HAYDON SCHOOL

Surveillance and CCTV Policy

Mission Statement

Haydon School is committed to the achievement of individual excellence, encouraging students to be creative and considerate, confident of their role in society and capable of rising to the challenges of a diverse and rapidly developing global economy.

Contents

Statement of Intent

At Haydon School ('the School'), we take our responsibility towards the safety of staff, visitors and students 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 2018 and the UK GDPR. We also seek to ensure compliance with privacy laws;
- we reassure those persons whose images are being captured, that the images are being handled in accordance with data protection legislation as using of images of individuals could affect their privacy;
- the images that are captured are useable for the purposes we require them for.

This Policy covers the use of CCTV surveillance system and the door entry system (Paxton Entry system) which capture moving images of people who could be identified, as well as information relating to individuals for any of the following purposes:

- monitor the safety and security of the school site including identification of visitors at the school gates, observing what an individual is doing and identifying vehicle movement around the school site;
- maintain a safe environment, increase personal safety and reduce the fear of crime;
- act as a deterrent for inappropriate and anti-social behaviour;
- protect the School's buildings and our assets;
- deter criminal acts against the School's property;
- assist in the prevention, investigation and detection of crime;
- assist in the identification, apprehension and prosecution of offenders, including use of images as evidence in criminal proceedings;
- provide evidence for the School to use in our internal investigations and/or disciplinary processes in the event of behaviour by staff, students or other visitors on the site which breaches or is alleged to breach the School's policies.

The School uses CCTV only when it is necessary in pursuit of a legitimate aim and only proportionate to that aim. This Policy applies to all Haydon School staff and contractors who operate, supervise the operation of, and maintain the CCTV system and Paxton Entry system.

1.Legal framework

1.1 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 UK General Data Protection Regulation ('UK GDPR');
- The Data Protection Act 2018 ('DPA 2018');
- The Freedom of Information Act 2000;
- The Education (Pupil Information) (England) Regulations 2005 (as amended in 2016);
- The Freedom 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.

1.2 This Policy takes into account best practice as set out in codes of practice issued by the Information Commissioner and by the Home Office:

- Home Office (2021) 'The Surveillance Camera Code of Practice';
- ICO (2021) 'Guide to the UK general Data Protection Regulation (UK GDPR)';
- ICO (2017) 'In the picture: A data protection code of practice for surveillance cameras and personal information';
- ICO (2022) 'Video Surveillance'.

1.3. This Policy operates in conjunction with the following School's policies:

- E-Safety and ICT Policy;
- Freedom of Information Policy;
- GDPR Policy;
- Code of Conduct;
- Records Management and Retention Policy;
- Protocol for passing information to the Police.

1.4. This Policy should also be viewed in conjunction with our Privacy Notices (available on the School's website).

2.Definitions

2.1 For the purpose of this Policy the following definitions are given for the below terms:

- **surveillance** – monitoring the movements and behaviour of individuals; this can include video, audio or live footage e.g. real-time recordings and live streams. For the purpose of this Policy only video and audio footage will be applicable;

- o**overt surveillance** – surveillance which is clearly visible and signposted around the school site and does not fall under the Regulation of Investigatory Powers Act 2000;
- o**covert surveillance** – any use of surveillance which is intentionally not shared with the subjects it is recording. Subjects will not be informed of such surveillance;
- o**biometric data** – data which is related to the physiological characteristics of a person, which confirm the unique identification of that person, such as fingerprint recognition, facial recognition (FRT), or iris recognition. Sensitive data obtained via biometric technology will be processed via special conditions (listed in Article 9 of the UK GDPR).

2.2 The School does not condone the use of covert surveillance when monitoring the School's staff, students, governors, contractors, visitors and/or volunteers. Covert surveillance will only be operable in exceptional circumstances, for example to prevent or detect an unlawful act or other serious misconduct, and if there is no other less intrusive means of achieving those purposes. Covert surveillance will only be carried out for a limited period consistent with the purpose of the recording/monitoring. All decisions to engage in covert surveillance will be recorded and will be undertaken with the authorisation of the Headteacher (or in their absence Deputy Headteacher) or the Director of Finance and Operations.

3.Roles and responsibilities

3.1 Haydon School is the data controller.

3.2 **The Governing Board** of Haydon School has overall responsibility for ensuring that records are maintained, including security and access arrangements in accordance with regulations.

3.3 The role of the data controller includes:

- o processing surveillance and CCTV footage legally and fairly;
- o collecting surveillance and CCTV footage for legitimate reasons and ensuring that it is used accordingly;
- o collecting surveillance and CCTV footage that is relevant, adequate and not excessive in relation to the reason for its collection;
- o ensuring that any surveillance and CCTV footage identifying an individual is not kept for longer than is necessary;
- o protecting footage containing personal data against accidental and/or unlawful destruction, alteration and disclosure – especially when processing over networks.

3.4 The Governing Body has delegated day-to-day responsibility for implementation of this Policy to the staff identified below. All relevant members of staff have been made aware of the Policy and have received appropriate training.

3.5 The role of the **Data Protection Officer** (DPO) includes:

- dealing with Freedom of Information Requests and Subject Access Requests (SARs) in line with legislation, including the Freedom of Information Act 2000 and the UK GDPR;
- ensuring that surveillance and CCTV footage is obtained in line with legal requirements;
- ensuring consent is clear, positive and unambiguous - pre-ticked boxes and answers inferred from silence are non-compliant with the UK GDPR;
- keeping 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;
- informing data subjects of how their data captured in surveillance and CCTV footage will be used by the School;
- informing data subjects of their data protection rights;
- reporting on the School's level of risk relating to data protection to the highest management level of the School, the Governing Board;
- abiding by confidentiality requirements in relation to the duties undertaken while in the role;
- monitoring the performance of the School's Data Protection Impact Assessments (DPIAs), and providing advice where requested;
- where a high risk to individuals' interests is identified and it cannot be overcome consulting with the ICO;
- reviewing the Surveillance and CCTV Policy to ensure it is compliant with current legislation;
- advising on compliance with the UK GDPR and other data protection legislation and monitoring legislation to ensure the School is using surveillance fairly and lawfully;
- communicating any changes to legislation to all members of staff.

3.6 The role of the **Director of Finance and Operations** includes:

- ensuring that all school's employees and contractors handle and process surveillance and CCTV footage in accordance with data protection legislation;
- meeting with the DPO and the Network Manager to decide where CCTV is needed to justify its means;
- responsibility for the evaluation of the CCTV cameras location;
- responsibility for the evaluation of locations where live and recorded CCTV images are available for viewing, maintaining the list of such locations and the list of School's personnel authorised to operate CCTV system;

- o conferring with the DPO with regard to the lawful processing of the surveillance and CCTV footage;
- o conducting public consultation where required;
- o authorisation for new CCTV camera installation;
- o responsibility for ensuring compliance with this Policy;
- o preparing and presenting management information on the School's level of risk related to data protection and processing performance;

3.7 The role of the **Network Manager** includes:

- o responsibility for ensuring that the CCTV system specifications comply with the law and best practice referred to in clause 1 of this Policy;
- o informing data subjects of the measures implemented by the School to protect individuals' personal information via the E-Safety and ICT Policy;
- o ensuring that CCTV footage is kept for no longer than necessary and ensuring that surveillance and CCTV footage is destroyed in line with legal requirements when it falls outside of its retention period;
- o ensuring CCTV systems are tested for security flaws termly;
- o ensuring the system is being kept operational at all times;
- o protecting footage against accidental and/or unlawful destruction and/or alteration;
- o identification of system's faults and their repair in a timely manner;
- o maintaining a list of the CCTV cameras locations;
- o where new surveillance systems are proposed, consulting with the DPO to determine whether a prior DPIA is required;
- o conduct a DPIA on the DPO's recommendation;
- o record outcomes of the DPIA, including any difference of opinion with the DPO or individuals/ stakeholders consulted;
- o keep DPIAs under review and revisit them annually.

3.8 **Receptionist's** duties include:

- o monitor 'live' footage (external cameras only) where required, identify callers at the gates and Reception door and vehicle movement to ensure safety and security of the school's site, raise an alert of a potential unauthorised visitor;
- o ensure desktop monitor is facing away from the public.

4.Purpose and justification

4.1 The School will use surveillance cameras for the safety and security of the school site and our staff, students, contractors, volunteers and visitors.

4.2 Surveillance will be used as a deterrent for inappropriate and/or illegal behaviour and vandalism. Surveillance will be also used to assist with the identification, apprehension and prosecution of offenders as well as to assist

with the identification of actions that might result in disciplinary proceedings against staff and students.

4.3 In exceptional circumstances the School may consider installing a CCTV camera in a 'sensitive' area as an absolute last resort to address a particular serious concern (such as truancy, vandalism, fighting, smoking or safeguarding concerns) that cannot be addressed by less intrusive means. 'Sensitive' areas where there is a particularly high expectation of privacy include toilets and classrooms. If a CCTV camera is being installed in a sensitive location a DPIA will be updated to establish whether a more suitable alternative could be implemented. The cameras will not be concealed and appropriate signage will be installed both outside and within the sensitive area. The cameras will point away from the cubicles and the personal privacy of students, staff and visitors to the School will not be compromised.

4.4 If the surveillance and CCTV systems fulfil their purpose and are no longer required the School will deactivate them.

5.The data protection principles

5.1 Data collected from surveillance and CCTV will be:

- processed lawfully, as determined by a DPIA, or from advice from the DPO. In less common circumstances, lawful processing will be determined by a legitimate interests assessment (LIA). Sensitive data obtained via biometric technology will be processed via special conditions (listed in Article 9 of the UK GDPR);
- processed fairly in a manner that people would reasonably expect, and taking into account advancements in technology that may not be anticipated by some people;
- processed in a transparent manner, meaning that people are informed when their data is being captured;
- 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 purposes or statistical purposes shall not be considered to be incompatible with the initial purposes;
- adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed;
- accurate and, where necessary, kept up-to-date; every reasonable step will be taken to ensure that personal data that are inaccurate, having regard to the purposes for which the data are processed, are 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 are processed;
- processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.

6.Objectives

6.1 The surveillance system will be used to:

- Safeguard students, staff, governors and visitors to the school site and to maintain a safe environment;
- ensure the welfare of students, staff and visitors;
- increase personal safety and reduce the fear of crime;
- deter criminal acts against persons and property as well as anti-social behaviour and protect the School's buildings and our assets;
- assist with the identification, apprehension and prosecution of offenders;
- assist with the identification of actions that might result in disciplinary proceedings against staff and students.

7.Protocols and System Description

7.1 The surveillance system is registered with the ICO in line with data protection legislation.

7.2 The surveillance system is a closed digital system which could record audio. Please be advised that the audio recording feature is currently disabled. We will complete a DPIA and will let data subjects know by issuing a 'just in time' Privacy Notice if our position changes.

7.3 The CCTV system continuously records activities.

7.4 The CCTV system installed within the school site covers school's gates, building entrances, car parks, external arrears (such as courtyards, playing fields, tennis courts, Undercroft), internal areas (such as social spaces, Library, Canteen, Sixth Form Café, Sixth Form Common Room, Sixth Form Study Room, rooms with high value equipment, corridors and reception areas), and in exceptional circumstances and as an absolute last resort, within sensitive areas (toilets and classrooms). A list of locations is maintained by the Network Manager.

7.5 Warning signs have been placed throughout the premises where the surveillance system is active at strategic points including entrance and exit points, as mandated by the ICO's Code of Practice, so that students, staff, governors, contractors, volunteers, visitors and members of the public are made aware that they are entering an area covered by the CCTV. Warning signs will be more prominent in areas where surveillance is less expected to be in operation, and when using systems that can capture a large amount of personal data at one time. CCTV cameras are installed in such a way that they are not hidden from view.

7.6 The surveillance system has been designed for maximum effectiveness and efficiency; however, the School cannot guarantee that every incident will be detected or covered and 'blind spots' may exist.

7.7 The surveillance system is not generally trained on individuals or vehicles unless an immediate response to an incident is required. Please note that if a motion is detected, our external CCTV cameras can follow a detected individual/ vehicle on school site between the hours of 6pm and 6am.

7.8 The surveillance system will not be trained on private vehicles outside the perimeter of the School unless an immediate response to an incident is required.

7.9 The surveillance system will not be trained on private property outside the perimeter of the School.

8.Security

8.1 Access to the surveillance system, software and data is strictly limited to authorised staff that need to have access with the purposes of the system. The CCTV system is password protected, and where appropriate, will be encrypted.

8.2 Where large amounts of information need to be collected and retained, the School will consider using cloud storage. This will be secure and only accessible to authorised individuals.

8.3 The school's authorised CCTV system operators are:

- Headteacher;
- Deputy Headteachers;
- Director of Finance and Operations;
- Assistant Headteachers;

- DSL (or in their absence their Deputy);
- Year Leaders and their Deputies;
- Site Manager;
- Health and Safety Officer;
- Network Manager;
- IT Technician(s);
- HR Manager;
- Receptionists (access to external cameras only);
- Maintenance engineers authorised to install and/or maintain the system.

8.4 The DPO may be granted temporary access for the fulfilment of their tasks.

8.5 A list of the personnel authorised to view CCTV images is maintained by the Director of Finance and Operations.

8.6 Staff will be trained in security procedures, and sanctions will be put in place for those who misuse security system information. Staff will be made aware that they could be committing a criminal offence if they do this.

8.7 Access to images will be restricted to staff that need to have access in accordance with the purposes of the system. No unauthorised access will be permitted at any time. Access to images will be limited to the above authorised CCTV system operators and the school's employees who have been granted authorisation by the Headteacher or the Director of Finance and Operations as well as to the Police Officers where appropriate and any other person with statutory power of entry.

8.8 Before permitting access to the images, authorised CCTV system operators must satisfy themselves of the identity of any viewer and existence of the appropriate authorisation granted by the Headteacher or by the Director of Finance and Operations.

8.9 All access to the system must be logged in the Viewing Log (located in the shared CCTV folder on Google Drive).

8.10 Every Network Comms room is kept secure and locked when not in use.

8.11 Where authorised personnel access CCTV images/ recorded footage on a School's desktop, they must ensure that the images are not visible to unauthorised persons. Where images are accessed via a mobile device, same security protocol must be followed. **Desktop and mobile device screens must always be locked when left unattended.**

8.12 The School recommends using School's equipment to view images. In exceptional circumstances, when viewing CCTV images on a personal device, authorised operators must ensure the technology is in place to protect the footage and the authorised operators must be alert and security vigilant when accessing the images. No copies of the footage should be retained/saved on any personal device.

8.13 The ability to produce copies of information will be limited to the appropriate staff. All access and a record of any copies made must be maintained in the CCTV Viewing Log. Copies of any unnecessary footage will be securely deleted from the School's system.

8.14 Remote access to the School's systems must adhere to all policies that apply to their use. DPO advice on the use of personal devices for school related business and securing personal/home Wi-Fi must be strictly followed. Our E-Safety and ICT Policy must be strictly followed.

8.15 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.

8.16 Surveillance and CCTV systems will be tested for security flaws termly by the Network Team to ensure that they are being properly maintained at all times. Appropriate log of checks ('Maintenance log') will be maintained in the shared CCTV folder on Google Drive.

8.17 Any cameras that present faults will be repaired as soon as practical to avoid any risk of a data breach.

8.18 Surveillance and CCTV systems will not be intrusive.

8.19 Visual display monitors are located in Reception and Headteacher's Office.

9.Privacy by design

9.1 The use of surveillance cameras and CCTV will be critically analysed using a Data Protection Impact Assessment (DPIA), in consultation with the DPO.

9.2 A DPIA will be carried out prior to new installation of any surveillance, CCTV, or biometric system. A DPIA will be kept under review by the Network Manager and revised prior to any amendments to the existing surveillance and CCTV system.

9.3 A DPIA will:

- describe the nature, scope, context, and purposes of the processing;
- assess necessity, proportionality, and compliance measures;
- identify and assess risks to individuals;
- identify any additional measures to mitigate those risks.

9.4 If the DPIA reveals any potential security risks or other data protection issues, the School will ensure they have provisions in place to overcome these issues.

9.5 Where the School identifies a high risk to an individual's interests, and it cannot be overcome, the School will consult the ICO, and the School will act on the ICO's advice.

9.6 The School will ensure that the installation of the surveillance and CCTV systems will always justify its means.

9.7 If the use of a surveillance and CCTV system is too privacy intrusive, the School will seek amendments.

10.Code of practice

10.1 The School recognises that recording images of identifiable individuals constitutes as processing of their personal information and could affect individuals' privacy. Therefore, the School will ensure that the operation of its surveillance and CCTV system is consistent with the School's obligations outlined in the School's GDPR Policy (on the website) and is in line with the data protection principles.

10.2 The School notifies all students, staff and visitors of the purpose for collecting surveillance data via this Policy, our Privacy Notices and strategically placed signage.

10.3 Students, staff and visitors will be made aware of the following:

- whenever they are being monitored by a surveillance camera system;
- who is undertaking the activity;
- the purpose for which the associated information is being used.

10.4 CCTV cameras are mainly placed where they do not intrude on anyone's privacy and only placed where they are necessary to fulfil their purpose.

10.5 CCTV images are not retained for longer than necessary for the purposes for which they are being processed. Data storage is managed by the Network

Manager - historical data is overwritten in chronological order to produce an approximate thirty one day rotation in data retention. The images are automatically erased following the expiration of the retention period provided that there is no legitimate reason for retaining the CCTV images.

10.6 All retained CCTV footage will be stored securely on the School's Safeguarding or Data network drives and kept for no longer than necessary for the purpose for which they have been collected. The Network Manager will conduct an annual audit of all retained footage and will ensure that the footage is destroyed when it falls outside its retention period. Only images/footage that are still required for the purposes they have been collected for will be kept.

10.7 The surveillance and CCTV system is owned by the School and images from the system are strictly controlled and monitored by authorised trained personnel only.

10.8 The School will ensure that:

- the surveillance and CCTV system is used to create a safer environment for staff, students, governors, contactors and visitors to the School;
- CCTV system operation is consistent with the School's obligations outlined in data protection legislation;
- the School will seek solutions that warrant respect for individual privacy of our students, staff, governors, contractors and visitors.

10.9 The surveillance and CCTV system will:

- be designed to take into account its effect on individuals and their privacy;
- be transparent and include a contact point, info@haydonschool.org.uk, through which people can access information and submit complaints;
- have clear responsibility and accountability procedures for 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 as long as required for the purposes for which they have been collected;
- restrict access to retained images and information with clear rules on who can gain access;
- consider all operational, technical and competency standards, relevant to the surveillance and CCTV system and its purpose, and work to meet and maintain those standards in accordance with the law;
- be subject to stringent security measures to safeguard against unauthorised access;
- be regularly reviewed and audited to ensure that policies and standards are maintained;
- only be used for the purposes for which it is intended;

- will not be intrusive;
- be accurate and well maintained to ensure information is up-to-date.

10.10 The use of any video conferencing technology will be fair and transparent. Any students and staff who are part of any video conference calls will be informed of its purpose, and recording and publication of any video to an indefinite audience will be consented to and will not be used outside of the intended purpose.

11.Individual Rights and Access

11.1 Recorded images are considered to be personal data of individuals (data subjects) whose images have been recorded by the School's CCTV system.

11.2 Under the UK GDPR, individuals have the right to obtain confirmation that their personal information is being processed. Data subjects have a right of access to **their** personal data under the UK GDPR in certain circumstances, including the right to have their data erased, rectified, to restrict processing and to object to the processing of their personal data.

11.3 All recorded footage belong to, and remain the property of, the School.

11.4 Data subjects can exercise their rights by submitting a Subject Access Request (SAR) to gain access to **their** personal data in order to verify the lawfulness of the processing.

11.5 Individuals have the right to have personal data erased if:

- the data is no longer necessary for the original purpose it was collected for;
- the School is relying on legitimate interests as a basis for processing, the individual objects to the processing of their data, and there is no overriding legitimate interest to continue the processing;
- the data has been processed unlawfully;
- there is a specific legal obligation.

11.6 There are certain exceptions where the right to erasure cannot be exercised, these include, but are not limited to:

- where the processing is needed for the performance of a task in the public interest or an official authority;
- certain research activities;
- compliance with a specific legal obligation.

11.7 As an alternative to the right of erasure, individuals can limit the way their data is used if they have issues with the content of the data held by the School or they object to the way it was processed.

11.8 Data can be restricted by either:

- moving the data to another processing system;
- making the data unavailable to users;
- temporarily removing published data from a website.

11.9 All information requests should be submitted in writing to the DPO, dpo@haydonschool.org.uk.

11.10 The strict procedures will be followed in the event that a data request is received from an individual or a third party.

11.11 The School will verify the identity of the person making the request before any information is supplied.

11.12 In the event that a large quantity of information is being processed about an individual, the School will ask the individual to specify the information the request is in relation to.

11.13 Images that have been recorded may be viewed on site by the data subject whose images have been captured (or a parent/carer of a student if the student does not have sufficient understanding of their data protection rights or with their child's consent). **No copies may be taken off site or delivered electronically without the authorisation from the Headteacher.**

11.14 Where data requests contain the personal data of a separate individual, the rights and freedoms of others will be protected by asking for their consent, or removing specific footage where appropriate.

11.15 We may offer a transcript of the CCTV footage requested if we cannot ensure effective third party data redaction.

11.16 All requests will be responded to without delay and at the latest, within one month of receipt.

11.17 In the event of numerous or complex requests, the period of compliance will be extended by a further two months. The individual 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.

11.18 Where a request is manifestly unfounded or excessive, the School holds the right to refuse to respond to the request. The individual will be informed of this decision and the reasoning behind it within one month of the receipt of the request. The individual will also be informed of their right to complain to the ICO and to a judicial remedy.

11.19 Images may be viewed by the data subject on site free of charge. However, where a request is manifestly unfounded, excessive or repetitive, a reasonable fee will be charged. The School may impose a 'reasonable fee' to comply with requests for further copies of the same information. All fees will be based on the administrative cost of providing the information (available from the Director of Finance and Operations).

11.20 It is important that access to, and disclosure of, the images recorded by surveillance and CCTV footage are 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 evidential purposes.

11.21 Unlike data subjects, **third parties** who wish to have an access to CCTV images (i.e. images not of the person making the request) do not necessary have a right of access to images under the UK GDPR, and care will be taken when complying with such requests to ensure that neither the UK GDPR or the CCTV Policy are breached. Requests by persons outside the School for viewing or copying disks, or obtaining digital recordings, will be assessed by the Headteacher or the Director of Finance and Operations, who will consult the DPO, on a case-by-case basis with close regard to data protection and freedom of information legislation. Releasing the recorded images to third parties will be permitted only in the following limited and prescribed circumstances, and to the extent required or permitted by law:

- o the law enforcement agencies including the Police with a statutory right to obtain information – where the images recorded would assist in a specific criminal inquiry or help a uniform Police Officer with their response to an incident;
- o prosecution agencies – such as the Crown Prosecution Service (CPS);
- o relevant legal representatives – such as lawyers and barristers (the School may approach data subjects for their consent);
- o 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.

11.22 The images will be disclosed to law enforcement agencies including the Police once in possession of a written confirmation certifying that the images are required for an investigation concerning national security, the prevention or detection of crime, or the apprehension or prosecution of

offenders, and that the investigation would be prejudiced by failure to disclose the information. Where images are sought by other bodies/agencies to obtain information, evidence of that statutory authority will be sought before CCTV images are disclosed.

11.23 Where a request is made for a copy of the images by a law enforcement agency (for example, the Police), the images may be saved onto an encrypted memory device (all secure delivery methods will be considered) and passed to the law enforcement agency using secure method of delivery.

11.24 Requests for access or disclosure will be recorded by the DPO. The Headteacher or the Director of Finance and Operations in consultation with the DPO will make the final decision as to whether recorded images may be released.

11.25 Requests for CCTV information under the Freedom of Information Act 2000 will be considered in accordance with the School's Freedom of Information Policy.

12. Complaints

12.1 Complaints and queries regarding the CCTV system and its operation must be in writing to the DPO, dpo@haydonschool.org,uk, within seven days of the day of the incident giving rise to the complaint.

12.2 Complaints in relation to the release of images should be addressed to the Director of Finance and Operations as soon as possible and in any event no later than three month from the event giving rise to the complaint.

12.3 If a complainant is not satisfied with the response they may appeal to the Governing Body and the ICO. Please refer to our Complaints Policy on our website) for more information.

13.Monitoring and review

13.1 This Policy will be monitored and reviewed on a bi-annual basis to determine whether the use of the CCTV system remains justified.

13.2 Changes in the use of the CCTV system can be implemented only in consultation with the School's Data Protection Officer or the School's legal advisers.

13.3 The scheduled review date for this Policy is June 2023.

Appendix 1

REQUEST TO VIEW*

Name of person making request			
Organisation (if applicable)			
Date of request			
Date of incident		Time of incident	
Camera Number/Location			
Reason for request:			
To be completed by a staff member authorising the disclosure (the Headteacher or the Director of Finance and Operations)			
All processing of personal data must have a legal basis. Please choose what legal basis applies to this request: **Please consult the DPO if you have any queries*	Consent of the data subject		
	Performance of a contract		
	Comply with a legal obligation		
	Protect vital interests		
	Performance of a public task		
	Legitimate interests		
Request Granted:		Reason for allowing access/ disclosure	
Request Denied:		Reasons for refusing access/ disclosure	
Name and position/role			
Signed:		Date:	

Appendix 2

VIEWING CAMERA

Date:			
Viewed:	*From (time)*		*to (time)*
Camera Name/location			
Operated By:			
Viewed by (please list all):			
Description of what was observed			
Images copied and saved on the school's Safeguarding or Data drive		YES	NO
Signed:		Date:	

Please present the form to the authorised CCTV system operator and then forward it to the DPO for recordkeeping

Document History

Date	Status	Comments
June 2018	New	New Policy – To F&P Committee on 14 June 2018 – Approved. To FGB 5 July 2018
March 2020	Updated	To F & P 18.06.20. Approved. To FGB 08.07.20 for ratification. Approved
December 2020	Updated	To FGB. Approved 03.12.20
June 2022	Updated	To FGB. Approved 20.07.22
Next Review Date: June 2023		