PEMBROKE
HOUSE

DATA PROTECTION POLICY

Contents

1. POLICY STATEMENT

1.1. This Policy aims to provide a guide on how to handle and protect the personal data of individuals in our school community.

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

2. SCOPE OF THE 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 or in electronic information systems.

2.2. 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. DEFINITIONS

3.1. "**Data Subject**" means an identified or identifiable natural person who is the subject of personal data. It includes pupils, parents, guardians, visitors, directors, employees, consultants, suppliers.

3.2. **"Personal Data"** means information relating to an identified or identifiable individual/person. An identifiable individual is one who can be identified directly or indirectly by 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.

3.3. "**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.

3.4. "**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.

4. ROLES AND RESPONSIBILITIES

4.1. The School Council: The Council shall have the overall responsibility of ensuring that the school meets its data protection compliance obligations under relevant data protection legislation.

4.2. 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.

4.3. Data Protection Officer (DPO) is responsible for:

a. Advising the school on data processing requirements provided for under the Kenya Data Protection Act, 2019 or any other written law.

b. Ensuring on behalf of the school that the Data Protection Act 2019 is complied with.

c. Facilitating capacity building of staff involved in data processing operations

d. Providing advice on data protection impact assessments

e. Cooperating with the Data Commissioner and any other authorities, on behalf of the school on matters relating to data protection.

You can reach out to the DPO with any questions or concerns about data protection at dpo@pembrokehouse.com

4.4. 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:

a. 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.

b. Access or process personal data only where it is required as part of your role.

c. Complete relevant data protection training appropriate to your role.

d. Follow advice, guidance and tools/methods issued from time to time on data protection compliance.

e. Employees should approach the DPO with any data protection questions or concerns.

5. PRINCIPLES OF DATA PROTECTION

5.1. All employees must adhere to the following data protection principles when handling personal data:

a) **Respect for Privacy:** Personal data must be processed in accordance with an individual's right to privacy.

b) **Lawfulness, Fairness, and Transparency:** Personal data must be processed lawfully, fairly, and in a transparent manner.

c) **Purpose Limitation:** Data should be collected for specified, explicit, and legitimate purposes and not further processed in a manner incompatible with those purposes.

d) **Data Minimisation:** Personal data should be adequate, relevant, and limited to what is necessary in relation to the purposes for which they are processed.

e) **Accuracy:** Personal data should be accurate and, where necessary, kept up to date.

f) **Storage Limitation:** Personal data should be kept in a form that permits identification of data subjects for no longer than is necessary for the purposes for which the data are processed.

g) **Integrity and Confidentiality:** Personal data should be processed in a manner that ensures appropriate security, including protection against unauthorised or unlawful processing and against accidental loss, destruction, or damage.

6. PRIVACY BY DESIGN AND BY DEFAULT

6.1. We integrate data protection measures into the design and operation of our systems, processes, and services from the outset. This proactive approach ensures that privacy considerations are embedded at every stage of our activities. We implement technical and organisational safeguards to protect personal data against unauthorised access, disclosure, or misuse. Our goal is to create systems and processes that uphold data protection principles by design, thereby minimising risks and enhancing the security of personal data.

6.2. We also configure our systems and processes to ensure that privacy settings are set to the highest level by default. Personal data is collected and processed only to the extent necessary for the intended purpose. We limit data sharing to what is legally required or explicitly consented to by the data subject. This approach ensures that personal data is protected by default, with default settings favouring the highest level of privacy.

6.3. All employees and stakeholders must adhere to these principles in their roles and responsibilities. Regular reviews and updates to our systems and processes will be conducted to ensure ongoing compliance with these principles. We are committed to fostering a culture of privacy and data protection within our organisation

7. GUIDELINES FOR HANDLING PERSONAL DATA RELATING TO SCHOOL VISITORS

1. **Types of Data Collected:**

    - **Visitor Log:** Name, contact details, purpose of visit, time of arrival, and time of departure.
    - **ID Verification:** An ID document (e.g., national ID or Passport, driver's licence).

2. **Best Practice Guidelines:**
   When handling visitors' data as part of your job requirements, take note of the following:

    - **Registration Process:** Ensure all visitors sign in upon arrival and sign out upon departure. The visitor log should be maintained securely and accessed only by authorised personnel.
    - **Data Minimisation:** Collect only the information necessary for security and administrative purposes.
    - **Access Control:** Limit access to visitor logs to authorised staff members only. Avoid sharing visitor information with third parties unless legally required.
    - **Retention and Disposal:** Retain visitor logs for a specified period (e.g. 12 months) and then securely dispose of them. If ID copies are taken, ensure they are destroyed after the visit unless otherwise required for security reasons.

Example: When a visitor arrives at the school, ask them to sign in and provide their name, identification information, contact information, and purpose of visit. All visitors must always wear badges.

8. HANDLING PERSONAL DATA RELATED TO PARENTS AND PUPILS

1. **Types of Data Collected:**
   - **Personal Information:** Names, addresses, contact numbers, email addresses, emergency contact details.
   - **Educational Records:** Academic performance, extra-curricular activities and records, attendance records, behavioural notes, special education needs (SEN) details.
   - **Sensitive Information:** Health records, religious beliefs, and any other information deemed sensitive.

2. **Best Practice Guidelines:**
   When handling parents and pupils' data as part of your job requirements, take note of the following:

a) **Data Collection:** Ensure that data collected from parents and pupils is necessary for school purposes or required by law. Obtain consent where necessary, particularly for use of images, marketing purposes or use of children's information.

b) **Secure Storage:** Store pupil records in secure school-approved systems, whether in physical filing cabinets or encrypted digital databases. Access should be restricted to teachers, administrative staff, and other authorised personnel.

c) **Data Sharing:** Share pupil data with external parties (e.g., other educational institutions, examination bodies) only when legally required or with explicit consent from parents or guardians.

d) **Parental Access:** Parents or guardians have the right to access their child's data. Ensure a clear process is in place for parents to request and receive copies of their child's records.

e) **Retention:** Retain pupil data for as long as the child is enrolled at the school and the period specified in our data retention and disposal policy or as required by law. Securely dispose of records after this period.

Practical Example: School Event Registration: When organising a school event, collect only the information required for the event, such as the names of attendees and emergency contact details. Avoid asking for unnecessary details like medical history unless it is relevant to the event (e.g., a sports day).

9. HANDLING EMPLOYEE-RELATED DATA

1. **Types of Data Collected:**
   - **Personal Information:** Names, addresses, contact numbers, statutory records
   - **Employment Records**: employment contracts, performance records, disciplinary records, payroll information.

- **Sensitive Information:** Medical information, criminal background checks next of kin details.

2. **Best Practice Guidelines:**
When handling employee data as part of your job requirements, take note of the following:

a) **Data Collection:** Collect staff data that is necessary for employment purposes, such as payroll, benefits, and performance management. Ensure consent is obtained, especially for use of images or children's data.
b) **Confidentiality:** Treat all staff data with strict confidentiality. Limit access to HR personnel, line managers, and other authorised individuals.
c) **Secure Storage:** Store physical records in locked cabinets and digital records in secure HR systems. Use measures approved by the IT department to protect digital files e.g. use of passwords.
d) **Data Sharing:** Share staff data with third parties (e.g., payroll processors, government agencies) only when necessary and with appropriate safeguards in place.
e) **Retention and Disposal:** Retain staff records for the duration of employment and for a legally specified period afterward. Securely dispose of records once they are no longer required.

Practical Example: During onboarding, collect only the necessary data from new staff, such as bank details for payroll and emergency contact information. Ensure that sensitive data, such as medical history, is collected only if it directly impacts job performance or workplace safety.

10. HANDLING HEALTH INFORMATION

1. **Types of Data Collected:**

a. **Pupil Health Information:** Allergies, chronic conditions, vaccination records, medication requirements.
b. **Staff Health Information:** Sick leave records, medical certificates, workplace accommodations.

2. **Best Practice Guidelines:**
When handling health data as part of your job requirements, take note of the following:

a) **Data Collection:** Collect health data only when necessary for the safety and well-being of pupils and staff. Ensure that data collection is proportionate and relevant.

b) **Secure Storage:** Store health records separately from other personal data, with heightened IT and physical security measures such as encryption and limited access. Physical records should be kept in a locked cabinet in the school nurse's office.

c) **Confidentiality:** Health data is particularly sensitive and should be accessed only by authorised individuals, such as the school nurse, HR personnel, or senior management when necessary.

d) **Data Sharing:** Share health data with external parties (e.g., healthcare providers, emergency services) only when necessary for the health and safety of the individual, and with appropriate consent.

e) **Retention:** Retain health data for as long as necessary to fulfil its purpose, such as during the period of a pupil's enrolment or an employee's tenure. Securely dispose of health records when no longer required.

Practical Example: Before a school field trip, collect updated health information and emergency contacts for all participating pupils. Ensure that teachers and trip organisers have access to this information during the trip. In addition, if a pupil has a medical emergency, provide the relevant health information (e.g., allergies, chronic conditions) to emergency responders to ensure they can provide appropriate care.

11. HANDLING ALUMNI DATA

1. **Types of Data Collected:**

    - **Biodata:** Names, contact details, addresses, and dates of attendance.
    - **Academic Records:** Degrees awarded, academic achievements, and participation in alumni activities.
    - **Sensitive Information:** Any sensitive data previously collected, such as health information if relevant to alumni services.

2. **Best Practice Guidelines:**

    a) **Data Collection**: Collect alumni data only for purposes that benefit alumni relations, such as event invitations, newsletters, or updates about the institution. Ensure that alumni are aware of how their data will be used and obtain consent where necessary.

    b) **Secure Storage**: Store alumni data in secure systems, whether physical or digital, with access limited to authorised personnel only. Employ encryption and other security measures to protect digital records.

c) **Data Sharing**: Share alumni data with third parties (e.g., event organizers, external partners) only when necessary and with explicit consent from the alumni. Ensure that any third parties comply with data protection requirements.

d) **Retention and Disposal**: Retain alumni data for as long as it is necessary to fulfil its purpose, such as maintaining connections or providing updates. Regularly review and securely dispose of data that is no longer needed or upon request from the alumni.

Practical Example: When organising an alumni event, collect only the necessary information such as names, contact details, and RSVP status. Ensure that you obtain consent from the alumni and that data used for event organisation is protected and used solely for the event's purpose.

12. DATA SUBJECT RIGHTS

a. All data subjects (individuals) have the following rights over their personal data:

a) Right to information
b) Right to access their personal data.
c) Right to request rectification of inaccurate or incomplete data.
d) Right to request erasure of their personal data (subject to certain conditions).
e) Right to restrict processing of their data.
f) Right to data portability.
g) Right to object to the processing of their data.
h) Rights related to automated decision-making
i) Right to grant consent for processing their personal data in certain instances and the right to withdraw that consent at any time.

b. All staff must:

a) Promptly escalate any data subject requests (e.g., access, rectification, or erasure) to the Data Protection Officer (DPO) or the designated authority within the school.

b) Record all data subject requests, including the nature of the request and the date received. This information should be stored securely for auditing purposes.

c) Ensure that data subject requests are handled confidentially, and that data is only disclosed to the appropriate individuals.

d) Verify the identity of the data subject before fulfilling any request.

e) Not obstruct a data subject's right to exercise their rights, nor delay or unjustifiably deny a request.

f) Work closely with the DPO and other departments to ensure timely and compliant responses to requests.

g) Communicate clearly with data subjects about the process of exercising their rights.

h) Adhere to legal requirements and internal procedures when handling data subject rights requests.

i) Report any challenges or breaches related to data subject requests.

13. WORKING WITH THIRD PARTIES

a) All third parties who process personal data on behalf of the school must be subject to data protection agreements that specify their obligations to maintain the confidentiality, security, and integrity of personal data.

b) Due diligence must be conducted on all third parties to assess their data protection measures before entering into any agreements.

c) Data sharing with third parties should be limited to what is necessary and lawful, with appropriate safeguards in place.

14. RESPONDING TO A PERSONAL DATA BREACH

In the event of a personal data breach:

a. **Immediate Reporting:** Staff must immediately report any suspected data breach to the Head Teacher, the School Bursar and the Data Protection Officer (Incident Response Team)

b. **Containment and Recovery:** Where required, employees must cooperate with the Incident Response Team, in relation to: -

   a) Any investigations into the nature and causes of the breach.

   b) containment the breach and recovery the data, where possible

c. **Review and Lessons Learned:** After the breach has been managed, review the incident to identify improvements that can prevent future breaches.

15. CONSEQUENCES OF NON-COMPLIANCE

Non-compliance with this policy can result in: -

- Disciplinary action, up to and including termination of employment.
- Legal action against the school, which may include fines and penalties.
- Reputational damage to the school, potentially resulting in a loss of trust from parents, staff, and the community.

16. MONITORING AND REVIEW

This Policy shall be reviewed annually, or more frequently if appropriate, to be consistent with future developments, industry trends and/or any changes in legal or regulatory requirements.