HARRODIAN

CCTV Policy

1. Introduction

Harrodian takes the responsibility towards the safety of staff, visitors and pupils very seriously. To that end, we use surveillance cameras to monitor any instances of aggression or physical damage to our School and its members.

The purpose of this policy is to manage and regulate the use of the surveillance and CCTV systems at the School and ensure that:

- We comply with data protection legislation, including the **Data Protection Act 1998** and the **General Data Protection Regulation (GDPR)** – the latter of which came into effect on 25th May 2018.
- Any images that are captured are useable for the purposes that we require them for.
- We reassure those persons whose images are being captured, that the images are being handled in accordance with relevant data protection legislation.

This policy covers the use of surveillance and CCTV systems which capture moving and still images of people who could be identified, as well as information relating to individuals for any of the following purposes:

- Observing what an individual is doing.
- Taking action to prevent a crime.
- Using images of individuals that could affect their privacy.

2. Contents

This policy has due regard to legislation and statutory guidance, including, but not limited to the following:

- **The Regulation of Investigatory Powers Act 2000**
- **The Protection of Freedoms Act 2012**
- **The General Data Protection Regulation (GDPR)**
- **The Data Protection Act 1998**
- **The Freedom of Information Act 2000**
- **The Education (Pupil Information) (England) Regulations 2016**
- **TheFreedom of Information and Data Protection (Appropriate Limit and Fees) Regulations 2004**
- **The School Standards and Framework Act 1998**
- **The Children Act 1989**
- **The Children Act 2004**

- **The Equality Act 2010**
- **Home Office (2013) 'The Surveillance Camera Code of Practice'**
- **Information Commissioner's Office (ICO) (2017) 'Overview of the General Data Protection Regulation (GDPR)'**
- **ICO (2017) 'Preparing for the General Data Protection Regulation (GDPR) 12 steps to take now'**
- **ICO (2017) 'In the picture: A data protection code of practice for surveillance cameras and personal information'**

This policy should also be read alongside our *Health and Safety Policy*, *Emergency Policies* and *Pupil Safety Policy*.

3. Definitions

For the purpose of this policy, a set of definitions are outlined in accordance with the surveillance code of conduct.

Surveillance which includes monitoring the movements and behaviour of individuals; this can include video, audio and/or live footage.
Overt surveillance which includes any use of surveillance for which authority does not fall under the **Regulation of Investigatory Powers Act 2000**.

4. Chief Privacy Officer (CPO) Duties

On a day-to-day basis, the Headmaster's responsibility as regards the administration of the GDPR will be devolved to the CPO, who will:

- Deal with all Freedom of Information Requests and Subject Access Requests (SAR) in line with legislation, including the **Freedom of Information Act 2000**.
- Ensure that all data controllers at the School handle and process surveillance and CCTV footage in accordance with Data Protection legislation.
- Ensure that all surveillance and CCTV footage is obtained in line with legal requirements and this policy.
- Ensure that all consent is clear and positive and does not fall into non-compliance.
- Ensure that all surveillance and CCTV footage is destroyed in line with legal requirements when it falls outside of the relevant retention period.
- Keep comprehensive and accurate records of all data processing activities, including surveillance and CCTV footage, detailing the purpose of the activity and making these records public upon request.
- Inform data subjects of how their data will be used by the School, their rights for the data to be destroyed and the measures implemented by the School to protect personal information.
- Prepare reports and management information on the School's level of risk related to Data Protection.
- Monitor the performance of the School's Data Privacy Impact Assessment and provide advice where requested.

5. Data Controller Duties

Harrodian is the data controller. The Proprietor, Headmaster and the Operations Director have overall responsibility for ensuring that records are maintained, including security and access arrangements in accordance with regulations. They will meet with the CPO to decide where CCTV is needed to justify its means, ensure that lawful processing of the surveillance and CCTV footage takes place, review the CCTV Policy to ensure it is compliant with current legislation, monitor legislation to ensure the School is using the surveillance fairly and lawfully and they will communicate any changes to legislation with all members of the School staff.

The role of the data controller includes:

- Processing surveillance and CCTV footage legally and fairly.
- Collecting surveillance and CCTV footage for legitimate reasons.
- Collecting surveillance and CCTV footage that is relevant, adequate and not excessive in relation to the reason for its collection.
- Ensuring that any surveillance and CCTV footage identifying an individual is not kept for longer than is necessary.
- Protecting footage containing personal data against accidental, unlawful destruction, alteration and disclosure, especially when processing over networks.

6. Purpose and Justification

The School will only use surveillance cameras for the safety and security of the School, its staff, pupils and visitors.

Surveillance is used as a deterrent for violent behaviour and damage to the School and its property.

Under no circumstances are there any surveillance or CCTV cameras present in School classrooms or changing facilities.

7. The Data Protection Principles

Any data collected from surveillance cameras and CCTV will be:

- Processed lawfully, fairly and in a transparent manner in relation to individuals.
- Collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes – further processing for archiving purposes in the public interest, scientific or historical research or statistical purposes shall not be considered to be incompatible with the initial purposes.
- Adequate, relevant and limited to what is in relation to the purposes for which they are processed.
- Accurate and, where necessary, kept up-to-date with every reasonable step being taken to ensure that personal data that is inaccurate, is erased or rectified without delay.
- Kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data is processed. Personal data may be stored for longer periods, insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research or statistical

purposes subject to implementation of the appropriate technical and organisational measures required by the GDPR in order to safeguard the rights and freedoms of individuals.

8. Objectives

The surveillance system will be used to:

- Maintain a safe environment.
- Ensure the welfare of pupils, staff and visitors to the School.
- Deter any potential criminal acts against persons and/or property.
- Assist the police in identifying persons who have committed an offence, where necessary.

In the following locations:

Security Lodge: *Controlled and accessed by Moises de Matos, Daniel Dee, Alejandro Barroca and Hubert Ferte.*

DVR1:
1. Entrance gate (Main Building)
2. Security Lodge (Main Building)
3. Exit gate (Pre-Prep) M/Z
4. Pre-Prep building (Main Building) M/Z
5. Maintenance gate/field (cloister) M/Z
6. Car park (Music Block) M/Z
7. Main Building side entrance (Main Building) M/Z
8. Senior entrance (Senior Building) M/Z
9. Allotment gate/side Pre-Prep (Pre-Prep)
10. Pre-Prep pedestrian gate (Pre-Prep)
11. Front of Main Building (Main Building)
12. Entrance gate drive (Main Building)

DVR2:
1. Front door of Main Building (Main Building)
2. Bicycle rack (Main Building)
3. Lower sport field/break time area (Cloisters)
4. Back Main Building/Cloister entrance (Main Building)
5. Senior courtyard corridor between Cloister and Senior Building (Main Building)
6. Senior Library 1
7. Senior Library 2
8. Senior Building locker room

Sports Block: *Controlled and accessed by Ben Proudfoot and Dave Wicks*
4 cameras outside changing room entrances.

Maintenance office: *Controlled and accessed by Dave Wicks and Justin Wiseman*
4 cameras surveying tennis court, sport block, maintenance gate and garages.

Sixth Form office: *Controlled and accessed by Dave Wicks*
4 cameras surveying the 2 corridors and Room 606.

9. Protocols

- The surveillance system will be registered with the ICO in line with Data Protection legislation.
- The surveillance system is a closed digital system which does not record audio.
- Warning signs have been placed throughout the premises where the surveillance system is active, as mandated by the ICO's Code of Practice.
- The surveillance system has been designed for maximum effectiveness and efficiency, however, the School cannot guarantee that every incident will be detected and/or covered and that blind spots may exist.
- The surveillance system will not be trained on individuals unless an immediate response to an incident is required.
- The surveillance system will not be trained on private vehicles or private property outside the perimeter of the School.

10. Security

Access to the surveillance system, software and data will be strictly limited to authorised operators and will be password protected. The School's authorised CCTV system operators are: Moises de Matos, Daniel Dee, Alejandro Barroca, Ben Proudfoot, Dave Wicks, Justin Wiseman and Hubert Ferte (as listed at point **8**).

- The main control facility is kept secure and locked when not in use.
- If, in exceptional circumstances, covert surveillance is planned, or has taken place, copies of the Home Office's authorisation forms will be completed and retained.
- Surveillance and CCTV systems will be tested for security flaws annually to ensure that they are being properly maintained at all times.
- Surveillance and CCTV systems will not be intrusive.
- The CPO and Headmaster will decide when to record footage.
- Any unnecessary footage captured will be securely deleted from the School system.
- Any cameras that present faults will be repaired immediately so as to avoid any risk of a data breach.

11. Code of Practice

The School understands that recording images of identifiable individuals constitutes as processing personal information, so it is done in line with data protection principles.

The School notifies all pupils, staff and visitors of the purpose for collecting surveillance data via signs in the school grounds where cameras are based. CCTV cameras are only placed where they do not intrude on anyone's privacy and are necessary to fulfil their purpose. All surveillance will be kept for security purposes for 30 days for all equipment and cameras pertaining to the Security Lodge and for all other equipment and cameras.

The School has a surveillance system for the purpose of the prevention and detection of crime and the promotion of health, safety and welfare of staff, pupils and visitors. The surveillance and CCTV system is owned by the School and images from the system are strictly controlled and monitored by authorised personnel only.

The surveillance and CCTV system will:

- be designed to take into account its effect on individuals and their privacy and personal data. It will also be transparent and include the CPO as a designated contact point through which people can access information and submit complaints
- have clear responsibility and accountability procedures for all images and information collected, held and used
- have defined policies and procedures in place which are communicated throughout the School
- only keep images and information for 30 days
- restrict access to retained images and information. Only authorised system operators can access the system
- be subject to stringent security measures to safeguard against unauthorised access
- be regularly reviewed and audited to ensure that standards are met
- only be used for the purposes for which it is intended
- be accurate and well maintained to ensure all information is kept up to date

12. Access

Under the GDPR, individuals have the right to obtain confirmation that their personal information is being processed. Individuals have the right to submit a SAR to gain access to their personal data in order to verify the lawfulness of the processing. The School will verify the identity of the person making the request before any information is supplied.

A copy of the information will be supplied to the individual free of charge in the first instance. The School has the right to charge a fee for any requests for further copies of the same information. Where a request is unfounded, excessive or repetitive, a reasonable fee will be charged. Any fees will be based on the administrative cost of providing the information being requested.

Where a SAR has been made electronically, the information will be provided in a commonly used electronic format.

Requests made by persons outside the School for viewing or copying disks, or obtaining digital recordings, will be assessed by the CPO on a case by case basis with close regard to data protection and freedom of information legislation.

All disks containing images belong to, and remain the property of, the School.

All requests will be responded to without delay and at the latest within one month of receipt. In the event of numerous or complex requests, the period of compliance will be extended by a further two months. Individuals will be informed of this extension and will receive an explanation of why the extension is necessary, within one month of the receipt of the request.

Where a request is unfounded or excessive, the School holds the right to refuse to respond to the request. Individuals will be informed of this decision and any reasoning behind it, as well as their right to complain to the ICO, within one month of the refusal.

In the event that a large quantity of information is being processed about an individual, the

School will ask that individual to specify the information the request is in relation to.

It is important that access to, and disclosure of, the images recorded by surveillance and CCTV footage is restricted and carefully controlled, not only to ensure that the rights of individuals are preserved, but also to ensure that the chain of evidence remains intact, should the images be required for any evidential purpose.

Releasing any recorded images to third parties will only be permitted in the following limited circumstances, and to the extent required or permitted by law:

- The police, where the recorded images would assist in a specific criminal investigation.
- Prosecution agencies such as the Crown Prosecution Service (CPS).
- Relevant legal representatives including lawyers and barristers.
- Persons who have been recorded and whose images have been retained where disclosure is required by virtue of data protection legislation and the **Freedom of Information Act 2000.**

Requests for access will be recorded and the CPO will make the final decision as to whether recorded images may be released to persons other than the police.

Person responsible: Operations Director

Last update: September 2019
Next update: September 2020