



Salterns Academy Trust

CCTV Policy

Admiral Lord Nelson School

Approved by:	LGB	Date: April 26
---------------------	-----	-----------------------

Next review due by:	April 2027
----------------------------	------------

1. Aims

This policy aims to set out the school's approach to the operation, management and usage of surveillance and closed-circuit television (CCTV) systems on school property.

1.1 Statement of intent

The purpose of the CCTV system is to:

- Make members of the school community feel safe
- Protect members of the school community from harm to themselves or to their property
- Deter criminality in the school
- Protect school assets and buildings
- Assist police to deter and detect crime
- Determine the cause of accidents / incidents
- Assist in the effective resolution of any disputes which may arise in the course of disciplinary and grievance proceedings
- To assist in the defense of any litigation proceedings

The CCTV system will not be used to:

- Encroach on an individual's right to privacy
- Follow particular individuals, unless there is an ongoing emergency incident occurring

The list of uses of CCTV is not exhaustive and other purposes may be or become relevant.

The CCTV system is registered with the Information Commissioner under the terms of the Data Protection Act 2018. The system complies with the requirements of the Data Protection Act 2018 and UK GDPR.

Lawful basis for processing CCTV data

The lawful basis for processing personal data through the school's CCTV system is Article 6(1)(e) of the UK General Data Protection Regulation (UK GDPR) – processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the school and/or Trust. The use of CCTV is necessary and proportionate to support the school's statutory and public functions, including but not limited to:

- Safeguarding pupils, staff and visitors
- Promoting health and safety across the school site
- Preventing, detecting and investigating crime and anti-social behaviour
- Protecting school buildings, grounds and assets

The school does not rely on consent as the lawful basis for CCTV processing, as CCTV forms part of the school's core safeguarding and security arrangements and individuals are not able to opt out of this processing.

Where CCTV footage is disclosed to third parties such as the police or other public authorities for the purposes of crime prevention, investigation or safeguarding, such disclosures are carried out in accordance with data protection legislation and are supported by the same public task basis, or another appropriate lawful basis where applicable.

Footage or any information gleaned through the CCTV system will never be used for commercial purposes.

In the unlikely event that the police request that CCTV footage be released to the media, the request will only be complied with when written authority has been provided by the police, and only to assist in the investigation of a specific crime.

The footage generated by the system should be of good enough quality to be of use to the police or the court in identifying suspects.

2. Relevant legislation and guidance

This policy is based on:

2.1 Legislation

- [UK General Data Protection Regulation](#)
- [Data Protection Act 2018](#)
- [Human Rights Act 1998](#)
- [European Convention on Human Rights](#)
- [The Regulation of Investigatory Powers Act 2000](#)
- [The Protection of Freedoms Act 2012](#)
- [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](#)

2.2 Guidance

- [Surveillance Camera Code of Practice \(2021\)](#)

3. Definitions

Surveillance: the act of watching a person or a place

CCTV: closed circuit television; video cameras used for surveillance

Covert surveillance: operation of cameras in a place where people have not been made aware they are under surveillance

4. Covert surveillance

Covert surveillance will only be used in extreme circumstances, such as where there is suspicion of a criminal offence. If the situation arises where covert surveillance is needed (such as following police advice for the prevention or detection of crime or where there is a risk to public safety), a data protection impact assessment will be completed in order to comply with data protection law. Covert surveillance would only be undertaken where legally authorised and supported by external advice (e.g. police / legal)

5. Location of the cameras

Cameras are located in places that require monitoring in order to achieve the aims of the CCTV system (stated in section 1.1).

Cameras are located in:

Listed in Appendix 1

Wherever cameras are installed appropriate signage is in place to warn members of the school community that they are being recorded.

Cameras are not and will not be aimed off school grounds into public spaces or people's private property.

Cameras are positioned in order to maximise coverage, but there is no guarantee that all incidents will be captured on camera.

6. Roles and responsibilities

Data controller and accountability

For the purposes of the UK General Data Protection Regulation (UK GDPR) and the Data Protection Act 2018, Salterns Academy Trust is the data controller in respect of personal data processed through the CCTV system operating at Admiral Lord Nelson School.

As an Academy Trust, Salterns Academy Trust determines the purposes and means of processing personal data and retains overall accountability for ensuring that CCTV processing is lawful, fair, transparent and compliant with data protection legislation and relevant statutory guidance.

The Local Governing Body has responsibility for providing local oversight and assurance that the CCTV system is operated in accordance with this policy, the Trust's governance framework, and the Trust's scheme of delegation.

The Headteacher, acting under delegated authority from the Trust, is responsible for the day-to-day operation of the CCTV system at school level. This includes ensuring that the system is used only for authorised purposes and that access to CCTV footage is appropriately controlled in accordance with this policy and Trust instructions.

Operational responsibilities delegated to the Headteacher include:

- Ensuring that access to CCTV footage is restricted to authorised personnel
- Ensuring that CCTV footage is accessed, used and disclosed only where necessary and proportionate
- Ensuring that requests for access to CCTV footage, including subject access requests and third-party requests, are managed in accordance with Trust procedures

Strategic oversight, specialist advice and compliance assurance remain the responsibility of the Trust Data Protection Officer, who acts independently and:

- Advises the Trust and school on compliance with data protection legislation
- Oversees the handling of subject access requests and complex disclosure decisions
- Supports and reviews Data Protection Impact Assessments relating to CCTV
- Acts as the point of contact with the Information Commissioner's Office

Nothing in this delegation limits the Trust's role as data controller or its ultimate accountability for CCTV processing.

6.2 The Headteacher

The headteacher will:

- Take responsibility for all day-to-day leadership and management of the CCTV system
- Liaise with the data protection officer (DPO) to ensure that the use of the CCTV system is in accordance with the stated aims and that its use is needed and justified
- Ensure that the guidance set out in this policy is followed by all staff
- Review the CCTV policy to check that the school is compliant with legislation
- Ensure all persons with authorisation to access the CCTV system and footage have received proper training the use of the system and in data protection
- Sign off on any expansion or upgrading to the CCTV system, after having taken advice from the DPO and taken into account the result of a data protection impact assessment
- Decide, in consultation with the DPO, whether to comply with disclosure of footage requests from third parties

6.3 The Data Protection Officer

The data protection officer (DPO) will:

- Train persons with authorisation to access the CCTV system and footage in data protection
- Train all staff to recognise a subject access request
- Deal with subject access requests in line with the relevant legislation
- Monitor compliance with UK data protection law
- Advise on and assist the school with carrying out data protection impact assessments
- Act as a point of contact for communications from the Information Commissioner's Office
- Ensure data is handled in accordance with data protection legislation
- Ensure footage is obtained in a legal, fair and transparent manner
- Ensure footage is destroyed when it falls out of the retention period
- Keep accurate records of all data processing activities and make the records public on request
- Inform subjects of how footage of them will be used by the school, what their rights are, and how the school will endeavour to protect their personal information
- Ensure that the CCTV system is not infringing on any individual's reasonable right to privacy in public spaces
- Carry out termly checks, in conjunction with the trust network manager to determine whether footage is being stored accurately, and being deleted after the retention period
- Receive and consider requests for third-party access to CCTV footage

6.4 The Trust Network Manager

The trust network manager will:

- Take care of the day-to-day maintenance and operation of the CCTV system
- Monitor and Audit System access
- Check the system for faults and security flaws termly
- Ensure the data and time stamps are accurate termly
- Ensure that the CCTV systems are working properly and that the footage they produce is of high quality so that individuals pictured in the footage can be identified

6.5 The Buildings and Community Manager

- Oversee the security of the CCTV system and footage
- Train persons with authorisation to access the CCTV system and footage in the use of the system
- Ensure appropriate signage is in place to warn members of the school community that they are under surveillance.

7. Operation of the CCTV system

The CCTV system will be operational 24 hours a day, 365 days a year.

The system is registered with the Information Commissioner's Office.

The system will not record audio. Audio recording functionality is disabled to prevent accidental recording of audio.

Recordings will have date and time stamps. This will be checked by the system manager termly and when the clocks change.

8. Storage of CCTV footage

Footage will be retained for 30 days. At the end of the retention period, the files will be overwritten automatically, unless footage has been exported for evidence.

On occasion footage may be retained for longer than 30 days, for example where a law enforcement body is investigating a crime, to give them the opportunity to view the images as part of an active investigation.

Recordings will be downloaded and encrypted, so that the data will be secure and its integrity maintained, so that it can be used as evidence if required.

The DPO will carry out termly checks to determine whether footage is being stored accurately, and being deleted after the retention period.

9. Access to CCTV footage

Access will only be given to authorised persons, for the purpose of pursuing the aims stated in section 1.1, or if there is a lawful reason to access the footage.

Any individuals that access the footage must record their name, the date and time, and the reason for access in the access log.

Any visual display monitors will be positioned so only authorised personnel will be able to see the footage.

9.1 Staff access

The following members of staff have authorisation to access the CCTV footage:

- The headteacher
- The deputy head(s)
- The Trust data protection officer
- The Trust network Manager
- The Buildings and Community Manager
- Anyone with express permission of the headteacher

CCTV footage will only be accessed from authorised personnel's work devices, or from the visual display monitors.

All members of staff who have access will undergo training to ensure proper handling of the system and footage.

Any member of staff who misuses the surveillance system may be committing a criminal offence, and will face disciplinary action.

9.2 Subject access requests (SAR)

According to UK GDPR and Data Protection Act 2018, individuals have the right to request a copy of any CCTV footage of themselves.

Upon receiving the request the school will immediately issue a receipt and will then respond within within one calendar month,

. The school may request an extension to where the request is complex or numerous .

All staff have received training to recognise SARs. When a SAR is received staff should inform the DPO in writing. When making a request, individuals should provide the school with reasonable information such as the date, time and location the footage was taken to aid school staff in locating the footage.

On occasion the school will reserve the right to refuse a SAR, Refusal must be based **specific statutory exemption** and justified as necessary and proportionate. The view of the Data Protection Officer, and if necessary the Trusts Legal advisors should be sought when considering withholding information. Partial disclosure must be considered in all cases

Images that may identify other individuals need to be obscured to prevent unwarranted identification. The school will attempt to conceal their identities by blurring out their faces, or redacting parts of the footage. If this is not possible school are unlikely to grant permission to view CCTV but will offer still images or a written description of the footage

The school reserves the right to charge a reasonable fee to cover the administrative costs of complying with an SAR that is manifestly unfounded or excessive

Footage that is disclosed in a SAR will be disclosed securely to ensure only the intended recipient has access to it.

Records will be kept that show the date of the disclosure, details of who was provided with the information (the name of the person and the organisation they represent), and why they required it.

Individuals wishing to make an SAR can find more information about their rights, the process of making a request, and what to do if they are dissatisfied with the response to the request on the [ICO website](#).

9.3 Third-party access

CCTV footage will only be shared with a third party to further the aims of the CCTV system set out in section 1.1 (e.g. assisting the police in investigating a crime).

Footage will only ever be shared with authorised personnel such as law enforcement agencies or other service providers who reasonably need access to the footage (e.g. investigators).

All requests for access should be set out in writing and sent to the headteacher and the DPO.

The school will comply with any court orders that grant access to the CCTV footage. The school will provide the courts with the footage they need without giving them unrestricted access. The DPO will consider very carefully how much footage to disclose, and seek legal advice if necessary.

The DPO will ensure that any disclosures that are made are done in compliance with UK GDPR.

All disclosures will be recorded by the DPO.

The school follows the principle of privacy by design. Privacy is taken into account during every stage of the deployment of the CCTV system, including its replacement, development and upgrading.

The system is used only for the purpose of fulfilling its aims (stated in section 1.1).

When the CCTV system is replaced, developed or upgraded a DPIA will be carried out to be sure the aim of the system is still justifiable, necessary and proportionate.

The DPO will provide guidance on how to carry out the DPIA.

Those whose privacy is most likely to be affected, including the school community and neighbouring residents, will be consulted during the DPIA, and any appropriate safeguards will be put in place.

A new DPIA will be done at the point of installation and/or whenever cameras are moved, and/or new cameras are installed.

If any security risks are identified in the course of the DPIA, the school will address them as soon as possible.

11. Security

- The system manager will be responsible for overseeing the security of the CCTV system and footage
- The system will be checked for faults once a term
- Any faults in the system will be reported as soon as they are detected and repaired as soon as possible, according to the proper procedure
- Footage will be stored securely and encrypted wherever possible
- The CCTV footage will be password protected and any camera operation equipment will be securely locked away when not in use
- Proper cyber security measures will be put in place to protect the footage from cyber attacks
- Any software updates (particularly security updates) published by the equipment's manufacturer that need to be applied, will be applied as soon as possible

12. Complaints

Complaints should be directed to the Headteacher and should be made according to the school's complaints policy.

13. Monitoring

The policy will be reviewed annually by the DPO to consider whether the continued use of a surveillance camera remains necessary, proportionate and effective in meeting its stated purposes.

14. Links to other policies

- Data protection policy
- Privacy notices for parents, pupils, staff, governors and suppliers
- Safeguarding policy

1

1

1



3

10

1

L

CAM	LOCATION	FLOOR	INTERNAL /	DIRECTION	VIEWING
1	Maths 2 / Double	Second	Internal	North	Pointing alongside
2	Maths corridor	Second	Internal	South	pointing towards
3	Maths Lobby	Second	Internal	East	Facing cupboard and
4	North stairs	Second	External	East	Pointing down
5	Lift	Second	Internal	East	Facing lift and external
6	Outside finance	Second	Internal	South	Pointing along
7	Middle stairs	Second	External	East	Pointing down
8	English Lobby	Second	Internal	East	Facing external door
9	South stairs	Second	External	East	Pointing down
10	English office	Second	Internal	North	Fixed to end wall
11	Outside Media	First	Internal	South	Facing towards top of
12	Outside Sci 1	First	Internal	South	Facing along sci
13	Science Lobby	First	Internal	East	Facing towards
14	Science corridor	First	Internal	South	Facing along sci
15	Outside Sci 5	First	Internal	West	Facing top off stairs
16	Inside Admin	First	Internal	West	Facing towards
17	Middle Lobby	First	Internal	North	Pointing back
18	Middle Lobby	First	Internal	East	Facing Lift and
19	Middle Lobby	First	Internal	South	Pointing along Langs
20	Langs / Design	First	Internal	East	Pointing towards
21	Design 1	First	Internal	North	Pointing along
22	North Bike Shed	Ground	External	North	Pointing into bike
23	North Car park	Ground	External	North	Pointing towards
24	Design Lobby	Ground	Internal	North	Facing Music /
25	Design Music	Ground	Internal	West	Facing the stairs and
26	Katrinass Garden	Ground	External	West	Pointing towards
27	Outside Science	Ground	Internal	North	Pointing along
28	KS3 Lobby	Ground	Internal	South	Pointing towards
29	KS3 Lobby	Ground	Internal	East	Facing External Lobby
30	KS3 Lobby	Ground	Internal	North	Facing towards
31	Outside Design 3	Ground	Internal	West	Pointing towards
32	Admin	Ground	Internal	West	Staff area - towards
33	Comms room	Ground	Internal	West	Servers and cupboard
34	Behind reception	Ground	Internal	East	Reception / Mall
35	Outside English 5	Ground	Internal	West	Towards main
36	Outside Lift	Ground	Internal	East	Facing Middle
37	Mall	Ground	Internal	South	Pointing towards hall
38	Main hall	Ground	Internal		Main Hall
39	Outside Gym	Ground	Internal	North	Pointing towards Mall
40	Bottom of South	Ground	Internal	North	Pointing up stairs /
41	Hamiltons	Ground	Internal	East	Pointing towards
42	Outside PE	Ground	Internal	South	Facing changing
43	Sports hall	Ground	Internal		Sports Hall
44	Deck Boiler	Ground	External	East	Facing field
45	Deck Bar	Ground	Internal		Deck Bar
46	Deck Reception	Ground	Internal		Deck Reception
47	Deck Reception	Ground	External	West	Facing outwards onto
48	Back of Fitness	Ground	External	South	Facing ATP
49	Back of Fitness	Ground	External	North	Facing Canteen
50	On pole by bike	Ground	External		Facing Pitch towards
51	Back of	Ground	External	South	Facing ATP
52	Back of	Ground	External	North	Facing Canteen
53	Back of School -	Ground	External	South	Facing Canteen
54	Back of School -	Ground	External	North	Facing North
55	Back of School -	Ground	External	South	Facing South
56	Back of School -	Ground	External	North	Facing North
57	Outside	Ground	External	West	Facing front car park
58	Outside Katrinass	Ground	External	West	Facing front car park
59	New Build	Ground	External	North	Facing front car park
60	Reception	Ground	Internal		Reception
61	Corridor by	Ground	Internal		Corridor
62	Corridor by WC's	Ground	Internal		Corridor by
63	WC Area	Ground	Internal		WC Area
64	Exit Corridor adj	Ground	Internal		Exit Corridor
65	Corridor adj	Ground	Internal		Corridor
66	Corridor adj	Ground	Internal		Corridor
67	Exit corridor adj	Ground	Internal		Exit corridor
68	End of Hums	Ground	Internal		Corrdior
69	Exit Corridor adj	Ground	Internal		Exit Corridor
70	Conference	Ground	Internal		Conference Room
71	Meeting Room	Ground	Internal		Meeting Room
72	Outside Meeting	Ground	External		External Area
73	Outside	Ground	External		Outside Reception
74	Outside Hums 1	Ground	External		External Area
75	Outside exit adj	Ground	External		External Area
76	Outside Hums 4	Ground	External		External Area
77	Outside Hums 6	Ground	External		External Area
78	Outside on pole	Ground	External		External Area
79	Outside Hums 10	Ground	External		External Area
80	Outside Hums 10	Ground	External		External Area
81	Outside End of	Ground	External		External Area
82	Staff Bike Shed	Ground	External		Staff Bike Shed
83	On Pole by	Ground	External		South Entrance Gates
84	Broadside GF	Ground	External		Broadside GF
85	On Pole by bike	Ground	External		Facing Big 3G Pitch
86	On Pole by Bike	Ground	External		Facing into South
N/A	Server Room	Ground	Internal	n/a	n/a
N/A	Server Room	Ground	Internal	n/a	n/a
N/A	Server Room	Ground	Internal	n/a	n/a