Reviewed January 2026

Prince Henry's Grammar School

COLLABORATIVE LEARNING TRUST

POLICY
ON THE USE OF
CCTV

1. Introduction

The purpose of this Policy is to regulate the management, operation and use of closed circuit television (CCTV) at Prince Henry's Grammar School and ensure that:

- We comply with Data Protection Legislation, including the General Data Protection Regulation (GDPR).
- The images that are captured are only used for the purposes we require them for.
- We reassure those persons whose images are being captured that the images are being handled in accordance with data protection legislation.

This Policy covers the use of the CCTV system to 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. Rationale for the use of CCTV at Prince Henry's

At Prince Henry's, we take our responsibility towards the safety of students, staff and visitors very seriously. To that end, we use CCTV cameras to monitor any instances of aggression or physical damage to our school and its members. Specifically, the CCTV system has the following key objectives:

- To maintain a safe environment.
- To ensure the welfare of students, staff and visitors.
- To increase personal safety and reduce the fear of crime or undesirable behaviour.
- To protect the school buildings and assets.
- To deter criminals from targeting the school and discourage antisocial behaviour.
- To assist the Police in identifying persons who have committed an offence.
- To assist in the operational management of the school, including the management of behaviour.

3. Protocols for the use of CCTV

- In line with data protection legislation, the school is registered with the Information Commissioner's Office (ICO) for the purposes of processing personal data, including CCTV. The school's registration number is ZA550276.
- A Data Protection Impact Assessment has been completed to enable the school to identify, assess and mitigate potential risks to data privacy.
- The CCTV system at Prince Henry's is owned and operated by the school.
- The system records 24 hours a day, every day of the year.
- The system comprises a number of fixed internal and external cameras located around the school site. These produce colour images.
- The CCTV system is a closed digital system which does not record audio.
- Warning signs are placed throughout the premises where the system is active, as mandated by the ICO's Code of Practice.
- The system has been designed for maximum effectiveness and efficiency. However, the school cannot guarantee that every incident will be detected.
- Cameras will not be focused on individuals unless an immediate response to an incident is required.
- The system will not be focused on private homes, gardens or other areas of private property outside the perimeter of the school.
- The school will only use CCTV cameras for the safety and security of the school and its staff, students and visitors.
- Under no circumstances will CCTV cameras be present in school classrooms or any changing facility.

- Cameras placed in particularly sensitive areas such as student toilets are integral to the safeguarding of our students. Such cameras must be appropriately angled as to maintain the safety and security of students without the loss of dignity, respect or decency. Where fitted, cameras will be carefully angled to monitor communal areas only (e.g. doorways, wash basin areas). Under no circumstances will cameras be directed at urinals or inside cubicles.
- For security purposes, **live** CCTV images can be viewed in the School Reception, Library, school kitchens and site offices.
- Access to **recorded** images is password protected and therefore restricted to a limited number of authorised staff detailed in section 4. These staff also have access to live CCTV images in designated Key Stage offices.
- An electronic CCTV Access Log form (accessible via the link on SharePoint) will be completed whenever recorded images of students / staff / visitors are viewed. These will be retained by the Executive Officer: Site, Health & Safety.

4. Security and access

The main control facility is kept secure and locked when not in use. Visual display monitors are located in the School Reception, Library, Henry's Diner and site offices. Access to recorded images is limited to authorised members of staff and is password protected. These are:

- The school's Executive Officer: Site, Health & Safety.
- Members of the school's Safeguarding Team
  - The Designated Safeguarding Lead
  - Year Managers
  - Key Stage Directors
- Designated members of the Senior Leadership Team

In exceptional circumstances, this can be extended to other relevant members of staff to identify individuals, but this must be with the permission of a designated member of the Safeguarding Team or Senior Leadership Team.

The Executive Officer: Site, Health & Safety is responsible for checking the efficiency and security of the system and, in particular, that the equipment is properly recording and that cameras are working. Where there is a problem with any of the CCTV cameras or recording equipment that cannot be resolved by the Executive Officer: Site, Health & Safety, the CCTV contractor will be contacted.

5. Retention and erasure

The archive period of recordings is no longer than is necessary to achieve the objectives of the system. The digital recorders are set up in such a way as to overwrite old footage after 30 days (unless capacity constraints mean that the footage has already been deleted).

Recordings will only be retained for longer than this period where required in relation to a specific incident, including in the circumstances set out in section 6.

6. Sharing of CCTV images

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:

- The Police – where the images recorded would assist in a specific criminal inquiry
- Prosecution agencies – such as the Crown Prosecution Service (CPS)
- Relevant legal representatives – such as 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

Materials or knowledge secured as a result of CCTV will not be used for any commercial purpose. Images will only be released to the media for use in the investigation of a specific crime and with the written authority of the Police. Images will never be released to the media for purposes of entertainment.

7. Subject Access

Data Protection Legislation provides Data Subjects (individuals to whom "personal data" relate) with a right to data held about themselves, including those obtained by CCTV. Individuals have the right to submit a data subject access request (SAR) to gain access to their personal data in order to verify the lawfulness of the processing.

For details of how we will respond to a Subject Access Request, see section 9.3 of the Trust's Data Protection Policy (available via a link on the 'School Policies' page of the school website).

Requests by persons outside the school for viewing or obtaining digital recordings will be assessed by the Headteacher (or a delegated member of the Senior Leadership Team), who will consult the Data Protection Officer (DPO) on a case-by-case basis with close regard to data protection and freedom of information legislation.

The Headteacher (or a delegated member of the Senior Leadership Team) will make the final decision as to whether recorded images may be released to persons other than the Police.

8. Legal framework

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

- The Regulation of Investigatory Powers Act 2000
- The Protection of Freedoms Act 2012
- The Data Protection Act 2018 (DPA2018)
- The United Kingdom General Data Protection Regulation (UK GDPR)
- The Privacy and Electronic Communications (EC Directive) Regulations 2003
- 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

This policy has been created with regard to the following statutory and non-statutory guidance:

- Home Office (2021) 'The Surveillance Camera Code of Practice'
- 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'

9. Data protection principles

Data collected from 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.
- 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 they 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.

10. Privacy by design

Any future planned extension of the current CCTV system will be critically analysed using a Data Protection Impact Assessment (DPIA), in consultation with the DPO.

If the DPIA reveals any potential security risks or other data protection issues, the school will ensure that provisions are in place to overcome these issues. Where the school identifies a high risk to an individual's interests, and it cannot be overcome, the school will consult the ICO for advice.

The school will ensure that the installation and operation of CCTV systems will justify its means. If the use of the CCTV system is too privacy intrusive, the school will seek alternative provision.

11. Monitoring and review

This policy will be monitored on an ongoing basis and reviewed every two years, or sooner, where appropriate. The Executive Officer: Site, Health & Safety will be responsible for monitoring any changes to legislation that may affect this policy, and make the appropriate changes accordingly.