St Andrew's School, Turi

Data Protection and Privacy Policy

Compiled by:	**Legal Counsel**
Reviewed by:	**Finance and Strategy Director**
Approved by:	**FAR & Board of Governors March 14, 2025**
Date of review:	**November 2024**
Date of next review:	**November 2025**

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 and may thus affect any of our students and employees. The School thus ensures 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

This Policy applies to all staff and Governors as well as persons working on behalf of the school including service providers involved in the processing of personal data, and are therefore required to comply with this Policy, as well as prevailing legislation on data protection. The School's Privacy Notice also provides further information on the use of personal data.

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; data breach refers to 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; significant data breach refers to data breach that could result in real risk of harm to the data subject and or cause reputational damage to the school.

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 unless an incident, guidance or new legislation requires an earlier date of review.

The school will directly communicate to staff, students, parents and any other data subjects on any substantial changes that may affect their rights as data subjects.

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 it processes personal and sensitive data. The DPO ensures that these data is processed in accordance with the law. The Legal Counsel & Company Secretary (legalandcompliance@turimail.co.ke) is the School's appointed DPO.

The DPO is also 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 data provided to the School regarding their employment is accurate and up-to-date.
- Review the data availed by the School from time to time in written or automated form, and inform the School of any errors or changes to be made and updated.

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 shall apply due care and due diligence in processing information held by the School and handle such information with appropriate care.

Staff shall at all times ensure that:

- All personal data is stored securely;
- They only process data relevant to their work needs;
- They hold data for the minimum duration required to fulfill their work;
- They destroy data when no longer required;
- They do not share data with any third party except expressly authorized by the data subject and approving authority within the School;
- They only process data they have authorized access to;
- Personal data is not disclosed to any unauthorized third party. Unauthorized disclosure may be treated as a disciplinary matter, and may be considered gross misconduct in some cases.

3. Principles

The School obtains holds and processes data relating to staff, students, parents and other data subjects for administrative, operational, and commercial purposes. The School also processes such data to fulfill legal obligations and contractual agreements.

Staff and other third parties must ensure that personal data is:-

- Processed in accordance with the data subject's right to privacy;
- Processed lawfully, fairly and in a transparent manner;
- Collected for explicit, specified and legitimate purpose and not further processed in a manner compatible with those purposes;
- Adequate, relevant and limited to what is necessary in relation to the purpose for which it is processed;
- Collected only where a valid explanation is provided whenever information relating to family or private affairs is required;
- Accurate, kept up to date and ensure that any inaccurate data is erased or rectified without delay;
- Kept in a form which identifies the data subjects 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.

The school ensures that any contracts with third parties have the necessary provisions binding each party to observe the provisions of the DPA.

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

These include but not limited to:

<u>Personal Data</u>

- Name, ID and passport number, postal and physical addresses, email addresses and other contact details.

Sensitive Personal Data

- Gender, nationality, ethnic social origin, religion;
- Marital status and family details e.g. names of spouse and children;
- biometric information;
- property details, bank details and other financial information, including parents paying 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;
- 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;
- students' images 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 ensures that personal data is collected from the data subject (in the case of students, from their parents) unless consent to obtain data from a third party or source is granted by the data subject. The data may be collected via forms, in the course of interaction or communication with the data subject (such as email or written assessments).

Personal data may also be supplied by third parties (for example another school, or other professionals or authorities working with that individual). The School shall notify the relevant data subject within fourteen (14) days of collection of the data from third parties.

The School obtains, holds and processes data for the following uses:

- student enrollment and to confirm the identity of prospective students and their parents;
- recruitment and employment of staff;
- 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;
- 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 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 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 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;
- for the school's operations and purposes including obtain appropriate professional advice and insurance for the School.

The School may process sensitive personal data relating to health, ethnicity, religion, 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. These reasons may include but not limited to:-

- to safeguard students' welfare and provide appropriate pastoral care
- to provide 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

The School will in the ordinary course of business and in fulfillment of its legal and statutory obligations share personal information relating to data subjects with relevant government authorities and agencies including KRA, the police, Ministry of Education or Immigration; as well as its professional advisers such as lawyers, accountants and auditors, to fulfill any contractual engagement between the school and such advisers.

The School recognizes that it may also receive legitimate and lawful requests for personal data from third parties eg lawyers. In this instance, staff are expected to seek the approval of their respective line managers, prior to sharing the data. The school shall upon such request, setting out the purpose for which the data is required and the duration the data will be retained share the requested personal data. The school shall also notify the relevant data subject of the same.

The school ensures that personal data is accessed and processed only by the relevant staff in fulfilment of their duties especially in relation to:-

- medical records which are 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 which are 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.

Data relating to SEN students will be provided to staff to provide the necessary care and education that the student requires.

The school is required to record or report incidences and concerns that arise or are brought to its attention. These may include file notes on personnel or safeguarding files, and in some cases referrals to relevant authorities such as the police which is considered as personal and sensitive information.

As such, parents and staff are required to notify the school of such incidences in line with the School's Safeguarding Policy.

The school also ensures that data processed on its behalf by third parties including web developers or cloud storage providers is done in accordance with the DPA and in line with contractual obligations relating to data protection.

7. Retention of Personal Data

The school shall retain data for the duration required to fulfill the purpose for which such data was collected and in line with the periods stipulated in the Retention of Records Policy**.**

The school may however retain incident reports and safeguarding files for longer durations in accordance with specific legal requirements.

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 that consider that their personal data is no longer relevant or required to be held by the school may request that the same is erased through contacting the Legal Counsel & Company Secretary on legalandcompliance@turimail.co.ke. However, despite such a request the School may have lawful reasons and obligations to hold on to some data.

8. Protection of Data

The school protects all personal data during collection, processing, storage, transit, usage and destruction from unauthorized internal and external disclosure. The school also restricts access to sensitive data 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.

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 Protection Impact Assessment

The school shall ensure that all new processes, projects and information systems are developed and implemented in a secure and structured manner and comply with data protection requirements. The school will therefore ensure that a formal assessment is completed to assess whether any new or proposed changes to its processes, projects and or information systems impacts on the integrity, confidentiality and accessibility of personal information.

The considerations (initial evaluation) that should be taken into account are whether the new or change in processes, or information system will:-

- Affect the quality of personal information already collected and held by the school;
- Allow personal information to be checked for relevancy, accuracy and validity;
- Have an adequate level of technical and organisational security measures to ensure that
- personal information is protected from unlawful or unauthorised access and from accidental loss, destruction or damage;
- Enable data retrieval to support continuity in school operations in the event of an emergency;
- Enable the timely location and retrieval of personal information to meet a data subject's access request.

Where after considering the above it is determined that the new or change in the school's processes or information system is likely to result in high risk to the rights and freedoms of any data subject by virtue of its nature, scope, context and purposes the school shall carry out a Data Protection Impact Assessment (DPIA).

The staff member and their respective Line Manager seeking to undertake the implementation of the new or change in the school's process, or systems with support from the DPO and the IT Manager will carry out the initial evaluation and DPIA.

The DPIA shall include the following:

I. A systematic description of the envisaged processing operations and the purposes of the processing, including, where applicable, the legitimate interest pursued by the data controller or processor.
II. An assessment of the necessity and proportionality of the processing operations in relation to the purposes.
III. An assessment of the risks to the rights and freedoms of data subjects.
IV. The measures envisaged to address the risks and the safeguards, security measures and mechanisms to ensure the protection of personal data and to demonstrate compliance with this Act, considering the rights, and legitimate interests of data subjects and other persons concerned.

The completed DPIA must be submitted to the DPO who will make an initial review of the completed DPIA and either request further information to satisfy regulatory requirements or otherwise pass the DPIA to the School Executive Committee for approval and sign off by the Director.

12. Data Portability

Data subjects have 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 data subject shall also have the right to request the school where technically possible, to directly transmit their data to another data controller or processor.

The School must comply with the request 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.

13. Transfer of Personal Data Outside Kenya

The School will 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

14. 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.

15. 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.

16. Data Subjects' rights

Data subjects have various rights under the DPA 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 Counsel & Company Secretary 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 seven days 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.

17. Consent

The School acknowledges that data subjects should issue consent to the school to collect and process their personal data. However, the School may have another lawful reason to process the personal data in question even without the data subject's consent (where appropriate, the school will inform the data subject that their data will be processed even without 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.

The school also recognizes the rights of data subjects to withdraw consent to process personal data previously given. The data subject is required to notify the DPO that they wish to withdraw their consent by sending an email to legalandcompliance@turimail.co.ke.
The DPO shall upon such notification from the data subject immediately inform the relevant staff /departments to cease any processing of the data subject's data and confirm this to the data subject in writing. The School may however for lawful reasons e.g. an ongoing court case, external or internal investigation or child safeguarding matter retain some or all of the data. Withdrawal of consent shall not affect the lawfulness of processing undertaken by the school based on prior consent before its withdrawal.

18. 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 Counsel & Company Secretary 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.

19. Data Breach

The School is has put in place proper technical and organizational measures and integrated necessary safeguards to minimize the risk of any data breach.

However, where personal data has been accessed by an unauthorized person either internally or externally, resulting in a real risk of harm to the data subject whose personal data has been subjected

to the unauthorized access, the DPO shall notify the Office of the Data Protection Commission within seventy-two hours of becoming aware of such breach in line with the DPA. The DPO shall also communicate to the data subject in writing within at least 14 days unless the identity of the data subject cannot be established. In cases involving breach of students' data the school shall notify the parents of such breach.

Immediately a data breach has been identified, the same will be reported to the direct line manager and the DPO.

As soon as an incident has been reported, measures must be taken to contain the breach, which will be assessed on a case by case basis. Such measures will be taken so as to stop any further risk/breach to the school, staff, students, third-party, systems or data prior to investigation and reporting.

The DPO will maintain an electronic log of all data breaches howsoever occurring, setting out the facts of the breach, its effects and the remedial action taken. The DPO shall also notify the Board through the Finance Audit and Risk Committee in its quarterly meetings of any data breaches.

However, in the event of the occurrence of a significant data breach, the DPO shall immediately inform the FAR Committee and the Board Chairman of the same.

The DPO is responsible for carrying out a full investigation, appointing the relevant staff to contain the breach, recording the incident on a breach incident form and making any relevant and legal notifications.

A full investigation is conducted and recorded on the incident form, with the outcome being communicated to all staff involved in the breach, in addition to the school executive committee. A copy of the completed incident form will be stored electronically for audit and documentation purposes.

20. Queries and complaints

Any comments or queries on this policy should be directed to the Legal Counsel and Company Secretary 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.

21. Compliance with the Policy

Compliance with Data Protection is the responsibility of all members of staff and all staff are thus required to read and familiarize themselves with this policy. 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.

The school shall provide at least an annual training to staff on data protection.

22. Further Documentation

- 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