St Andrew's School, Turi

Data Protection and Privacy Policy

Compiled by:	**Finance and Strategy Director**
Reviewed by:	**SEC**
Date of review:	**October 2023**
Date of next review:	**October 2024**
Approved by:	**FAR & Board of Governors November 17, 2023**

1. Policy Statement

The School recognizes its legal and statutory obligation to collect, handle and process personal and sensitive data in accordance with the Kenya Data Protection Act (2019) (DPA).

The School further recognizes its legal and statutory obligation to adhere to the EU's General Data Protection Regulation (GDPR), which applies to all EU citizens wherever they are located and may affect any of our students and employees. As such, the School is also ensuring that its systems in so far as it is possible are also compliant with the GDPR.

The DPA is established to, among other things:

- Give effect to Article 31(c) and (d) of the Constitution of Kenya;
- Establish the office of Data Protection Commissioner;
- Make provision for the regulation of the processing of personal and sensitive data;
- Provide for the rights of data subjects and obligations of data controllers and processors.

1.1 Scope

Anyone who works for, or acts on behalf of the School (including staff, volunteers, governors and service providers) and is involved in the processing of personal data is required to comply with this Policy, as well as prevailing legislation on data protection. The School's Staff Privacy Notice also provides further information about how personal data about those individuals will be used.

1.2 Definition

"Data Protection" is the process of safeguarding personal and sensitive information from corruption compromise and/or loss and includes implementation of appropriate administrative, technical and physical means to guard against unauthorized, intentional or accidental disclosure, modification or destruction of data.

"Data" means information which:-

a) is being processed by means of equipment operating automatically in response to instructions given for that purpose;
b) is recorded with the intention that it should be processed by means of such equipment;
c) is recorded as part of a relevant filing system or with the intention that it should form part of a relevant filing system;
d) does not fall within paragraph (a), (b) or (c) but forms part of an accessible record, or;
e) is recorded information held by a public authority and does not fall within any of paragraphs (a) to (d)

"Data Commissioner" refers to the person appointed by the Public Service Commission in accordance with Section 6 of the DPA 2019.

"Data Controller" refers to a person (natural or legal) who (either alone or jointly or in common with other persons) determines the purposes for which and the manner in which any personal data are, or are to be, processed.

Pursuant to the DPA, the School is deemed to be a data controller, and therefore the Board of Governors and Management is expected to oversee compliance by the School to the DPA.

"Data Processors" refers to a person (natural or legal) who (either alone or jointly or in common with other persons) processes personal data on behalf of the data controller. This may include contractors, suppliers, vendors and other service providers.

"Data Subjects" are identifiable or identified natural persons who are the subject of personal data.

"Personal data" means any information relating to an identified or identifiable natural person. It covers current and former employees, job applicants, contract and other staff, students, parents, suppliers, marketing and business contacts and such other persons from whom the school collects and processes personal data in the ordinary course of business.

"Identifiable natural person" means a person who can be identified directly or indirectly, by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social or social identity.

"Sensitive Personal Data" refers to data revealing an individual'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 etc.

"Consent" refers to any voluntary, specific and informed expression of will of a data subject to process personal data.

"Data Breach" refers to a breach of security that results in an accidental, unauthorized or illegal access, disclosure, modification, loss, transmission or destruction of data.

"Processing" refers to any action or set of actions performed on personal information, including obtaining, organizing, viewing, copying, modifying, amending, adding, deleting, extracting, sharing, storing, disclosing or destroying information.

1.3 Terminology

In this Policy, '**Board**' refers to the Board of Governors; '**School**' refers to both the Senior and Preparatory Schools either separately or jointly depending on the context; **'Director'** refers to the School's Executive Director; '**Head**' refers to both the Head of the Senior School and the Head of the Preparatory School; **'Operations Director'** refers to the Operations & Projects Director; **'F & S Director'** refers to the Finance and Strategy Director; '**Staff**' refers to all those working for or on behalf of the School (including staff working on behalf of third party contractors), full or part-time, permanent or temporary, in either paid or voluntary capacities; and '**Parents**' includes one or both of the parents, and legal or education guardians

1.4 Legal and regulatory framework

This Policy is based on the DPA and best practice in data protection.

1.5 Review

This Policy will be subject to annual review by the School Executive Committee (SEC) (unless an incident, guidance or new legislation requires an earlier date of review) and shall make recommendations on any amendments for the Board's consideration and approval.

Any substantial changes that affect the rights of staff, students, parents and other data subjects will be directly communicated as far as is reasonably practicable.

2. Roles and responsibilities

2.1 The Board

The Board has overall responsibility for ensuring that the School has a robust framework for managing data held by the School through appropriate documented policies and procedures, appointment of suitably trained personnel and provision of adequate resources to enhance data protection.

2.2 The Data Protection Officer

In accordance with the DPA, the School is required to appoint a Data Protection Officer (DPO) since the School undertakes processing of data including sensitive categories of personal data. The DPO may be a member of staff who shall ensure that all the data that is received and handled by the School is processed in accordance with the law. The Legal & Compliance Officer (LCO) (legalandcompliance@turimail.co.ke) is the School's appointed DPO.

The DPO is responsible for:

- monitoring and reporting compliance with data protection legislation to the Board;
- dealing with all requests and enquiries from data subjects concerning the School's use of personal data;
- chairing incident panels and investigations into data breaches and recording any data protection breaches that have come to light and how they have been resolved;
- providing guidance to staff and governors on data processing requirements in accordance with data protection legislation;
- facilitate training of staff involved in data processing operations;
- co-operate with the Data Commissioner (DC) and any other authority on matters relating to data protection.

2.3 Staff Responsibilities

2.3.1 Information provided by staff to the School

All staff shall:

- Ensure that all personal information which they provide to the School about their employment is accurate and up-to-date.
- Inform the School of any changes to information, for example, changes of address.
- Check the information which the School shall make available from time to time, in written or automated form, and inform the School of any errors;

The School shall not be held responsible for errors of which it has not been informed.

2.3.2 Information Held or Processed by Staff

All Staff are to apply due care and due diligence in processing information held by the School. All staff are expected to handle such information with appropriate care. Care of students data should be taken

very seriously. Staff shall at all times ensure that:

- All personal information is stored securely;
- They shall only take data relevant to their work needs;
- They shall only hold data for the minimum time required to complete their work;
- They shall destroy data when no longer required;
- They shall not share data with any third party except expressly authorized by the data subject and approving authority within the School;
- They only process information they have authorized access to;
- Personal information in any form (including visual, verbal, written, electronic or any other media or manner) is not to be disclosed accidentally or otherwise to any unauthorized third party. Unauthorized disclosure may be a disciplinary matter, and may be considered gross misconduct in some cases.

3. Principles

In the ordinary course of business, the School obtains, holds, and processes information about staff, students, parents and other data subjects for administrative, operational, and commercial purposes. The School may also process such information to fulfill legal obligations and contractual agreements. When handling such information, staff or others who process or use any personal information must comply with the DPA which indicates that data shall be processed in accordance with the following principles:

- In accordance with the right to privacy;
- Lawfully, fairly and in a transparent manner;
- Collected for explicit, specified and legitimate purpose;
- Adequate, relevant and limited to what is necessary;
- Collected only where a valid explanation is provided;
- The data must be accurate and where necessary kept up to date with every reasonable step being taken to ensure that any inaccurate data is erased or rectified without delay;
- Kept for no longer than is necessary for the purposes which it was collected;
- Not transferred outside Kenya unless consent is obtained or there is proof of adequate data protection safeguards.

4. Types of personal and sensitive personal data processed by the School

These will include by way of example and are not limited to:

- names, gender, nationality, religion, addresses, telephone numbers, e-mail addresses and other contact details;
- marital status and family details e.g. spouse and children's details;
- biometric information, which will be collected and used by the School in accordance with the School's Policy
- bank details and other financial information, e.g. about parents who pay fees to the School;
- past, present and prospective students' academic, disciplinary, admissions and attendance records (including information about any special needs), and examination scripts and marks;
- where appropriate, information about students' and employees' health, and contact details for their next of kin;
- references given or received by the School about students, and information provided by previous educational establishments and/or other professionals or organizations working with students;

- images of students (and occasionally other individuals) engaging in school activities, and images captured by the School's CCTV system (in accordance with the School's policy on taking, storing and using images of children).

5. Collection of Personal Data by the School

The School is to ensure that personal data is collected from the data subject (in the case of students, from their parents) unless consent to obtain data from elsewhere is granted by the data subject. This may be via a form, or simply in the ordinary course of interaction or communication (such as email or written assessments).

However in some cases, personal data may be supplied by third parties (for example another school, or other professionals or authorities working with that individual). In such an instance, the School is obliged to notify the relevant data subject that it is sourcing such information from a third party.

The School expects that it shall obtain, hold and process data for the following uses:

- for the purposes of student selection (and to confirm the identity of prospective students and their parents);
- for recruitment and employment of staff;
- to provide education services, including musical education, physical training or spiritual development, career services, and extra-curricular activities to students, and monitoring students' progress and educational needs;
- maintaining relationships with alumni and the School community, including direct marketing or fundraising activities;
- for the purposes of donor due diligence, and to confirm the identity of prospective donors and their background and relevant interests;
- for the purposes of management planning and forecasting, research and statistical analysis, including that imposed or provided for by law (such as diversity or gender pay gap analysis and taxation records);
- to enable relevant authorities to monitor the School's operations and performance and to intervene or assist with incidents as appropriate;
- to give and receive information and references about past, current and prospective students, including relating to outstanding fees or payment history, to/from any educational institution that the student attended or where it is proposed they attend; and to provide references to potential employers of past students
- to enable students to take part in national or other assessments, and to publish the results of public examinations or other achievements of students of the School;
- to safeguard students' welfare and provide appropriate pastoral care;
- to monitor (as appropriate) use of the School's IT and communications systems in accordance with the School's Acceptable Use of IT Policy;
- to make use of photographic images of students in school publications, on the School website and (where appropriate) on the School's social media channels in accordance with the School's Use of Images of Children Policy;
- for security purposes, including CCTV in accordance with the School's CCTV Policy;
- where otherwise reasonably necessary for the School's purposes, including to obtain appropriate professional advice and insurance for the School.

In addition, the School may need to process sensitive **personal data** (concerning health, ethnicity, religion, or sexual life) or criminal records information (such as when carrying out DBS checks) in

accordance with rights or duties imposed on it by law, including as regards safeguarding and employment, or from time to time by explicit consent where required. These reasons may include but not limited to:-

- to safeguard students' welfare and provide appropriate pastoral (and where necessary medical care), and to take appropriate action in the event of an emergency, incident or accident, including by disclosing details of an individual's medical condition where it is in the individual's interests to do so, for example for medical advice, social services, insurance purposes or to organizers of school trips;
- to provide educational services in the context of any special educational needs of a student;
- to provide spiritual education in the context of any religious beliefs;
- in connection with employment of its staff, for example DBS checks, welfare or pension plans;
- to run any of its systems that operate on biometric data, such as for security and other forms of employee identification;
- for legal and regulatory purposes (for example child protection, diversity monitoring and health and safety) and to comply with its legal obligations and duties of care.

6. Access and sharing of Personal data

Occasionally, the School will need to share personal information relating to data subjects with third parties, such as professional advisers (lawyers and accountants) or relevant government authorities and agencies including KRA, the police, Ministry of Education or Immigration.

For the most part, personal data collected by the School will remain within the School, and will be processed by appropriate individuals only in accordance with access protocols (i.e. on a 'need to know' basis). Particularly strict rules of access apply in the context of:-

- medical records held and accessed only by the School Doctor and appropriate medical staff under his/her supervision, or otherwise in accordance with express consent; and
- pastoral or safeguarding files held and accessed by the Designated Safeguarding Leads (DSL's), appropriate pastoral staff, Governors with specific responsibility for Safeguarding and Boarding and School inspectors under the supervision of the DSL's.

However, a certain amount of any SEN student's relevant information will need to be provided to staff more widely in the context of providing the necessary care and education that the student requires.

Students, parents and staff are reminded that the School is under duties imposed by law and statutory guidance to record or report incidents and concerns that arise or are reported to it, in some cases regardless of whether they are proven, if they meet a certain threshold of seriousness in their nature or regularity. This may include file notes on personnel or safeguarding files, and in some cases referrals to relevant authorities such as the police. For further information about this, please view the School's Safeguarding Policy.

Finally, in accordance with Data Protection Law, some of the School's processing activity is carried out on its behalf by third parties, such as IT systems, web developers or cloud storage providers. This is always subject to contractual obligations that personal data will be kept securely and only in accordance with the School's specific directions and data protection laws.

7. Retention of Personal Data

The School will retain personal data securely. The periods of retention of data depends on legal and operational requirements and is more fully explained in the School's Retention of Records Policy.

Typically, the recommendation for the duration of retaining ordinary student and staff personnel files is up to 7 years following departure from the School. However, incident reports and safeguarding files will need to be kept much longer, in accordance with specific legal requirements.

In line with the data protection principles, data should be retained no longer than it is required for the purposes of supporting school operations. Staff should ensure that personal data is not kept on their endpoints for a period longer than what is designated for processing.

The means for retention of data shall account for the form which data is held (paper, electronic), the cost of storage, current state of technology and legal & regulatory requirements.

Staff who may wish to request that personal data that they no longer believe to be relevant is considered for erasure, should contact the Legal & Compliance Officer on legalandcompliance@turimail.co.ke. However, despite such a request the School may have lawful and necessary reasons to hold on to some data.

8. Protection of Data

All personal data should be adequately protected in collection, storage, transit, use, and in destruction from unauthorized disclosure (both internal and external). This applies to sensitive information whether physical or electronic. Access to sensitive data should be restricted to authorized staff.

9. Processing of Personal Data

The School must ensure that all relevant documents evidence that consent to process data has been given by the data subject. Records must be kept to demonstrate that consent has been given. Procedures must also be put in place to record and act upon withdrawal of consent.

The School shall not process personal data unless:

- The data subject consents for specified purpose(s).
- The processing is necessary to discharge the School's normal operations, perform a contract, comply with a legal obligation or to protect vital interests of the data subject or for legitimate interests pursued by the School without prejudice to the rights and freedoms of data subjects.
- The collection, storage or use of personal data is for a purpose which is lawful, specific and explicitly defined.
- Where the data relates to a student, consent is given by the student's parent or legal guardian.

10. Restrictions on Processing

The School shall at the request of a data subject restrict the processing of personal data where amongst others the accuracy of the personal data is contested by the data subject.

The School needs to ensure that systems are set up to identify restricted personal data. The School should comply with a request to restrict processing of data where:-

- The individual has objected to the processing and the School is considering if there are overriding legitimate grounds that justify continued processing;
- The processing is unlawful;
- The accuracy of the personal data is being contested and the School is verifying that data;
- The Data is no longer required for the purpose of processing

Where data processing is restricted, the School may only process personal data with the consent of the data subject, for legal claims, for protection of rights and freedoms of others or for reasons of important public interest. The School must inform the data subject before withdrawing the restriction on processing.

11. Data Portability

A data subject has the right to receive personal data concerning them in a structured, commonly used and machine – readable format and to transmit the said data to another data controller without any hindrance.
The School must comply within a period of 30 days or longer depending on the nature of the request. No objection or difficulties should be raised by the School where a data subject presents such a request.

12. Transfer of Personal Data Outside Kenya

The School will generally not transfer personal data outside Kenya unless there are sufficient and valid reasons for doing so. Prior to such transfer, the School shall ensure that either:

- valid grounds exist (as provided under section 48 of the DPA) prior to such transfer and that proper safeguards have been put in place to address the security and protection of such data; or
- the School has given proof to the Data Commissioner on the appropriate safeguards with respect to the security and protection of the personal data

13. Keeping in touch and supporting the School

The School will use the contact details of parents, alumni and other members of the School community to keep them updated about the activities of the School, or alumni and parent events of interest, including by sending updates and newsletters by email. The School shall with the consent of the data subject:

- share personal data about parents and/or alumni, as appropriate, with organizations set up to help establish and maintain relationships with the School community, such as the Parents' Association, the Old Turians' Association and the UK Trust;
- contact parents and/or alumni (including via the organizations above by email in order to promote and raise funds for the School and, where appropriate, other worthy causes;

Should any individual wish to limit or object to any such use, or would like further information about them, contact should be made with the Admissions Director on Admissions.Director@turimail.co.ke in writing.

A data subject always has the right to withdraw consent, where given, or otherwise object to direct marketing or fundraising. However, the School may need nonetheless to retain some of your details

(not least to ensure that no more communications are sent to that particular address, email or telephone number).

14. Duty to Notify

The School must ensure that staff, parents and other data subjects are informed when personal data about them is being collected and their right to have their data protected and be advised of the reasons for obtaining the data.

15. Data Subjects' rights

Data subjects have various rights under Data Protection Laws to access and understand personal data about them held by the School, and in some cases ask for it to be erased or amended or for the School to stop processing it, but subject to certain exemptions and limitations as may be provided by law.

In particular, the School shall ensure that the following rights of data subjects (staff, parents, students etc.) are upheld:

- To be informed of the use for which personal data is to be put;
- To access personal data in the custody of the School;
- To object to processing of personal data;
- To correction of false or misleading information;
- To deletion of false or misleading information;
- To receive personal data in a portable format where personal data is requested.

Any individual wishing to access or amend their personal data, or wishing it to be transferred to another person or organization, or who has some other objection to how their personal data is used, should put their request in writing to the Legal & Compliance Officer on legalandcompliance@turimail.co.ke

The School will endeavor to respond to any such written requests as soon as is reasonably practicable and in any event within one month in the case of requests for access to information. The School will be better able to respond quickly to smaller, targeted requests for information. If the request is manifestly excessive or similar to previous requests, the School may ask the individual to reconsider or charge a proportionate fee.

Data subjects should be aware that certain data is exempt from the right of access. This may include information which identifies other individuals, or information which is subject to legal professional privilege. The School is also not required to disclose any student examination scripts (though examiners' comments may fall to be disclosed), nor any confidential reference given by the School for the purposes of the education, training or employment of any individual.

Students are required to respect the personal data and privacy of others, and to comply with the School rules set out in the Student Codes of Conduct. Staff are under professional duties to do the same covered under the Staff Code of Conduct.

16. Consent

The School acknowledges that consent granted to process personal data, may be withdrawn at any time. However, the School may have another lawful reason to process the personal data in question even without the data subject's consent.

That reason will usually have been asserted under this Policy or may otherwise exist under some form of contract or agreement with the individual (e.g. an employment or parent contract, or because a purchase of goods, services or membership of an organization such as an alumni or parents' association, has been requested).

The School will obtain parental consent to process personal data relating to students. The School may in extremely exceptional circumstances and in accordance with data protection laws process students' personal data without consulting the parents depending on the interests of the child, and the particular circumstances relating to the processing of that data.

17. Data accuracy and security

The School will endeavor to ensure that all personal data held in relation to an individual is as up to date and accurate as possible. Individuals must notify the Legal & Compliance Officer on legalandcompliance@turimail.co.ke of any significant changes to their personal information, such as contact details, held regarding them.

An individual has the right to request that any out-of-date, irrelevant or inaccurate or information about them is erased or corrected (subject to certain exemptions and limitations under Data Protection Law).

The School will take appropriate technical and organizational steps to ensure the security of personal data about individuals, including policies around use of technology and devices, and access to school systems. All staff and governors will be made aware of this policy and their duties under Data Protection Law and receive relevant training.

18. Data Breach

The School is required to put in place proper technical and organizational measures and integrated necessary safeguards to minimize the risk of any data breach. However, in the event any breaches occur the School should note to comply with the notification requirements of the DPA and take immediate action to remedy the breach.

19. Queries and complaints

Any comments or queries on this policy should be directed to the Legal and Compliance Officer on legalandcompliance@turimail.co.ke.

If an individual believes that the School has not complied with this Policy or acted otherwise than in accordance with data protection law, they should in the first instance raise the matter with the DPO. If the matter is not resolved with the DPO, the individual shall utilize the School Complaints Procedure which can be found on the School's website. Staff should use the School's Grievance Procedure which is available on the School's policy drive.

20. Compliance with the Policy

Compliance with Data Protection is the responsibility of all members of staff. Any deliberate or reckless breach of this Policy may lead to disciplinary, action. Any questions or concerns about the interpretation or operation of this policy should be taken up with the DPO.

21. Further Documentation

- Staff Privacy Notice
- CCTV Policy
- Use of Images of Children Policy
- Acceptable Use of IT Policy
- E-Safety Policy
- Retention of Records Policy
- Staff Code of Conduct
