

Review: October 2021

Next Review: October 2022

Responsibility: Network Manager/Compliance Officer



DAME ALLAN'S SCHOOLS CCTV POLICY

The purpose of this policy is to regulate the management and operation of the Closed Circuit Television (CCTV) System (the system) at Dame Allan's Schools (the Schools).

The Schools believe that CCTV has a legitimate role to play in helping to maintain a safe and secure environment for all pupils, parents, staff, governors and volunteers (members of the Schools' community) and our visitors. However, the Schools recognise that the use of CCTV may raise concerns about the effect on individuals and their privacy. This policy is intended to address these concerns.

Images recorded by the system, by means of its fixed and domed cameras, are personal data, which must be processed in accordance with the General Data Protection Regulation 2018 (GDPR). This policy also serves as a notice and a guide to data subjects (including pupils, parents, staff, governors, volunteers, visitors to the Schools and members of the public) regarding their rights in relation to personal data recorded via the system.

The System is administered and managed by the Schools, which act as the Data Controller (as defined by the GDPR).

This policy will be reviewed regularly, and should be read with reference to the Schools'

- Data Protection Policy;
- Privacy Notices for Parents, Pupils, Staff, Governors and Suppliers;
- Taking, Storing and Using Images of Children Policy.

The Schools also have regard to the guidance contained in the Information Commissioner's Office document "In the picture: A data protection code of practice for surveillance cameras

and personal information” (available at <https://ico.org.uk/media/for-organisations/documents/1542/cctv-code-of-practice.pdf>).

All fixed cameras are in plain sight on the Schools’ premises and the Schools do not routinely use CCTV for covert monitoring or monitoring of private property outside of the Schools’ grounds.

CCTV cameras are currently found in the following locations:

- Senior Schools’ vehicular and pedestrian gates;
- Florence Moat Library and Jennifer Cole Room at the Senior Schools;
- Queen’s Building – at the main entrance, in the ground floor study area, in the first floor study area and in the corridor leading from the Queen’s Building into the RE corridor;
- Junior School Building – north, south and west sides of the building covering doors;
- Junior School vehicular and pedestrian gates;
- Junior School Kitchen.

The Schools’ purposes for using the CCTV system are set out below and, having fully considered the privacy rights of individuals, the Schools believe these purposes are all in their legitimate interests. Data captured for the purposes below will not be used for any commercial purpose.

1. Objectives of the System

- 1.1 To protect the personal safety of all members of the Schools’ community, visitors and members of the public.
- 1.2 To protect the Schools’ buildings and equipment, and the personal property of all members of the Schools’ community, visitors and members of the public, from damage, disruption, vandalism and other crime.
- 1.3 To act as a deterrent against crime.
- 1.4 To support the police and community in preventing and detecting crime, and assist in the identification, apprehension and prosecution of offenders.
- 1.5 To monitor the security and integrity of the Schools’ sites, deliveries, arrivals and departures.
- 1.6 To monitor staff and contractors when carrying out work duties, in order to ensure the health and safety of all.

- 1.7 To monitor and uphold discipline among pupils in line with the Schools' Rules and the Whole School Behaviour Policy.

2. Positioning

- 2.1 Locations have been selected, both inside and out, that the Schools reasonably believe require monitoring to address the objectives stated above.
- 2.2 Adequate signage has been placed in prominent positions to inform members of the Schools' community, visitors and members of the public that they are entering a monitored area. These signs contain details, identifying the Schools as the organisation operating the system and giving contact details for further information regarding the system.
- 2.3 No images will be captured from areas in which individuals would have a heightened expectation of privacy, including changing and washroom facilities.
- 2.4 No images of public spaces will be captured except to a limited extent at site entrances.
- 2.5 Prior to placing a new CCTV camera in any location, the Schools will carefully consider if that is appropriate by carrying out a privacy impact assessment (PIA). This is intended to assist the Schools in deciding whether new surveillance cameras are necessary and proportionate in the circumstances and whether they should be used at all or whether any limitations should be placed on their use. Any PIA will consider the nature of the problem which the Schools are seeking to address at that time and whether a CCTV camera is likely to be an effective solution, or whether a better solution exists. In particular, the Schools will consider the effect a CCTV camera will have on individuals and therefore whether its use is a proportionate response to the problem identified.

3. Maintenance

- 3.1 The system will be operational 24 hours a day, every day of the year.
- 3.2 The System Manager (defined below) will check and confirm that the system is properly recording and that cameras are functioning correctly, on a regular basis.
- 3.3 The system will be checked and (to the extent necessary) serviced no less than annually.

4. Responsibility for and supervision of the system

- 4.1 The Schools' Bursar has overall responsibility for ensuring compliance with relevant legislation and the effective operation of the system and this policy. Day-to-day responsibility for deciding what information is recorded, how it is used and to whom it may be disclosed has been delegated to the Compliance Officer. Day-to-day operational responsibility for CCTV cameras and the storage of data recorded is the responsibility of the Network Manager.
- 4.2 Staff authorised by the School to conduct routine supervision of the system may include Caretakers, SMT, IT Support and Office Staff (Gates only).
- 4.3 Images will be viewed and/or monitored in a suitably secure and private area to minimise the likelihood of or opportunity for access to unauthorised persons.

5. Storage of Data

- 5.1 The day-to-day management of images will be the responsibility of the Network Manager, who will act as the System Manager, or such suitable person as the System Manager shall appoint in his or her absence.
- 5.2 In order to ensure that the rights of individuals recorded by the system are protected, the Schools will ensure that the data gathered is stored in such a way that maintains its integrity and security. This may include encrypting the data, where it is possible to do so.
- 5.3 Images will be stored for up to a period of 4 weeks, and will then be automatically overwritten unless the Schools consider it reasonably necessary for the pursuit of the objectives outlined above, or if lawfully required by an appropriate third party, such as the police or local authority.
- 5.4 Where such data is retained, it will be retained in accordance with data protection laws. Information including the date, time and length of the recording, as well as the locations covered and groups or individuals recorded, will be recorded in the system electronic log book.

6. Access to Images

- 6.1 Access to stored CCTV images will only be given to authorised persons, under the supervision of the System Manager, in pursuance of the above objectives (or if there is some other overriding and lawful reason to grant such access).
- 6.2 Individuals also have the right to access personal data the Schools hold on them. Further details can be found in the Schools' Privacy Notices and Data Protection Policy, including information held on the system, if it has been kept. If an individual

wishes to access this data, the Schools will require specific details including, at least, the time, date and camera location before it can properly respond to any such requests. This right is subject to certain exemptions from access, including in some circumstances where others are identifiable.

- 6.3 The System Manager must satisfy themselves of the identity of any person wishing to view stored images or access the system and the legitimacy of the request. The following are examples when the System Manager may authorise access to CCTV images:
- 6.3.1 Where required to do so by the Principal, the Police or some relevant statutory authority;
 - 6.3.2 To make a report regarding suspected criminal behaviour;
 - 6.3.3 To enable one of the Schools' Designated Safeguarding Leads to examine behaviour which may give rise to any reasonable safeguarding concern;
 - 6.3.4 To assist the Schools in establishing facts in cases of unacceptable pupil behaviour, in which case, the parents/guardian will be informed as part of the Schools' management of a particular incident;
 - 6.3.5 To data subjects (or their legal representatives) pursuant to an access request under the GDPR and on the basis set out in 6.2 above;
 - 6.3.6 To the School's insurance company where required in order to pursue a claim for damage done to insured property; or
 - 6.3.7 In any other circumstances required under law or regulation.
- 6.4 Where images are disclosed under 6.3 above a record will be made in the system electronic log book including the person viewing the images, the time of access, the reason for viewing the images, the details of images viewed and a crime incident number (if applicable).
- 6.5 Where images are provided to third parties under 6.3 above, wherever practicable, steps will be taken to obscure images of non-relevant individuals.

7. Other CCTV systems

- 7.1 The Schools never engage in covert monitoring or surveillance (where individuals are unaware that the monitoring or surveillance is taking place), unless, in highly exceptional circumstances, there are reasonable grounds to suspect that criminal activity or extremely serious malpractice is taking place and, after suitable consideration, the Schools reasonably believe that there is no less intrusive way to tackle the issue. In the unlikely event that covert monitoring is considered to be

justified, it will only be carried with the express written authorisation of the Principal, with reasons for the decision being fully documented.

- 7.2 The Schools do not own or manage third party CCTV systems, but may be provided by third parties with images of incidents where this is in line with the objectives of the Schools' own CCTV policy and/or the Schools' Rules.
- 7.3 Many pupils travel on coaches provided by third party contractors and a number of these coaches are equipped with CCTV systems. The Schools may use these in establishing facts in cases of unacceptable pupil behaviour, in which case the parents/guardian will be informed as part of the Schools' management of a particular incident.

8. Complaints and queries

- 8.1 Any complaints or queries in relation to the School's CCTV system, or its use of CCTV, or requests for copies of this policy, should be referred, in the first instance, to the Schools' Compliance Officer.
- 8.2 For any other queries concerning the use of your personal data by the School, please see the details provided in the Schools' applicable Privacy Notice.

9. Breaches of this policy

Any breach of this policy may, in appropriate circumstances, be treated as a disciplinary matter, and may be dealt with using the Schools' disciplinary procedures for pupils (in accordance with the Whole School Behaviour Policy) and staff (in accordance with the Staff Code of Conduct).