PEMBROKE
HOUSE

DATA PROTECTION POLICY

Reviewed: October 2023 – CT, MAm, EM, IR & DN
Next Review: October 2024

Pembroke House Data Protection Policy

TABLE OF CONTENTS

DEFINITIONS

"Consent"	means any manifestation of express, unequivocal, free, specific, and informed indication of the data subject's wishes by a statement or by a clear affirmative action, signifying agreement to the processing of personal data relating to the Data Subject.
"Data Controller"	means an organisation that has full authority to decide how and why personal data is to be processed and has the overall responsibility for the data. This includes deciding on use storage and deletion of the data
"Data Subject"	means an individual who is the subject of personal data. It includes shareholders, directors, employees, consultants, suppliers, agents
"Data Controller"	A person nominated by the president (with the approval of the national Assembly) to oversee the implementation of and is responsible for the enforcement of the Data Protection Act, 2019.
Data Commissioner	means the Regulator appointed pursuant to the provisions of the Data Protection Act, 2019 and whose main responsibility is to oversee the implementation and enforcement of the Data Protection Act.
"Data Protection Impact Assessment"	This is an assessment done prior to rolling out any new process, system or policy relating to Personal Data that may impact a Data Subject's rights and freedoms. The Data Protection Impact Assessment is described in more detail in Clause 8 of this Policy.

Direct Marketing	Refers to communication by whatever means of any advertising or marketing material, which is directed to individuals, which includes sending a catalogue addressed to a subject through any medium, displaying an advertisement on an online media site a data subject is logged on using their personal data, including data collected by cookies. Relating to a website, it includes the data subject has viewed or sent an electronic message to a data subject about a sale or other advertising material relating to a sale. Using personal data provided by the data subject.
"Data Protection by Design and by Default"	Data protection by design means embedding data privacy features and data privacy enhancing technologies directly into the design of projects at an early stage. Data Protection by default means that user service settings must be automatically data protection friendly and that only data which is necessary for each specific purpose should be gathered.
Personal Data"	means information relating to an identified or identifiable individual/person. An identifiable individual is one who can be identified directly or indirectly in particular reference to an identifier such as a name, identification number, location data, an online identifier or to one or more factors specific to physical, physiological, genetic, mental, economic, cultural, or social identity of that natural person.
"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"	Any action taken with personal data. It includes collection, use, storage, disclosure, destruction, or retention of data.
"Sensitive Personal Data"	Means information revealing a person's race, health status, ethnic social origin, conscience, belief, generic data, biometric data, property details, marital status, family details.

Pembroke House Data Protection Policy

1. Policy Statement

1.1. The objectives of this Data Protection Policy are to ensure that Pembroke House School (the "School") and its governors and employees are informed about, and comply with, their obligations under the Data Protection Act, 2019 and supporting regulations ("data protection laws") and other data protection legislation.

1.2. The School is the Data Controller for all the Personal Data processed by the School.

1.3. Everyone has rights with regard to how their personal information is handled. During the course of our activities we will process personal information about a number of different groups of people and we recognise that we need to treat it in an appropriate and lawful manner.

1.4. The type of information that we may be required to handle include details of job applicants, current, past and prospective employees, pupils, parents / carers and other members of pupils' families, governors, suppliers and other individuals that we communicate with. The information, which may be held on paper or on a computer or other media, is subject to certain legal safeguards specified in the Data Protection Laws. The Data Protection Laws impose restrictions on how we may use that information.

1.5. Breach of the Data Protection Act may expose the School to enforcement action by the Data Commissioner's Office, including the risk of fines. Furthermore, certain breaches of the Act can give rise to personal criminal liability for the School's employees. At the very least, a breach of the Data Protection Act could damage our reputation and have serious consequences for the School and for our stakeholders.

1.6. Any breach of this policy by members of employees will be taken seriously and may result in disciplinary action and serious breaches may result in dismissal.

1.7. This policy does not form part of any employee's contract of employment and it may be amended at any time.

2. Scope of this Policy

2.1. This Policy applies to all personal data created or held by the School in whatever format e.g., paper or electronic and however it is stored, for example, lockable cabinets, archives, email, personal filing drawers.

2.2. This policy should be read in conjunction with the School's other policies and procedures relating to data protection, including any relevant Privacy Notices, and the Policy Procedure for Handling Data Subject Rights.

2.3. This Policy applies to all employees of the School (meaning permanent, fixed term and temporary employees, any third-party representatives or consultants and interns) and pertains to the processing of personal information.

3. Roles and Responsibilities

3.1. The School Council: Overall responsibility of ensuring that the School meets its data protection compliance obligations lies with the School Council.

3.2. **The Headteacher:** The Headteacher is responsible for ensuring compliance with data protection legislation and this policy within the day-to-day activities of the school and that all employees are trained on data protection.

3.3. **The Data Protection Officer** ("DPO"): The Data Protection Officer is responsible for the School's Day to day compliance with the Data Protection Act. In particular, the Data Protection Officer has the following responsibilities: -

- to act as a central authority for the implementation of the School's Data Privacy Program.
- to develop and maintain the School's Data Protection Policy and Manual.
- to monitor the School's compliance with the Data Protection Act 2019 and any other provisions of the law relating to data protection.
- to conduct Data Protection Impact Protection Assessments relative to the School's activities, measures, projects, programs, or systems.
- to advise the School regarding the exercise by Data Subjects of their rights.
- to cultivate awareness of privacy and data protection regulations within the Company, including this Manual, the Data Protection Act 2019 and its Regulations and any other government issuances on data privacy.
- to serve as the School's contact person vis-à-vis Data Subjects, the Data Commissioner and any other authorities in all matters relating to data protection.

3.4. Employee Responsibilities: Throughout the course of working with the School and depending on the nature of your role, you may have access to various extracts of personal data pertaining to pupils, parents/guardians, alumni, visiting speakers, employees (job applicants, employees, consultants, interns, casual labourers), suppliers, members of the public and website users. and any other individual, You are required:

- to abide by and follow the rules and guidelines contained in this Policy and any other data protection policies or rules that may be issued from time to time.
- to access or process personal data only where it is required as part of your role.
- to complete relevant data protection training, appropriate to your role.
- to follow advice, guidance and tools/methods issued from time to time on data protection compliance.
- to identify new systems, processes (including changes to existing processes) contracts, agreements and other activities involving personal data that may

require Data Protection Impact Assessments and cooperating with the Data Protection Officer or any advisors to support an assessment and implementation of recommendations to address risks as appropriate.

- when processing personal data on behalf of the School, to only use it as necessary for your role and not disclosing it unnecessarily or inappropriately.
- to recognise, report internally, and cooperate with any remedial work arising from personal data breaches.
- to recognise, report internally and cooperate with the fulfilment of data subject rights, requests when requested to do so by the Data Protection Officer.
- to ensure that any personal information provided to the School in connection with your employment, registration or other contractual agreement is accurate.
- to respond to requests to check the accuracy of the personal information held on them and processed by the School and informing the School of any errors or changes to be made.

**********INTENTIONALLY BLANK**********

4. Data Protection Principles

All employees of the School shall apply the following principles when processing personal data: -

Principle	Meaning of Principle	How it works in practice
Respect for Privacy	Personal data shall be processed in accordance with the right to privacy of the data subject.	All personal data processing activities must be geared towards respecting an individual's right to privacy. When handling personal data, ask yourself, how am I ensuring privacy of the information I am handling?
Lawfulness, fairness, and transparency	Personal data shall be processed lawfully, fairly and in a transparent manner in relation to the data subject.	a) **Lawfulness:** Whenever you process personal data, you must ensure that you have a lawful ground for and using personal data (**see 5.2 on the lawful grounds we apply**). b) **Transparency:** At the School, we provide information to data subjects concerning how we process their personal data. This information is provided at the point of collection of the data by way of privacy policies which must be written in clear and plain language and easily accessible to the data subjects. c) **Fairness**: you are expected to handle personal data in a way that the data subject would reasonably expect you to. We endeavour to: - o grant data subjects the highest degree of autonomy with respect to control over their personal data.

Principle	Meaning of Principle	How it works in practice
		o enable data subjects to exercise and communicate their rights. o eliminate discrimination against a data subject o guard against the exploitation of the needs or vulnerabilities of a data subject. o incorporate human intervention to minimise biases that automated decision-making processes may create.
Data Minimisation	Personal data must be adequate, relevant, and limited to what is necessary in relation to the purposes for which they are processed.	At the School we only process the minimum amount of personal data required to achieve the objective and purpose for which the data was collected. Ask yourself: - o Why do I need this information? o How is this data relevant to the processing in question? o Do I need to pseudonymised personal data that is no longer necessary? How can I achieve this? o Do I need to anonymise personal data where it is no longer necessary for its purpose? o What technologies can we adopt to achieve data minimisation?
Purpose Limitation	Personal data shall be collected for explicit, specified, and legitimate purposes and not further processed in a manner	Before we process any personal data, you must: - ● be clear about why you are collecting personal data and what you will do with it,

Principle	Meaning of Principle	How it works in practice
	that is incompatible with those purposes	• communicate or confirm that we have communicated to the data subject, through a privacy policy, the reasons why you need the data • not use personal data for reasons other than what has been specified/communicated to the data subject.
Valid Explanations for family information	Personal data relating to an individual's family or private affairs must only be collected where a valid explanation is provided	
Accuracy	Personal data must be accurate and where necessary, kept up to date, with every reasonable step being taken to ensure that any inaccurate record of personal data is erased or rectified	• We must periodically review the data we have collected to confirm if it is accurate and up to date.
Storage Limitation	Personal data should be kept in a form which identifies the data subjects for no longer than is necessary for the purpose for which it was collected.	At the School, we regularly: • maintain personal data in accordance with our Data Retention and Disposal Policy • review the length of time we keep personal data • delete or anonymise personal information that is no longer necessary • ensure that it is not possible to re-identify anonymised data or recover deleted data
Transferability	Personal data shall not be transferred outside Kenya,	At the School, we endeavour to respect this principle and have put in place measures to: -

Principle	Meaning of Principle	How it works in practice
	unless there is proof of adequate data protection safeguards or consent from the data subject	● determine whether the country you are transferring the data to has adequate data protection safeguards ● seek clearance from the Data Commissioner before transfer ● ensuring adequate safeguards and protections of the Data

5. Lawfulness Grounds for Processing

The School must determine the lawful grounds for processing before starting any collection of personal data. All lawful grounds are set out in section 30 of the Act and at least one of these must apply whenever personal data is processed. These grounds are identified prior to data collection and processing and included in relevant privacy policies.

Lawful Basis	Meaning	How it works in practice
Consent	The individual has given clear consent to process their personal data for a specific purpose.	● We only rely on consent where the following conditions have been met: - o Before collection of the data, the data subject has been fully informed either by written notice, oral statement and audio or visual message: - ▪ the identity of the data controller or data processor. ▪ the purpose of each of the processing operations for which consent is sought. ▪ the type of personal data that is collected and used. ▪ information about the use of personal data for automated decision-making, where relevant.

Lawful Basis	Meaning	How it works in practice
		▪ the possible risks of data transfers due to absence of an adequacy decision or appropriate safeguards. ▪ whether personal data shall be shared with third parties ▪ the right to withdraw consent o the data subject has capacity to give Consent. o the data subject voluntarily Consent o the Consent is specific to the purpose of processing o where information relates to a child, a parent has been given full information on the consent and the parent takes an affirmative action to signify consent o the data subject has been informed that he/she has the right to withdraw the consent at any time. o the data subject has been informed on how they can withdraw consent. o the data subject has been informed on the implications of providing, withholding, and withdrawing consent. ● In case Consent is provided orally, the person obtaining the consent must keep a record on how and when the consent was obtained.

Lawful Basis	Meaning	How it works in practice
		● where a data subject withdraws consent, we shall restrict the aspect of processing of which the consent is withdrawn. ● due to the technical nature of Consent, you are advised to consult the Data Protection Officer before relying on Consent as a ground for processing personal data.
Contract	The processing is necessary for a contract with the individual, or because the individual has asked the School to take specific steps before entering a contract.	Personal data of information from pupils, parents/guardians, alumni, visiting speakers, employees (job applicants, employees, consultants, interns, casual labourers), suppliers, members of the public and website users. any other individual may be processed on the basis that such processing is necessary for the School to enter a contract with them. For example, we may need personal data to onboard new investors or to fulfil investor orders. We may also need personal data for: - ● Recruitment, employment, and management of employees
Legal Obligation	the processing is necessary to comply with the law (not including contractual obligation)	The School processes personal data in compliance with legal obligations or laws to which it is subject. For example, we process PINs to comply with tax laws, NSSF and NHIF to comply with employer obligations set out in NSSF and NHIF Acts of Parliament.
Vital interests	The processing is necessary to protect the vital interests of the data subject or another natural person	This means that the processing necessary to protect someone's life, dignity, security, or health.

Lawful Basis	Meaning	How it works in practice
Public task	the processing is necessary for the performance of any task carried out by a public authority	This applies where The School is requested by a public authority to carry out any processing.
Public Interest	The processing is necessary for the exercise, by any person in the public interest, of any other functions of a public nature	This applies where there is a clear public interest to pursue such processing. Consult the Data Protection Officer before you rely on this ground for processing
Legitimate Interests:	The processing is necessary for The school's legitimate interests or the legitimate interests of a third party to whom the data is disclosed, except if the processing is unwarranted in any particular case having regard to the harm and prejudice of the rights and freedoms or legitimate interests of the data subject.	The School processes personal data on basis of legitimate interests provided that the rights and interests of individuals are not prejudiced. Before relying on this basis, you must do an assessment test to check in whose favour the interests lie. The matters we consider include: - ● Whether the interest is legal (the interest must be legal) ● Whether the interest represents a genuine and direct need for the company ● Whether the same result can be achieved through means that are less invasive of the privacy of the data subject ● The nature of the School /the third party's interest in the processing ● The benefit that the processing would provide ● The detriment that may ensue from the processing ● The effects of the processing on the data subject ● How the processing measures would affect the data subject

Lawful Basis	Meaning	How it works in practice
		If the processing presents more risks to the data subject than to the School, then this may not be an appropriate ground for processing
Historical, statistical, journalistic, literature, art or scientific research purposes	The School may process personal data for the purpose of historical, statistical, journalistic, literature and art or scientific research. For example, we may use investor data to analyse trends and enhance our website.	

6. Data Subject Rights

6.1. The Data Protection Act, 2019 grants data subjects the following rights over their Personal Data:

- Right to information
- Right of access
- Right to rectification
- Right to erasure
- Right to restrict processing
- Right to data portability
- Right to object
- Right to automated decision making

6.2. Please refer to Procedures for Handling Data Subject Requests set out here for elaboration on how to facilitate Data Subject's Rights.

6.3. All data subject requests must be brought to the attention of the Data Protection Officer on insert email If an employee fails to inform the DPO of the request, they may be liable to disciplinary action.

6.4. The DPO shall, with the assistance of relevant employees, ensure that all Data Subject requests are responded to within the timeframes set out in this manual.

6.5. Failure to respond to the requests within the stipulated timelines may lead to disciplinary action.

7. Privacy by Design and by Default

7.1. The School observes the principles of privacy by design in its approach to data protection compliance. Privacy by design is an approach that promotes privacy and data protection compliance before rolling out a new system, project, process, system, or initiative that involves the use of personal data.

7.2. We assess what Privacy by Design and by Default measures can be implemented on all programs, systems, or processes that Process Personal Data by taking into account the following:

- The state of the art
- The cost of implementation
- The nature, scope, context and purpose of Processing
- The risks of varying likelihood and severity of rights and freedoms of the Data Subjects posed by the Processing.

7.3. Where a project, system, process, or initiative presents a hight risk to the data subjects, a Data Protection Impact Assessment (see clause 8 below) must be carried out.

7.4. When purchasing systems/software which involve personal data or considering transfers. Sharing of information on the "cloud", employees must evaluate the privacy and security of alternative solutions and vendors/partners. The use of such systems/software should to the maximum extent possible avoid personal data from being put at risk of data breach.

7.5. Employees should not purchase new the School systems or software without first undertaking a Data Protection Impact Assessment. All new systems/software purchases involving the use of personal data must be signed off by the DPO and Headmistress.

7.6. All suppliers must be vetted in accordance with our Vendor Data Protection requirements policy and there should be an appropriate data processing contract in place with each vendor

8. Data Protection Impact Assessments

8.1. The Act requires the School to carry out Data Protection Impact Assessments ("DPIA's) in certain circumstances.

8.2. The purpose of a Data Protection Impact Assessment is to identify, evaluate and address the risks to data subjects arising from the implementation of a given system, policy, or process.

8.3. The School will conduct DPIA's in all instances where personal data processing is likely to result in a high risk to the rights and freedoms of data subjects. Examples of instances where DPIA's will be conducted include where the processing involves: -

- automated decision making with legal or similar significant effects that include the use of profiling or algorithmic means or use of sensitive personal data as an element to determine access to services or that results in legal or similarly significant effects.
- use of personal data on a large-scale for a purpose other than that for which it was initially collected.
- processing biometric or genetic data.
- processing that involves financial and reputational benefits, demonstrating accountability and building trust and engagement with data subjects.
- where there is a change in any aspect of the processing that may result in higher risk to data subjects.
- processing sensitive personal data or data relating to children or vulnerable groups.
- combining, linking, or cross-referencing separate datasets where the datasets are combined from different sources and where processing is carried out for different purposes
- large scale processing of personal data
- a systematic monitoring of a publicly accessible area on a large scale

- innovative use or application of new technological or organizational solutions.
- where the processing itself prevents a data subject from exercising a right.

- The process of conducting a DPIA is consultative and includes: -
  - consulting relevant stakeholders to obtain their views on proposed system or project
  - identification of risks
  - assessment of risks
  - identification of solutions/mitigation measures
  - implementation of the DPIA

8.4. If you intend to implement or roll out a project, process, or system with any of the above components, consult the DPO prior to implementation, for guidance on how to undertake the DPIA.

8.5. Where an DPIA indicates a high-risk data processing, The School will consult the office of the Data Commissioner to seek its opinion as to whether the processing operation complies with the Data Protection Act.

8.6. All employees must comply with The School guidelines on Data Protection Impact Assessments.

9. Data Security

9.1. The personal data that The School collects, and processes must be secured by appropriate technical and organisational measures against accidental loss, destruction, or damage and against unauthorised or unlawful processing.

9.2. All employees are responsible for ensuring the security of personal data processed by The School in the performance of the School duties and tasks. You must ensure that you follow all the procedures that the School has put in place to maintain the security of personal data from collection to destruction.

9.3. All employees shall be required to sign a Non-Disclosure or Confidentiality Agreement which fully details their duty of confidentiality as regard the personal data to which they are exposed to and as regards the personal data shared with them by third parties.

9.4. All employees must observe and comply with the School's ICT Policy and related policies.

9.5. No employee shall attempt to circumvent any administrative, physical, or technical measures that the School has implemented as doing so may result in disciplinary action and in certain circumstances, may constitute a criminal offence.

9.6. The School shall conduct training or seminars on data protection and security at least once a year to keep employees and personnel generally aware of personal data privacy and

protection and to make them familiar with the School policies and practices for compliance with the law. All employees must attend data protection training sessions as and when they are made available.

10. Personal Data Breaches

10.1. The term "personal data breach" refers to a breach of security which has led to the destruction, loss, alteration, unauthorised disclosure of, or access to, personal data.

10.2. Data breaches can occur for different reasons. They may be caused by employees, parties external to the organisation or computer system errors. Possible ways in which a data breach may occur, and the School employees should be thoroughly aware of, are: -

i. **Human Error**

- loss of laptop, phone, data storage devices or paper records
- sending personal data to a wrong email or physical address or disclosing data to a wrong recipient
- improper disposal of personal data (e.g., hard disk, storage media or paper documents containing personal data is sold or discarded before data is properly deleted.

ii. **Malicious Activities**

- *Denial of Service:* an attack that consumes the resources on a system or network, preventing normal use of resources for legitimate purposes
- *Malicious Code:* programs such as viruses, worms, logic bombs, Trojan Horses that are surreptitiously inserted into system to destroy data, run destructive or intrusive programs, or to otherwise compromise the security and/or integrity of the victim environment
- *Unauthorised Access:* Gaining or escalating privileges on any computer, network, storage medium, system, program, file, user area or other private repository without the express permission of the owner.
- *Attempted Unauthorised Access:* The precursor to unauthorised access, this incident typically manifests as repeated failed login attempts. As an example, brute force attempts can show tens or hundreds of failed logins per second.
- *Inappropriate Usage:* Employee activity on a system that violates any of the established business or security policies.
- *System Compromise / Defacement:* Escalated privileges on a system that leverages to access, modify, or otherwise compromise the integrity of residing data, processes, content or function of a system or website.

- **o** *Data Compromise:* A malicious or unauthorised third party that accesses, manipulates or appropriates personal data, including sensitive or confidential data.
- **o** *Social Engineering:* Technical and non-technical methods for acquiring information or access into an environment. Examples include fake emails containing malicious links or code (also known as phishing), phone calls from individuals pretending to be an employee or member, or physical access attempts by individuals who are not authorized to be in a facility.
- *o* *Computer System Errors*
- **o** *Blagging* i.e. offences where information is obtained by deceiving the organisation who holds it
- **o** *Unforeseen circumstances* such as flooding

iii. Physical Security breaches

- *o* *Loss of laptops or mobile computing devices*
- *o* *Loss of keys*
- *o* *Unauthorised access of locked files*
- *o* *Unauthorised access to Oral information e.g., meetings or conversations*

10.3. At Pembroke House School, we apply a consistent approach to all reported incidents to ensure that: -

- o incidents are reported in a timely manner and can be properly investigated
- o incidents are managed by appropriately authorised and skilled employees
- o appropriate levels of Management are involved in response management
- o incidents are recorded and documented
- o the impact of the incident is understood, and action is taken to prevent further damage
- o evidence is gathered, recorded, and maintained in a form that will withstand both internal and external scrutiny
- o as appropriate, data subject or Data Protection Authorities are notified
- o timely management of incidents with minimal disruption to operations
- o incidents are reviewed to identify policy or procedure improvements.

10.4. Under the Data Protection Act, any confirmed or suspected personal data breaches must be reported to the Data Commissioner within 72 hours of the School becoming aware of the incident. Therefore, due to the tight timelines involved, employees strictly adhere to the reporting procedures set out in this policy.

- o If an employee knows or suspects that a data breach has occurred, **the employee must immediately report the breach to the Data Protection Officer** through

the email dpo@pembrokehouse.sc.ke with a copy to the employee's line manager.

- Employees must not take any further action in relation to the reported event, including notification of any affected individuals or Data Protection Officers.

- The Data Protection Officer, in consultation with senior management and external lawyers, where necessary, are responsible for determining whether to notify any affected individuals, Data Protection Authorities or other third parties regarding a Personal Data Breach

10.5. Once a report is made, the Data Protection Officer shall constitute an Incident response team as per the School's Personal Data Breach Response Plan and take steps to:
- Investigate and assess the severity of the breach
- contain the data breach
- recover, rectify, or delete the data that has been lost, damaged, or disclosed
- assess and record the breach in the school's data breach register
- Notify the Data Commissioner
- Notify the data subjects affected by the breach
- Notify other appropriate parties to the breach
- Take steps to prevent future breaches.

10.6. All data breaches will be documented irrespective of whether the breach is reported to the Data Commissioner. A log of all breaches shall be maintained by the Data Protection Officer.

10.7. The School may, where appropriate, take disciplinary action against any workforce members who contributed to the incidents, up to and including termination of employment for incidents resulting from unauthorised access and hacking, the company may consider legal action including cease and desist letters and civil lawsuit(s) where appropriate.

11. Data Retention

11.1. Personal data shall be retained only for the duration necessary to fulfil the identified lawful business purpose. All personal data of the data subjects shall be retained only for as long as necessary:
- for fulfilment of the declared, specified, and legitimate purpose, or when processing the relevant to the purpose has been terminated; or
- for the establishment, exercise or defence or legal claims

- for legitimate business purposes, which must be consistent with standards followed by the industry
- in some specific cases, as prescribed by law.

11.2. The School shall retain personal data in accordance with its Data Retention and Disposal Policy.

11.3. Upon expiration of identified lawful purposes or withdrawal of consent. The School shall take reasonable steps to securely destroy or permanently de-identify or anonymise any personal information if it is no longer needed. Data may be pseudonymised or anonymised, as deemed appropriate, to prevent unique identification to an individual.

11.4. Personal data shall not be retained in perpetuity in contemplation of a possible future use yet to be determined.

12. Direct Marketing

12.1. Direct marketing is marketing which is directed to specific individuals.

12.2. The use of personal data for direct marketing purposes is permitted where: -

- The School has obtained the data subject's express consent; or
- The School is authorised to do so by written law and the data subject has been informed of this through a Privacy Policy provided prior to collection of the personal data.

12.3. The use of sensitive personal data for direct marketing purposes is expressly forbidden.

12.4. When contacting individuals for direct marketing in whatever form, the following conditions must be followed: -

- The School provides a simple means by which the data subject may easily request not to receive (i.e., to OPT OUT) direct marketing communications from the School
- The School must confirm that the data subject has not exercised his right to OPT-OUT
- The School will not charge the data subject for giving effect to a request to OPT OUT of receiving direct marketing communications.

13. Sharing Personal Data

13.1. Generally, you are not allowed to share Personal Data with third parties unless certain safeguards and contractual arrangements have been put in place.

13.2. You may only share Personal Data held by the School with another employee, Child Protection Officer, Police, Parent or, third party medical providers, the IAPS on a need-to-know basis.

13.3. You may only share the Personal Data we hold with third parties named above if: -

- they have a need to know the information for the purposes of providing the contracted services.
- sharing the Personal Data complies with the Privacy Notice provided to the Data Subject and, if required, the Data Subject's Consent has been obtained.
- the third party has agreed to comply with the required data security standards, policies, and procedures, and put adequate security measures in place.
- the transfer complies with any applicable cross-border transfer restrictions.

14. Inquiries and Complaints

14.1. The DPO shall receive all inquiries and complaints related to the privacy of a data subject and, where necessary, institute investigations. All complaints shall be sent to dpo@pembrokehouse.sc.ke

14.2. Data subjects may inquire or request for any information regarding any matter relating to the processing of their personal data under the custody of the School, including data privacy and security policies implemented to ensure the protection of their personal data. They may write to the DPO and briefly discuss the inquiry, together with their contact details for reference.

14.3. The Data Protection Officer shall maintain a log of all inquiries and complaints.

15. Changes to this Manual

15.1. The School reserves the right to modify this manual from time to time to accurately reflect the regulatory environment and data protection principles.

15.2. Where any material changes are made to this manual, the School shall without undue delay notify its employees.

ACKNOWLEDGEMENT OF RECEIPT

I, _____ acknowledge that on this _____ day of _____ I received and read a copy of the Pembroke House School's Data Protection Policy dated and understand that I am responsible for knowing and abiding by its terms. I understand that the information in this Data Protection Policy is intended to help Company Personnel work together effectively on assigned job responsibilities and assist in the use and protection of Personal Data.

I understand that this Data Protection Policy does not set terms or conditions of employment or form part of an employment contract.

Signed …….

Name …….

Date ……