PEMBROKE
HOUSE

CCTV POLICY

Written: July 2022 – IR, CT, MAM & EM
Next Review: October 2023

Pembroke House CCTV Policy

TABLE OF CONTENTS

DEFINITIONS

"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 Processor"	means a natural or legal person, public authority, agency or other body which processes personal data on behalf of the Data Controller;
"DPO"	means the Data Protection Officer. This is the person within the organisation who is responsible for advising on and monitoring compliance with data protection laws.
"Data Protection Legislation"	means the Constitution of Kenya 2010, the Data Protection Act, 2019 and its attendant Regulations and any other relevant laws that may be enacted from time to time;
"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.
"Data Subject"	means an individual who is the subject of Personal Data. It includes shareholders, directors, employees, consultants, suppliers, agents;
"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; and
"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 CCTV Policy

1. Introduction

1.1. Pembroke House School ("the School") uses Close Circuit Television ("CCTV") within its premises. CCTV is used as a security measure to safeguard the School's property and business information.

1.2. We recognise that we collect personal data (i.e., images) belonging to our pupils, parents/guardians, employees i.e., teaching, administrative staff, casual workers, consultants and interns), persons visiting the school premises, alumni, suppliers, and members of the public. The School values the privacy of all its stakeholders and this policy sets out our position as to the management, operation, and use of the CCTV in its office premises.

1.3. The policy is formulated in compliance with Data Protection Legislation and current CCTV regulatory standards in Kenya and internationally.

2. Purpose of this Policy

2.1. This policy outlines the purpose, use and management of our CCTV monitoring system.

3. Scope of this Policy

3.1. This policy pertains to the use of CCTV monitoring at the School's premises.

3.2. This Policy applies pupils, parents/guardians, employees i.e., teaching, administrative staff, casual workers, consultants and interns), persons visiting the school premises , alumni, suppliers, and members of the public, or any other person whose personal information (i.e., images) may be captured using our CCTV system.

4. Roles and Responsibilities

4.1. The School Council has the ultimate responsibility for ensuring that the School complies with this policy.

4.2. The School Bursar is charged with the overall implementation of this policy.

4.3. ICT is responsible for the overall management and operation of the CCTV system, including activities relating to installations, recording, reviewing, monitoring, and ensuring compliance with this policy.

4.4. The Data Protection Officer("DPO") is responsible for the privacy and data protection aspects of this policy. Any questions you may have about this policy should be referred to the DPO.

4.5. This policy shall be reviewed annually by ICT in collaboration with the DPO.

5. CCTV System Overview

5.1. Management and Control of the CCTV System

5.1.1. The CCTV system is owned and managed by the School.

5.1.2. ICT is in-charge of the day-to-day running of the system. Under current Data Protection Legislation, the School is the 'Data Controller' for the images produced by the CCTV system.

5.1.3. The CCTV system operates to meet the requirements of the Data Protection Legislation and the relevant CCTV regulatory standards in Kenya and internationally.

5.2. Description of System

5.2.1. Our CCTV cameras are located in various locations within the School.

5.2.2. The CCTV system is operational and is capable of being monitored for 24 hours a day, every day of the year.

5.2.3. CCTV signs are placed all over the School to inform pupils, parents/guardians, employees i.e., teaching, administrative staff, casual workers, consultants and interns), persons visiting the school premises, alumni, suppliers, and members of the public that the school is under CCTV surveillance. The signage indicates that the system is managed by the School and a 24-hour contact number for the Security Control Centre is provided.

5.2.4. Any proposed new CCTV installation is subject to a Data Protection Impact Assessment.

6. Siting of Cameras

6.1.1. Cameras are sited to ensure that they secure the School's premises as far as is possible by monitoring vulnerable public facing areas.

6.1.2. Cameras will be sighted in prominent positions where they are clearly visible to all pupils, parents/guardians, employees i.e., teaching,

administrative staff, casual workers, consultants and interns), persons visiting the school premises, alumni, suppliers, and members of the public.

6.1.3. Cameras are not sited to focus on areas not intended to be monitored. The School will make all reasonable efforts to ensure that areas outside of our premises are not recorded.

6.1.4. Cameras will not be cited in areas where individuals have heightened expectations of privacy such as washrooms.

7. Purposes of the CCTV System

7.1. The School uses CCTV for the following purposes:

7.1.1. For the prevention reduction detection and investigation of crime and other security incidents

7.1.2. to promote the safety of all investors staff and members of the public

7.1.3. to assist in the investigation of suspected breaches of the School's regulations by staff

7.1.4. The School seeks to operate its CCTV system in a manner that is consistent with the right to privacy.

8. Guiding Principles

8.1. The School in its administration of the CCTV system complies with the Data Protection Legislation. In particular, we:

8.1.1. Respect the privacy of an individual when processing personal data.

8.1.2. Process personal information lawfully fairly and transparently

8.1.3. Collect data for specify the explicit and legitimate purposes and restricts processing to those purposes

8.1.4. Process personal data in a manner that ensures appropriate security and confidentiality of that information. We employ appropriate technical or organisational measures to protect your data against unauthorised access accidental loss destruction or damages

9. Data Subject Rights

9.1. Pupils, parents/guardians, employees i.e., teaching, administrative staff, casual workers, consultants and interns), persons visiting the school premises, alumni, suppliers, and

members of the public. have rights against the personal data we collect about them on our CCTV system. They have the following rights:

- 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

9.2. Data Subject requests will be handled according to our Policy Procedures for Handling Data Subject Rights and Requests.

9.3. Where the School is unable to comply with a Data Subject request without disclosing the personal data of another individual who is identified from that information, we are not obliged to comply with the request.

10. Disclosure of CCTV Images

10.1. In limited circumstances it may be appropriate to disclose images collected on our CCTV system to third parties. We may disclose personal information to third parties when it is required by law, in relation to the prevention or detection of a crime, or with a written law or court order.

10.2. Such disclosures will be made at the discretion of the head of IT in collaboration with their legal and compliance department, the head of security and the Data Protection Officer. Where a suspicion of misconduct arises and at the formal request of the investigating officer or the HR manager, CCTV images may be disclosed to be used in staff disciplinary cases.

11. Retention of Images

11.1. Images on our CCTV system are automatically overwritten after 30 days from the date of recording.

11.2. Where it is necessary to hold an image for longer than the period indicated above, for example for evidentiary purposes, the investigation of an offence or as required by law, this request will be in writing and directed to the Data Protection Officer.

11.3. The images held beyond their retention period will be reviewed on a three-month basis and any not required for evidentiary purposes will be deleted.

12. Inquiries and Complaints

12.1. 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 insert email

12.2. 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.

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

13. Policy Review

13.1. Pembroke House School reserves the right to modify this manual from time to time to accurately reflect the regulatory environment and data protection laws.

13.2. This policy will be reviewed annually by the head of the ICT to reflect current legislation and trends in the CCTV monitoring field.

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