THE MOUNTBATTEN SCHOOL

Audit, Finance and Risk Committee

CCTV Policy

January 2026

Review Date: January 2027

Company No. 07560175

Whitenap Lane Romsey Hampshire SO51 5SY
t: 01794 502 502 e: info@mountbatten.school
w: www.mountbatten.school Company No. 07560175

Founder Patron: 1st Earl Mountbatten of Burma CEO: Heather McIlroy Headteacher: Chris Cox Patron: The Lady Alexandra Knatchbull

Data Protection

Any personal data processed in the delivery of this policy will be processed in accordance with the school Data Protection policy.

1. Policy Statement

a. The Mountbatten School uses Close Circuit Television ("CCTV") within the premises of the school. The purpose of this policy is to set out the position of the school as to the management, operation and use of the CCTV at the School.

b. This policy applies to all members of our workforce, students and visitors to the school premises and all other persons whose images may be captured by the CCTV system.

c. This policy takes account of all applicable legislation and guidance, including:

- General Data Protection Regulation ("GDPR");
- CCTV Code of Practice produced by the Information Commissioner;
- Human Rights Act 1998.

d. The lawful basis for processing CCTV images is Article 6(1)(e) – task carried out in the public interest, and/or Article 6(1)(f) – legitimate interests.

e. This policy sets out the position of the school in relation to its use of CCTV and should be read in conjunction with the School Data Protection Policy.

f. The system comprises a number of internal and external day and night cameras and does not use any sound recording capability, apart from in exceptional circumstances. The CCTV system is owned and operated by the school and the deployment of it, is determined by the Senior Leadership Team. The Data Protection Officer ("DPO") or their representative has overall responsibility as delegated by the Data Controller (Board of Trustees).

g. Access and viewing are restricted to authorised operators only who will be aware of the procedures they are required to follow and their responsibilities under this policy. All employees will be aware of the restrictions in relation to access to, and disclosure of, recorded images. The further introduction of, or changes to, CCTV monitoring will be subject to consultation with staff where appropriate.

2. Purpose of CCTV

The school uses CCTV for the following purposes:

- To provide a safe and secure environment for pupils, staff and visitors;
- To protect the school buildings and assets;

- To assist in reducing the fear of crime and for the protection of private property;
- To assist in the prevention of crime and assist law enforcement agencies in apprehending offenders.

3. Policy Intent

The school will:

a. notify the Information Commissioners Office of its use of CCTV as part of the annual data protection registration;
b. complete a CCTV Data Privacy Impact Assessment ("DPIA") for the use of surveillance CCTV and will update this as appropriate when the system is upgraded or significantly modified;
c. treat the system and all information processed on the CCTV system as data which is covered by the Data Protection Act/GDPR;
d. use cameras to monitor activities within the school grounds to identify potential criminal activity for the purpose of securing the safety and well-being of the school, as well as for monitoring student behaviour;
e. not direct cameras outside of the school site at private property, an individual, their property or a specific group of individuals. The exception to this would be where an authorisation was obtained for Directed Surveillance to take place, as set out in the Regulation of Investigatory Power Act 2000;
f. display CCTV warning signs will be clearly and prominently placed at external entrances of the school site where CCTV is operational, including the school gates as coverage includes outdoor areas. The school will ensure that there are prominent signs placed at both the entrance of the CCTV zone and within the controlled area which will contain details of the purpose for using CCTV.
g. not guarantee that a system will or can cover or detect every single incident taking place in the areas of coverage;
h. not use materials or knowledge for any commercial purpose. Recorded materials will only be released for use in the investigation of a specific crime and with the written authority of the Police and in accordance with the Data Protection Act/GDPR.

4. Children and Safeguarding

The School recognises that the majority of individuals whose images are captured by the CCTV system are children. As such, the School acknowledges that CCTV footage constitutes personal data relating to minors and is afforded a higher level of protection under data protection law.

CCTV is used as a safeguarding support measure and may be relied upon as part of safeguarding, child protection, behaviour or serious incident investigations where it is necessary and proportionate to do so. CCTV does not replace appropriate supervision, professional judgement or established safeguarding procedures.

All CCTV footage relating to safeguarding concerns will be handled with heightened sensitivity and in accordance with the School's Safeguarding and Child Protection Policy and Keeping Children Safe in Education (KCSIE).

5. Privacy Information and Communication

The School provides clear and accessible information about its use of CCTV through:

• Prominent signage at points of entry and within CCTV-monitored areas; and
• A CCTV Privacy Notice, which is available on the School website and upon request from Reception.

Parents and carers are informed of the School's use of CCTV through published policies and privacy information. The School will ensure that information relating to CCTV use is transparent, accessible and reviewed regularly.

6. Siting Cameras

1. Cameras will be sited so they only capture images relevant to the purposes for which they are installed (described above) and care will be taken to ensure that reasonable privacy expectations are not violated. The school will ensure that the location of equipment is carefully considered to ensure that images captured comply with the Data Protection Act/GDPR requirements

2. CCTV is generally not sited in classrooms unless there is a specific need. For example, in an IT Suite to prevent vandalism of equipment.

3. Members of staff, on request can access details of CCTV camera locations.

7. Covert Monitoring

1. Covert monitoring will only be used in **exceptional circumstances** and where it is strictly necessary and proportionate, such as where there is a reasonable suspicion of serious misconduct or criminal activity and where informing individuals would prejudice the investigation.

2. The school does not conduct covert surveillance under statutory surveillance powers. Any covert monitoring undertaken is internal, limited in scope, time-bound and subject to strict safeguards.

3. Prior to any covert monitoring taking place:
    - Written authorisation must be obtained from the Headteacher;
    - The Data Protection Officer must be consulted; and
    - A specific Data Protection Impact Assessment (DPIA) must be completed.

4. Covert monitoring:
    - Will not be used in areas where individuals have a reasonable expectation of privacy, including toilets and changing areas;
    - Will not be used to assess staff performance or contribute to capability procedures;
    - Will cease immediately once the purpose of the monitoring has been achieved.

5. A written record will be retained detailing the justification, duration, authorisation and outcome of any covert monitoring.

8. Storage and Retention of CCTV Images

1. Recorded data will not be retained for longer than is necessary. While retained, the integrity of the recordings will be maintained to ensure their evidential value and to protect the rights of the people whose images have been recorded.

2. All retained data will be stored securely.

3. Recordings are kept for 31 days. Specific recordings which the school wishes to retain after this time will be logged.

4. CCTV footage is automatically deleted or overwritten after the standard retention period unless it has been identified for preservation due to a safeguarding concern, investigation, legal matter or other legitimate purpose.

5. Where footage is retained beyond the standard retention period, the reason for retention and the revised retention period will be documented and reviewed regularly.

6. Secure deletion of CCTV footage is managed by authorised IT staff only and ensures that data is permanently removed or rendered inaccessible.

7. An electronic file is held on a secure central server where specific CCTV image/recordings are retained. Access by staff to specific recordings are outlined below in section 11.

8. The Data Protection Act/GDPR does not prescribe any specific minimum or maximum retention periods that apply to all systems or footage. Rather, retention should reflect the organisation's purposes for recording information, which should be informed by the purpose for which the information is collected, and how long it is needed to achieve this purpose. Storage availability is also a factor to be considered in the ability to retain recordings.

9. Disclosure of Images to Data Subjects (Subject Access Requests)

1. Any Individual recorded in any CCTV image is a data subject for the purposes of the Data Protection Legislation, and has the right to request access to those images.

2. Any individual who requests access to images of themselves will be considered to have made a subject access request pursuant to the Data Protection Legislation. Such a request should be considered in the context of the School's Subject Access Request Policy.

3. Subject Access Requests relating to CCTV footage will be responded to within one calendar month of receipt, in accordance with data protection legislation. Where requests are complex or numerous, this period may be extended by up to a further two months, and the requester will be informed accordingly.

4. When considering requests involving third-party images, the School will undertake a balancing exercise between the rights of the requester and the rights and freedoms of others. Decisions will not be based solely on technical capability or available resources.

5. All requests should be made in writing to the Headteacher or Data Protection Officer. Individuals submitting requests for access will be asked to provide sufficient information to enable the footage relating to them to be identified. For example, date, time and location.

6. When such a request is made a member of the IT Services Team (as the CCTV system administrator) will review the CCTV footage, in accordance with the request.

7. If the footage contains only the individual making the request, then the individual may be permitted to view the footage. This must be strictly limited to that footage which contains only images of the individual making the request. The IT Services Team as the CCTV system administrators must take appropriate measures to ensure that the footage is restricted in this way.

8. If the footage contains images of other individuals, then the school must consider whether:
    - The request requires the disclosure of the images of individuals other than the requester, for example whether the images can be distorted so as

not to identify other individuals (the school does not have the resources or software to redact images);

- The other individuals in the footage have consented to the disclosure of the images, or their consent could be obtained; or
- If not, then whether it is otherwise reasonable in the circumstances to disclose those images to the individual making the request.

9. The school reserves the right to refuse access to CCTV footage where this would prejudice the legal rights of other individuals or jeopardise an ongoing investigation.

10. A record must be kept and held securely, of all disclosures which sets out:
    - When the request was made;
    - The process followed by the IT Services Team (as the CCTV system administrators) in determining whether the images contained third parties;
    - The considerations as to whether to allow access to those images;
    - The individuals that were permitted to view the images and when; and
    - Whether a copy of the images was provided, and if so to whom, when and in what format.

10. Disclosure of Images to Third Parties

1. The school will only disclose recorded CCTV images to third parties where it is permitted to do so in accordance with the Data Protection Legislation.

2. Third parties acting behalf of a duty subject will be handled in accordance with the School's Subject Access Request Policy.

3. CCTV images will only be disclosed to law enforcement agencies in line with the purposes for which the CCTV system is in place.

4. If a request is received form a law enforcement agency for disclosure of CCTV images, then the school must follow the same process as above in relation to subject access requests. Detail should be obtained from the law enforcement agency as to exactly what they want the CCTV images for, and any particular individuals of concern. This will then enable proper consideration to be given to what should be disclosed, and the potential disclosure of any third-party images.

5. The information above must be recorded in relation to any disclosure.

6. If an order is granted by a Court for disclosure of CCTV images, then this should be complied with. However very careful consideration must be given to exactly what the Court order requires. If there are any concerns as to disclosure, then the Data Protection Officer should be contacted in the first instance and appropriate legal advice may be required.

11. Access to CCTV Images

1. The ability to view live and historical CCTV data available via network software is only to be provided to authorised persons only. Direct access to recorded data is limited to the IT Services Team (as administrators), Site Manager, Pastoral and Head of Years.

2. Data from CCTV may be used within the school's' discipline and grievance procedures as required and will be subject to the usual confidentiality requirements of those procedures.

3. Access to live CCTV feeds and recorded footage is strictly restricted to authorised personnel and is granted on a role-based, need-to-know basis only.

   • Live viewing may only be undertaken for operational, safeguarding or security purposes.
   • Playback of recorded footage may only take place where there is a clear and documented purpose, such as safeguarding, behaviour management, serious incidents or criminal investigations.

   Requests to review recorded footage must be authorised by a member of the Senior Leadership Team or the Data Protection Officer.

   A secure audit log will be maintained which records:
   • The name and role of the individual accessing the footage
   • The date and time of access
   • The reason for access
   • The outcome of the review

   Unauthorised access to CCTV systems or footage may result in disciplinary action.

4. All staff authorised to access CCTV systems or footage will receive appropriate data protection and safeguarding training.

   The governing body will receive periodic assurance regarding:
   • Compliance with this policy
   • Any complaints or incidents relating to CCTV
   • Outcomes of policy reviews or DPIAs

12. **Complaints**

Complaints and enquiries about the operation of CCTV within the school should be directed to the Headteacher or Data Protection Officer in the first instance.

13. Further Information

For further information on CCTV and its use please see below:

- Data Protection Act 2018
- General Data Protection Regulation (GDPR)

- Surveillance Camera Code of Practice ICO Website (currently under consultation)

Policy approved by the Audit, Finance and Risk Committee on 19 January 2026.

Signed Date:
Chair of Audit, Finance and Risk