

# NEWLANDS GIRLS' SCHOOL

## POLICY DOCUMENT



# CCTV Policy

|  |                                     |               |
|--|-------------------------------------|---------------|
| <b>LAST UPDATED AND REVIEWED</b>                           | (by) School Business Manager        | December 2025 |
| <b>POLICY TYPE</b>   | Non-Statutory                       |               |
| <b>REVIEW FREQUENCY</b>                                    | Annually – December                 |               |
| <b>RESPONSIBLE</b>   |                                     |               |
| Leadership Team  | School Business Manager             |               |
| Governing Committee  | Resources, Audit and Risk Committee |               |
| <b>APPROVED/MEETING</b>                                    | Full Governing Body                 | 08.12.2025    |
| <b>UPDATED:</b><br>Shared Drive<br>Website (if applicable) | N/A                                 | 08.12.2025    |

**Courage Commitment Compassion**

## Contents:

### Statement of Intent

1. Legal Framework
2. Definitions
3. Roles and Responsibilities
4. Purpose and justification
5. Data Protection
6. Protocols
7. Security
8. Code of Practice
9. Access
10. Monitoring and Review
11. Appendices

### Statement of Intent

Newlands Girls School takes the responsibility towards the safety of staff, visitors and pupils very seriously. To that end surveillance / CCTV cameras are in operation in some areas of the school.

The purpose of this policy is to manage and regulate the use of the surveillance and CCTV systems at the school and ensure that:

- UK GDPR regulations are complied with.
- The images that are captured are usable for the purposes required.
- To reassure that those persons whose images are being captured, that the images are being handled within data protection legislation.

This policy covers the use of surveillance and CCTV systems which 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

The surveillance system will be used to:

- To ensure the safety and security of the school and its staff, pupils and visitors.
- Deter criminal acts against persons and property.
- Assist the police in identifying persons who have committed an offence.

## 1. Legal Framework

This policy has due regard to all relevant legislation and statutory guidance including, but not limited to, the following:

- Regulation of Investigatory Powers Act 2000
- Protection of Freedoms Act 2012
- The UK General Data Protection Regulation (GDPR)
- Data Protection Act 2018
- 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
- School Standards and Framework Act 1998
- Children Act 1989
- Children Act 2004
- Equality Act 2010

This policy operates in conjunction with the following statutory and non-statutory guidance:

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

This policy operates in conjunction with the following school policies:

- Photography and Images Policy
- Online Safety Policy
- Freedom of Information Policy
- School Premises Policy
- Data Protection Policy

## 2. Definitions

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

- **Data Protection Officer (DPO)** – Satswana Limited, Suite G12 Ferneberga House, Alexandra Road, Farnborough, Hants GU14 6DQ [info@satswana.com](mailto:info@satswana.com), 01252-759177
- **Data Protection Controller** – Newlands Girls School, Farm Road, Maidenhead SL6 5JB
- **School Data Protection Lead** – Kate Foreman, School Business Manager [kateforeman@newlandsgirls.co.uk](mailto:kateforeman@newlandsgirls.co.uk), 01628 502673
- **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.

- **Overt surveillance** – Surveillance which is clearly visible and signposted around the school and does not fall under the Regulation of Investigatory Powers Act 2000.
- **Covert surveillance** – Newlands Girls' School will not engage in covert surveillance.

### 3. Roles and Responsibilities

The role of the DPO includes assisting and providing professional advice to the school on:

- Dealing with freedom of information requests and subject access requests (SARs) in line with legislation, including the Freedom of Information Act 2000.
- Ensuring that all data controllers at the school handle and process surveillance and CCTV footage in accordance with data protection legislation.
- Ensuring that surveillance and CCTV footage is obtained in line with legal requirements.
- Ensuring that surveillance and CCTV footage is destroyed in line with legal requirements when it falls outside of its retention period.
- 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, their rights for the data to be destroyed and the measures implemented by the school to protect individuals' personal information.
- Preparing reports and management information on the school's level of risk related to data protection and processing performance.
- Reporting to the highest management level of the school, e.g. 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 assessment (DPIA) and providing advice where requested.
- Presenting reports regarding data processing at the school to senior leaders and the governing

The school, as the corporate body, is the data controller. The governing board therefore has overall responsibility for ensuring that records are maintained, including security and access arrangements in accordance with regulations.

The School Business Manager deals with the day-to-day matters relating to data protection and thus, for the benefit of this policy will act as the data controller.

The role of the data controller includes:

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

- Meeting with the DPO to decide where CCTV is needed to justify its means.
- Reviewing the Surveillance and CCTV Policy to ensure it is compliant with current legislation.
- Monitoring legislation to ensure the school is using surveillance fairly and lawfully.
- Communicating any changes to legislation with all staff members.

#### **4. Purpose and justification**

The school will only use surveillance cameras for the safety and security of the school and its staff, pupils and visitors, to deter criminal acts against persons and property and to assist the police in identifying persons who have committed an offence.

The school will only conduct surveillance as a deterrent and under no circumstances will the surveillance and the CCTV cameras be present in school classrooms or any changing facility.

If the surveillance and CCTV systems are no longer required, the school will deactivate them.

#### **5. Data Protection**

Data collected from surveillance and CCTV will be processed in line with the Data Protection Policy.

The use of surveillance cameras, CCTV, will be critically analysed using a DPIA, in consultation with the DPO.

A DPIA will be carried out prior to the installation of any surveillance, CCTV. 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.

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.

Where the school identifies a high risk to an individual's interests, and it cannot be overcome, the school will consult the ICO before they use CCTV, and the school will act on the ICO's advice.

The school will ensure that the installation of the CCTV system will always justify its means.

If the use of a CCTV system is too privacy intrusive, the school will seek amendments.

Surveillance and CCTV systems will not be intrusive. Pupils, 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

**The school does not use Facial Recognition Technology.**

## **6. Protocols**

**The surveillance system is a closed digital system.**

Warning signs have been placed throughout the premises where the surveillance system is active, as mandated by the ICO's Code of Practice.

The surveillance system has been designed for necessary effectiveness and efficiency, only areas highlighted below are covered by CCTV.

The surveillance system will not be used to focus on a particular group or individual unless an immediate response to an incident is required.

The surveillance system will not be trained on private vehicles or property outside the perimeter of the school.

## **7. Security**

Access to the surveillance system, software and data will be strictly limited to authorised operators, and will be password protected, and where appropriate, will be encrypted.

The school's authorised CCTV system operators are:

- Jo Capon, Headteacher
- Kate Foreman, School Business Manager
- Gareth Evans, Facilities and Transport Manager, Data Processor (except the medical room and the canteen)
- The reception staff

The main control facility is kept secure and locked when not in use.

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.

Surveillance and CCTV systems will be tested for security flaws once a month to ensure that they are being properly maintained at all times.

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.

The ability to produce copies of information will be limited to the appropriate staff.

Any unnecessary footage captured will be securely deleted from the school system.

**The audio feature on the CCTV system is deactivated.**

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

Visual display monitors are located in the main office and the Facilities and Transport Manager's office.

## **8. Code of Practice**

The school understands that recording images of identifiable individuals constitutes as processing personal information, so it is done in line with data protection principles.

The school notifies all pupils, staff and visitors of the purpose for collecting surveillance data via notice boards, signs, letters and emails.

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

CCTV footage will be retained for 32 days as standard. Where footage is required for an ongoing investigation or incident, it may be securely archived for up to 12 months before deletion. This aligns with the school's Data Management Policy and UK GDPR principles of data minimisation. For security purposes; the headteacher and the data controller are responsible for keeping the records secure and allowing access.

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

The school will ensure that the surveillance and CCTV system is used to create a safer environment for staff, pupils and visitors to the school, and to ensure that its operation is consistent with the obligations outlined in data protection legislation. The policy is available from the [www.newlandsgirlsschool.co.uk](http://www.newlandsgirlsschool.co.uk).

The surveillance and CCTV system will:

- Be designed to consider its effect on individuals and their privacy and personal data.
- Be transparent and include a contact point which enables people to request information and submit complaints via the DPO.
- 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.
- 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, including supporting public safety, the protection of pupils, staff and volunteers, and law enforcement.
- Be accurate and well maintained to ensure information is up-to-date.

## **9. Access**

Please refer to the school's Data Protection Policy.

All disks and hard drives containing images belong to, and remain the property of, the school.

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

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.

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.

Requests for access or disclosure will be recorded and the headteacher will make the final decision as to whether recorded images may be released to persons other than the police.

## **10. Monitoring and Review**

This policy will be monitored and reviewed on an annual basis by the School Business Manager and the headteacher in collaboration with the Facilities and Transport Manager.

The School Business Manager will be responsible for monitoring any changes to legislation that may affect this policy, and make the appropriate changes accordingly.

The headteacher will communicate changes to this policy to all members of staff.



| CCTV SUBJECT ACCESS REQUEST FORM   |                          |
|--|--------------------------|
| <i>This form is used to confirm the identity of the Data Subject (the person in the footage), the identity and authority of the applicant (where applicable) and to assist in locating Personal Data relating to the data subject.</i>   |                          |
| PLEASE SELECT ONE OF THE FOLLOWING:  |                          |
| I am the Data Subject. I am requesting my own CCTV personal information  | <input type="checkbox"/> |
| I am not the Data Subject. I am requesting information on behalf of someone else   | <input type="checkbox"/> |
| APPLICANT INFORMATION  |                          |
| Title:   | First Name:              |
| Surname:   |                          |
| Address:   |                          |
| Town/City:   | County:                  |
| Postcode:  | Telephone:               |
| Contact Email Address:   |                          |
| REPRESENTATIVE'S INFORMATION (IF YOU ARE REQUESTING ON BEHALF OF A THIRD PARTY)  |                          |
| Title:   | First Name:              |
| Surname:   |                          |
| Address:   |                          |
| Town/City:   | County:                  |
| Postcode:  | Telephone:               |
| Contact Email Address:   |                          |
| Please explain your entitlement to receive the Data Subject's CCTV images - e.g. Data Subject's signed authority-  |                          |
| What authorisation have you enclosed? E.g.: Power of Attorney, Court Order stamped or Signed Consent-  |                          |
| ACCEPTED PROOF OF IDENTIFICATION   |                          |
| <p><b>Verification documents for Name</b>, such as: Full valid driving license, birth certificate, full valid current passport.</p> <p><b>Verification documents for Address, such as:</b> Utility bill (gas, electricity, water in the data subject's name and 3 months old or less) or letter from a government department.</p> <p><b>Recent passport sized photograph:</b> to help identify the data subject in recorded images held.</p> <p><b>Please do not send original documents, good quality photocopies are acceptable.</b></p> |                          |

## FOOTAGE DETAILS REQUIRED

Our search for information relating to the Data Subject (the person in the footage) will be based on the information provided below.

Date and time of incident when you believe image was captured (within one hour):

|  |
|--|
|  |
|  |
|  |
|  |

Location of the incident:

|  |
|--|
|  |
|  |
|  |
|  |

Brief description of incident:

|  |
|--|
|  |
|  |
|  |
|  |

Brief description of the clothing worn by the data subject at time of incident:

|  |
|--|
|  |
|  |
|  |
|  |

## REPRESENTATIVE DECLARATION

**WARNING – it is a criminal offence to obtain another person's information by deception.**

I confirm I am the appointed representative of the Data Subject. I wish to receive a copy of the Data Subjects CCTV images and have included a copy of the relevant permission.

Representative's Signature:

Date:

**SIGNATURE**

In exercise of the right granted to me under the terms of the General Data Protection Regulation

I request that you provide me with a copy of the CCTV images about me which you process for the purposes I have indicated above.

I confirm that I am the Data Subject and not someone acting on his/her behalf.

I hereby give my authority for the representative named above to make a Subject Access Request on my behalf under the General Data Protection Regulation.

Signature of applicant:

Date:

Please send the completed form, along with all required proofs of ID or representation.

OFFICIAL USE ONLY – For completion by CCTV Manager only

Request (please tick)

Granted

Denied

|   |  |
|---|--|
| Camera number(s) / name(s)                                      |  |
| Start time of recording period                                  |  |
| End time of recording period                                    |  |
| Original CD/tape serial number / identifier                     |  |
| Date of issue   |  |
| Copy CD/tape serial number / identifier                         |  |
| Confirm copy tape/CD made for FODDC retention and where stored. |  |

Before issuing CCTV images, please check and sign

CCTV Manager  
Name:

Signature: