for erasure within **fourteen days** of the request.

g) The Company is not required to comply with the right of erasure if processing is necessary for one of the following reasons:

   i) to exercise the right of freedom of expression and information;

   ii) to comply with a legal obligation;

   iii) for the performance of a task carried out in the public interest

   iv) or in the exercise of official authority;

   v) for archiving 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

   vi) for the establishment, exercise or defence of a legal claim.

h) In the event that any personal data that is to be erased in response to a data subject's request has been disclosed to third parties, those parties shall be informed of the erasure (unless it is impossible or would require disproportionate effort to do so).

i) The Company does not charge a fee for the handling of normal requests for rectification of data.

Restriction of Personal Data Processing (Section 34 of the Act)

Data subjects may request that the Company restricts processing the personal data it holds about them on the following grounds:

a) the data subject contests the accuracy of their personal data;
b) the personal data has been unlawfully processed and the data subject opposes the erasure and requests restriction instead;
c) the data subject no longer needs their personal data but the data controller or data processor requires the personal data to be kept in order to establish, exercise or defend a legal claim; or
d) a data subject has objected to the processing of their personal data and the Company is considering legitimate grounds that override those of the data subject.
    a. The Company shall respond to a request for restriction within **fourteen days** of the request and:
        i) admit and implement the request;
        ii) indicate on the Company's system that the processing of the personal data has been restricted; and
        iii) notify any relevant third party of the restriction where personal data, subject to such restriction, may have been shared.
    b. The Company may implement a restriction to processing request by:
e) temporarily moving the personal data to another processing system;
f) making the personal data unavailable to third parties; or
g) temporarily removing published data specific to the data subject from its website or other public medium in its control.
    a. In the event that any affected personal data has been disclosed to third parties, those parties shall be informed of the applicable restrictions on

processing it (unless it is impossible or would require disproportionate effort to do so).

b. The Company will not process personal data that has been restricted, except to store the personal data.

h) The Company may decline to comply with a request for restriction in processing, where such request is manifestly unfounded or excessive.

i) Where a request for restriction is declined, the Company, in writing, notify a data subject of that refusal within **fourteen days** and shall provide reasons for the decision.

Objections to Personal Data Processing (Section 36 of the Act)

a) Data subjects have the right to object to the Company processing their personal data based on legitimate interests, for direct marketing (including profiling).

b) Where a data subject objects to the Company processing their personal data based on its legitimate interests, the Company shall cease such processing immediately, unless it can be demonstrated that the Company's legitimate grounds for such processing override the data subject's interests, rights, and freedoms, or that the processing is necessary for the conduct of legal claims. In such cases the Company shall inform the data subject of:

i) the reasons for declining the request for objection; and

ii) the right to lodge a complaint to the Data Commissioner where dissatisfied.

Where a data subject objects to the Company processing their personal data for direct marketing purposes, the Company shall cease such processing promptly.

Direct Marketing (Regulation 14, 15,16, 17 and 18 of the Data Protection General Regulations 2021)

The Company is subject to certain rules and regulations when marketing its appliances. The prior consent of data subjects is required for electronic direct marketing including catalogue

through any medium, displaying an advertisement on an online media site where the data subject is logged on using their personal data, email, text messaging, and automated telephone calls.

a) The Company shall not use sensitive personal data for direct marketing.

b) The Company may use personal data concerning a data subject for the purpose of direct marketing where—

    a) the Company has collected the personal data from the data subject;

    b) the data subject is notified that direct marketing is one of the purposes for which personal data is collected;

    c) the data subject has consented to the use or disclosure of the personal data for the purpose of direct marketing;

    d) the Company provides a simplified opt out mechanism for the data subject to request not to receive direct marketing communications; or

    e) the data subject has not made an opt out request.

c) The right to object to direct marketing shall be explicitly offered to data subjects in a clear and intelligible manner and must be kept separate from other information in order to preserve its clarity.

d) If a data subject objects to direct marketing, their request must be complied with promptly. A limited amount of personal data may be retained in such circumstances to the extent required to ensure that the data subject's marketing preferences continue to be complied with.

Personal Data Collected, Held, and Processed.

The personal data is collected, held, and processed by the Company (for details of data retention, please refer to the Company's Data Retention Policy) as set out in **Annexure 1.**

I. Data Security - Transferring Personal Data and Communications

The Company shall ensure that the following measures are taken with respect to all communications and other transfers involving personal data:

a) All emails containing personal data must be encrypted using 2FA, Password, Geo-restricted authentication, SSL Encryption or RSA Encryption.

b) All emails containing personal data must be marked "confidential";

Personal data may be transmitted over secure networks only; transmission over unsecured networks is not permitted in any circumstances;

c) Personal data may not be transmitted over a wireless network if there is a wired alternative that is reasonably practicable;

d) Personal data contained in the body of an email, whether sent or received, should be copied from the body of that email and stored securely. The email itself should be deleted.

e) All temporary files associated therewith should also be deleted.

f) Where personal data is to be sent by facsimile transmission the recipient should be informed in advance of the transmission and should be waiting by the fax machine to receive the data;

g) Where personal data is to be transferred in hardcopy form it should be passed directly to the recipient.

h) All personal data to be transferred physically, whether in hardcopy form or on removable electronic media shall be transferred in a suitable container marked "confidential";

II. Data Security – Storage

The Company shall ensure that the following measures are taken with respect to the storage of personal data:

a) All electronic copies of personal data should be stored securely using passwords and 2FA, Password, Geo-restricted authentication, SSL Encryption or RSA data encryption;

b) All hardcopies of personal data, along with any electronic copies stored on physical, removable media should be stored securely in a locked box, drawer, cabinet, or similar;

c) All personal data stored electronically should be backed up on GCP infrastructure with backups stored onsite. All backups should be encryptedSSL Encryption or RSA data encryption;

d) No personal data should be stored on any mobile device (including, but not limited to, laptops, tablets, and smartphones), whether such device belongs to the Company or otherwise [without the formal written approval of the **Tech and Data Director - Setriakor Nyomi <setriakor.nyomi@moringaschool.com> or Data Protection Officer - Ken Mbuki <ken.mbuki@moringaschool.com>** and, in the event of such approval, strictly in accordance with all instructions and limitations described at the time the approval is given, and for no longer than is absolutely necessary];

e) No personal data should be transferred to any device personally belonging to an employee, agent, contractor, or other party working on behalf of the Company and personal data may only be transferred to devices belonging to agents, contractors, or other parties working on behalf of the Company where the party in question has agreed to comply fully with the letter and spirit of this Policy and of the applicable

f) Data Protection Law (which may include demonstrating to the Company that all suitable technical and organisational measures have been taken).

III. Data Security – Disposal

When any personal data is to be erased or otherwise disposed of for any reason (including where copies have been made and are no longer needed), it should be securely deleted and disposed of. For further information on the deletion and disposal of personal data, please refer to the Company's Data Retention Policy.

IV. Data Security - Use of Personal Data

The Company shall ensure that the following measures are taken with respect to the use of personal data:

a) No personal data may be shared informally and if an employee, agent, contractor, or other party working on behalf of the Company requires access to any personal data that they do not already have access to, such access should be formally requested from **Tech and Data Director - Setriakor Nyomi <setriakor.nyomi@moringaschool.com> or Data Protection Officer - Ken Mbuki <ken.mbuki@moringaschool.com> or <DPO@moringaschool.com>**

b) No personal data may be transferred to any employee, agent, contractor, or other party, whether such parties are working on behalf of the Company or not, without the authorisation of **Tech and Data Director - Setriakor Nyomi <setriakor.nyomi@moringaschool.com> or Data Protection Officer - Ken Mbuki <ken.mbuki@moringaschool.com>;**

c) Personal data must be handled with care at all times and should not be left unattended or on view to unauthorised employees, agents, contractors, or other parties at any time;

d) If personal data is being viewed on a computer screen and the computer in question is to be left unattended for any period of time, the user must lock the computer and screen before leaving it;

e) Where personal data held by the Company is used for marketing purposes, it shall be the responsibility of <<insert position>> to ensure that the appropriate consent is

obtained and that no data subjects have opted out, whether directly or via a third-party service such as the TPS.

V. Data Security - IT Security

The Company shall ensure that the following measures are taken with respect to IT and information security: In summary we have implemented 2FA, Password, Geo-restricted authentication, SSL Encryption and RSA Encryption on our platforms.

a) All passwords used to protect personal data should be changed regularly and should not use words or phrases that can be easily guessed or otherwise compromised. All passwords must contain a combination of uppercase and lowercase letters, numbers, and symbols;
b) Under no circumstances should any passwords be written down or shared between any employees, agents, contractors, or other parties working on behalf of the Company, irrespective of seniority or department. If a password is forgotten, it must be reset using the applicable method. IT staff do not have access to passwords;
c) All software (including, but not limited to, applications and operating systems) shall be kept up-to-date. The Company's IT staff shall be responsible for installing any and all security-related updates as soon as reasonably and practically possible;
d) No software may be installed on any Company-owned computer or device without the prior approval of the **Tech and Data Director - Setriakor Nyomi <setriakor.nyomi@moringaschool.com>**

VI. Organisational Measures

The Company shall ensure that the following measures are taken with respect to the collection, holding, and processing of personal data:

a) All employees, agents, contractors, or other parties working on behalf of the Company shall be made fully aware of both their individual responsibilities and the

Company's responsibilities under Data Protection Law and under this Policy, and shall be provided with a copy of this Policy;

b) Only employees, agents, contractors, or other parties working on behalf of the Company that need access to, and use of, personal data in order to carry out their assigned duties correctly shall have access to personal data held by the Company;

c) All sharing of personal data shall comply with the information provided to the relevant data subjects and, if required, the consent of such data subjects shall be obtained prior to the sharing of their personal data;

d) All employees, agents, contractors, or other parties working on behalf of the Company handling personal data will be appropriately trained to do so;

e) All employees, agents, contractors, or other parties working on behalf of the Company handling personal data will be appropriately supervised;

f) All employees, agents, contractors, or other parties working on behalf of the Company handling personal data shall be required and encouraged to exercise care, caution, and discretion when discussing work-related matters that relate to personal data, whether in the workplace or otherwise;

g) Methods of collecting, holding, and processing personal data shall be regularly evaluated and reviewed;

h) All personal data held by the Company shall be reviewed periodically, as set out in the Company's Data Retention Policy;

i) The performance of those employees, agents, contractors, or other parties working on behalf of the Company handling personal data shall be regularly evaluated and reviewed;

j) All employees, agents, contractors, or other parties working on behalf of the Company handling personal data will be bound to do so in accordance with the principles of Data Protection Law and this Policy by contract;

k) All agents, contractors, or other parties working on behalf of the Company handling personal data must ensure that any and all of their employees who are involved in the processing of personal data are held to the same conditions as those relevant employees of the Company arising out of this Policy and Data Protection Law; and

l) Where any agent, contractor or other party working on behalf of the Company handling personal data fails in their obligations under this Policy that party shall indemnify and hold harmless the Company against any costs, liability, damages, loss, claims or proceedings which may arise out of that failure.

Transferring Personal Data to a Country Outside the Republic of Kenya (Section 48 and 49 of the Act)

The Company may, from time to time, transfer ('transfer' includes making available remotely) personal data to countries outside of the Republic of Kenya. The Data Protection Law restricts such transfers in order to ensure that the level of protection given to data subjects is not compromised.

a) Personal data may only be transferred to a country outside the Republic of Kenya if one of the following applies:
b) The Republic of Kenya has issued regulations confirming that the country in question ensures an adequate level of protection (referred to as 'adequacy decisions' or 'adequacy regulations').
c) Appropriate safeguards are in place including binding corporate rules, standard contractual clauses approved for use in the Republic of Kenya, an approved code of conduct, or an approved certification mechanism.
d) The transfer is made with the informed and explicit consent of the relevant data subject;
e) The transfer is necessary including the performance of a contract between the data subject and the Company; public interest reasons; for the establishment, exercise, or defence of legal claims; to protect the vital interests of the data subject where the data subject is physically or legally incapable of giving consent; or, in limited circumstances, for the Company's legitimate interests.

Data Breach Notification (Section 43 of the Act)

a) All personal data breaches must be reported immediately to the Company's Data Protection Officer.

b) If an employee, agent, contractor, or other party working on behalf of the Company becomes aware of or suspects that a personal data breach has occurred, they must not attempt to investigate it themselves. Any and all evidence relating to the personal data breach in question should be carefully retained.

c) If a personal data breach occurs and that breach is likely to result in a risk to the rights and freedoms of data subjects (e.g. financial loss, breach of confidentiality, discrimination, reputational damage, or other significant social or economic damage), the Data Protection Officer must ensure that the Office of the Data Protection Commissioner is informed of the breach without delay, and in any event, within **72 hours** after having become aware of it.

d) In the event that a personal data breach is likely to result in a high risk (that is, a higher risk than that described under Part 30.3) to the rights and freedoms of data subjects, the Data Protection Officer must ensure that all affected data subjects are informed of the breach directly and without undue delay.

   Data breach notifications shall include the following information:

   a) The categories and approximate number of data subjects concerned;
   b) The categories and approximate number of personal data records concerned;
   c) The name and contact details of the Company's data protection officer (or other contact point where more information can be obtained);
   d) The likely consequences of the breach;
   e) Details of the measures taken, or proposed to be taken, by the Company to address the breach including, where appropriate, measures to mitigate its possible adverse effects.

The following personal data or circumstances amount to a notifiable data breach the Office of the Data Protection Commissioner:

a) The amount of any wages, salary, fee, commission, bonus, gratuity, allowance or other remuneration paid or payable to the data subject by any person, whether under a contract of service or a contract for services.

b) The income of the data subject from the sale of any goods or property.

c) The number of any credit card, charge card or debit card issued to or in the name of the data subject.

d) The number assigned to any account the data subject has with any entity that is a bank or finance company.

e) Any information that identifies, or is likely to lead to the identification of, the data subject who is a child in conflict with the law or in need of care and protection.

Any private key of or relating to a data subject that is used or may be used —

- to create a secure electronic record or secure electronic signature;
- to verify the integrity of a secure electronic record; or
- to verify the authenticity or integrity of a secure electronic signature as provided under the Kenya Information and Communications (Electronic Certification and Domain Name Administration) Regulations, 2010 or any other related law.

The net worth or creditworthiness of a data subject.

f) The deposit or withdrawal of monies by a data subject with any entity.

g) The withdrawal by the individual of money deposited with any entity or a payment system.

The granting by a person of advances, loans and other facilities by which the data subject, being a customer of the entity, has access to funds or financial guarantees.

h) The existence, and amount due or outstanding, of any debt —

- owed by the data subject to an entity; or
- owed by an entity to the data subject.

i) The incurring by the entity of any liabilities on behalf of the data subject.

j) The payment of any money, or transfer of any property, by any person to the individual, including the amount of the money paid or the value of the property transferred, as the case may be.

The data subject's investment in any capital markets products.

k) Any term and condition, premium or benefits payable, or any detail relating to the condition of health, from an accident, health, or life policy of which the data subject is the policy owner or a beneficiary.

l) The assessment, diagnosis, treatment, prevention or alleviation by a health professional of any of the following affecting the data subject—

- any sexually- transmitted diseases;
- Human Immunodeficiency Virus Infection;
- mental disorder;
- substance abuse and addiction.

m) The provision of treatment to the individual for or in respect of:

- the donation or receipt of a human egg or human sperm; or
- any contraceptive operation or procedure or abortion.

n) Any of the following:

- the donation and removal of any organ from the body of the deceased individual for the purpose of its transplantation into the body of another individual;
- the donation and removal of any specified organ from the individual, being a living organ donor, for the purpose of its transplantation into the body of another individual;
- the transplantation of any organ mentioned in paragraph (a) or (b) into the body of the individual.

o) The suicide or attempted suicide of the individual.

p) Domestic abuse, child abuse or sexual abuse involving or alleged to involve the data subject.

q) Any of the following:

- information that the individual is or had been adopted pursuant to an adoption order made under the Children Act No 8 of 2001, or is or had been the subject of an application for an adoption order;
- the identity of the natural father or mother of the data subject;
- the identity of the adoptive father or mother of the subject;

- the identity of any applicant for an adoption order;
- the identity of any person whose consent is necessary under that Act for an adoption order to be made, whether or not the court has dispensed with the consent of that person in accordance with that Act.

Policy Review and Implementation

This Policy shall be deemed effective as of 26th March 2024. No part of this Policy shall have retroactive effect and shall thus apply only to matters occurring on or after this date.

This Policy has been approved and authorised by:

Name:	**Nikki Germany**
Position:	Chief Executive Officer
Date:	03 / 26 / 2024
Signature:	

Witnessed By:

Name:	Ronnie Gonahasa
Position:	Legal Associate
Date:	04 / 03 / 2024
Signature:	

Annexure 1

Type of Data	Purpose of Data
STUDENTS	
Personal -Name Personal -Email Financial -Debit/Credit cards Financial -Bank account Personal -Date of birth Personal -Next of kin Personal -Photograph Personal -Emergency contact Personal -Gender Personal -Nationality Personal -Personal interests Personal -Social media Personal -Telephone Personal -Address Personal -Parental consent Tracking Data -IP address Tracking Data -Cookies / apps Employment Details -Employment status Employment Details -Employment history	• Student enrollment, • Know Your Client (KYC) • Scholarship Enrollment • Feedback & Satisfaction, • Improve user experience • Data Bundle Disbursement • Communication, • Placement • Transaction purposes e.g invoicing,receiving payments
EMPLOYEES	
Personal -Name Personal -Address Personal - Referee name and contact no Personal -Date of birth Personal -Email Personal -Emergency contact Personal -Gender Personal -Nationality Personal -Next of kin Personal -Photograph Personal -Telephone Identity Documents -National ID card Financial -Bank account Financial -KRA Personal Identification Number Financial -National Health Insurance Fund (NHIF) Financial -National Social Security Fund (NSSF) Employment Details -Annual appraisals	• Payroll, • Personnel FIle, • Transactions, • Support, • Security, • Communication

Employment Details -Disciplinary Employment Details -Education/Training Employment Details -Employment history Employment Details -Employment status Employment Details -Annual leave Employment Details -Pre-employment checks Employment Details -References Employment Details -Work permit Employment Details -Annual appraisals Employment Details -Sickness Tracking Data -CCTV Tracking Data -Voice recording Tracking Data -Videos	
STUDENT ALUMNI	
Employment Details -Education/Training Employment Details -Employment history Employment Details -Employment status Financial -Bank account Financial -KRA Personal Identification Number Financial -National Health Insurance Fund (NHIF) Financial -National Social Security Fund (NSSF) Identity Documents -National ID card Personal -Dependents Personal -Email Personal -Name Personal -Nationality Personal -Next of kin	• Marketing • Communication • Training needs analysis • Placement
PARENTS/GUARDIANS	

Financial -Bank account Financial -Bank account	• Know Your Client (KYC) • Invoicing
EMPLOYER PARTNERS	
Personal -Email Personal -Name Personal -Telephone Financial -KRA Personal Identification Number Employment Details -Employment status Employment Details -Other Financial -Company Details"	• Student Progress and Marking • Payments, • Training needs analysis
CLIENTS	
Personal -Email Personal -Name Personal -Nationality Personal -Photograph Personal -Telephone	• Student Enrollment
SUPPLIERS	
Financial -Company Details Financial -Bank account Financial -Company Details Financial -KRA Personal Identification Number Financial -Other	• Payment Processing, • Invoicing, • Reporting
CONSULTANTS	
Financial -Bank Account Financial -KRA Personal Identification Number	• Payment Processing, • Invoicing, • Reporting
VENDORS	
Financial -Bank Account Financial -KRA Personal Identification Number Financial - Company Details Financial -Credit history Financial - Other	• Payment Processing, • Invoicing, • Reporting
UNSUCCESSFUL CANDIDATES	
Personal -Email Personal -Name Personal -Telephone	• Personnel File, • Communication

Dropbox Sign

Audit trail

Title	Moringa School _ Data Protection Policy _(Final 32624)
File name	1._Data_Protection_Policy_-_V2.pdf
Document ID	a740664228f5180370ea1d4ece1a25152a9d7b11
Audit trail date format	MM / DD / YYYY
Status	● Signed

Document History

SENT	**03 / 26 / 2024** 14:00:24 UTC	Sent for signature to Nikki Germany (nikki@moringaschool.com) and Ronnie Gonahasa (ronnie.gonahasa@moringaschool.com) from legal@moringaschool.com IP: 197.248.115.157
VIEWED	**03 / 26 / 2024** 17:14:32 UTC	Viewed by Nikki Germany (nikki@moringaschool.com) IP: 105.161.202.104
SIGNED	**03 / 26 / 2024** 17:16:00 UTC	Signed by Nikki Germany (nikki@moringaschool.com) IP: 105.161.202.104
VIEWED	**03 / 26 / 2024** 20:03:38 UTC	Viewed by Ronnie Gonahasa (ronnie.gonahasa@moringaschool.com) IP: 169.255.105.207

Dropbox Sign

Audit trail

Title	Moringa School _ Data Protection Policy _(Final 32624)
File name	1._Data_Protection_Policy_-_V2.pdf
Document ID	a740664228f5180370ea1d4ece1a25152a9d7b11
Audit trail date format	MM / DD / YYYY
Status	● Signed

Document History

SIGNED	**04 / 03 / 2024** 09:22:56 UTC	Signed by Ronnie Gonahasa (ronnie.gonahasa@moringaschool.com) IP: 197.248.115.157
COMPLETED	**04 / 03 / 2024** 09:22:56 UTC	The document has been completed.