The Robert Carre Trust

Surveillance and CCTV Policy

Contents:

Statement of intent

At the Robert Carre Trust, we take our responsibility towards the safety of staff, visitors and students very seriously. To that end, we use surveillance cameras to monitor any instances of aggression or physical damage to our schools and their members.

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

- We comply with the UK GDPR.
- The images that are captured are useable 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 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, or harm
- Using images of individuals that could affect their privacy

The surveillance system will be used to:

- Maintain a safe environment.
- Ensure the welfare of students, staff 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 (Student 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 (2021) 'The Surveillance Camera Code of Practice'
- ICO (2021) 'Guide to the UK General Data Protection Regulation (UK GDPR)'
- ICO (2017) 'In the picture: A data protection code of practice for surveillance cameras and personal information'
- ICO (2022) 'Video Surveillance'
- DfE (2022) 'Protection of biometric data of children in schools and colleges

This policy operates in conjunction with the following school policies:

- ICT Acceptable Use – Media form - Policy
- Online Safety Policy

- Freedom of Information Policy
- Trust Security Policy
- GDPR Policy

2. Definitions

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

- **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** – any use of surveillance which is intentionally not shared with the subjects it is recording. Subjects will not be informed of such surveillance.

The school does not condone the use of covert surveillance when monitoring the school's staff, students and/or volunteers. Covert surveillance will only be operable in extreme circumstances.

- **Biometric data** – data which is related to the physiological characteristics of a person, which confirm the unique identification of that person, such as fingerprint recognition, facial recognition (FRT), or iris recognition.
- **Automated biometric recognition system** – a system which uses technology to measure an individual's physical or behavioural characteristics by using equipment that operates 'automatically'.
- **Facial recognition** – the process by which a person can be identified or otherwise recognised from a digital facial image. Cameras are used to capture these images and facial recognition technology software produces a biometric template.

3. Roles and responsibilities

The role of the DPO includes:

- 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 consent is clear, positive and unambiguous. Pre-ticked boxes and answers inferred from silence are non-compliant with the UK GDPR.
- 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 board.

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

The ICT Services 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.
- Ensuring that the processing of any biometric data, including any processing carried out by a third party on their behalf complies with the Data Protection Act 2018, UK GDPR and Protection of Freedoms Act 2012.
- Identifying the additional risks associated with using automated biometric technology by conducting a DPIA ensuring decisions are documented.
- Ensuring that the processing of biometric data is done so in line with the school's Protection of Biometric Data Policy

The role of the Executive Headteacher/Headteacher, supported by the ICT Services Manager, includes:

- Meeting with the DPO and the ICT Services Manager to decide where CCTV is needed to justify its means.
- Conferring with the DPO with regard to the lawful processing of the surveillance and CCTV footage.
- 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 members of staff.

4. Purpose and justification

The Trust will only use surveillance cameras for the safety and security of the schools, staff, students and visitors.

Surveillance will be used as a deterrent for unsafe behaviour, harm and damage to the schools.

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

If the surveillance and CCTV systems fulfil their purpose and are no longer required, the Trust will deactivate them.

5. Data protection

Data collected from surveillance and CCTV will be:

- Processed lawfully, as determined by a DPIA, or from advice from the DPO. In less common circumstances, lawful processing will be determined by a legitimate interests assessment (LIA).
- Processed fairly, in a manner that people would reasonably expect, and taking into account advancements in technology that may not be anticipated by some people.
- Processed in a transparent manner, meaning that people are informed when their data is being captured.
- Collected for specified and legitimate purposes – data will not be processed further in a manner that is incompatible with the following purposes:
    - Further processing for archiving data in the public interest
    - Scientific or historical research
    - Statistical 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 is inaccurate, having regard to the purposes for which they are processed, is 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 is 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.

The use of surveillance cameras, CCTV, and biometric systems 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, or biometric system. 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.

Sensitive data obtained via biometric technology will be processed via special conditions (listed in Article 9 of the UK GDPR).

If the DPIA reveals any potential security risks or other data protection issues, the Trust will ensure it have provisions in place to overcome these issues.

Where a 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 Trust will ensure that the installation of the surveillance and CCTV systems will always justify its means.

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

Surveillance and CCTV systems will not be intrusive. Students, 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 use of any video conferencing technology will be fair and transparent. Any students and staff who are part of any video conference calls will be informed of its purpose, and recording and publication of any video to an indefinite audience will be consented to and will not be used outside of the intended purpose.

FRT will be justifiable, proportionate, and able to address specific needs.

6. Protocols

The surveillance system will be registered with the ICO in line with data protection legislation.

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. Warning signs will be more prominent in areas where surveillance is less expected to be in operation, and when using systems that can capture a large amount of personal data at one time.

The surveillance system has been designed for maximum effectiveness and efficiency; however, the school cannot guarantee that every incident will be detected or covered and 'blind spots' may exist.

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.

In exceptional cases where large amounts of information need to be collected and retained, the school will consider using cloud storage. This will be secure and only accessible to authorised individuals.

The Trust's authorised CCTV system operators are:

- Executive Headteacher and Headteachers of schools in the Trust
- Senior Leadership Teams of schools in the Trust
- DPO
- ICT Support Team
- Estates Team
- Office Administrative Teams (Paxton Net2 Security System)
- Sixth Form Management Teams (Access to Sixth Form Common Rooms)

Access to the CCTV system is only available using software installed on an authorised system operator's user account which is secured by password.

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.

The DPO, ICT Services Manager, and Executive Headteacher/ Headteacher will decide when to record footage, e.g., a continuous loop outside the school grounds to deter intruders.

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.

Where a CCTV camera can deliver an audio stream this functionality has been disabled. It is not possible for a system operator to enable audio. The only exception to this is the Paxton Net2 security system which delivers real time audio to an Entry Monitor to facilitate secure visitor site access when paired with an Entry Panel. No audio is recorded by the Paxton Net2 security system.

Any cameras that present faults will be repaired, removed, or disabled promptly as to avoid any risk of a data breach.

The schools authorised CCTV system operators have camera monitoring software installed on their computer workstations. Access to this software is secured by membership of a

Microsoft Windows Active Directory Security Group and user password. Visual display screens are not available for public/open viewing.

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 students, 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.

All surveillance footage will be kept for 30 days for security purposes; the Executive Headteacher/Headteacher and the data controller are responsible for keeping the records secure and allowing access.

The school has a surveillance system for the purpose of the prevention and detection of crime and the promotion of the health, safety and welfare of staff, students and visitors.

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, students 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 Trust website.

The surveillance and CCTV system will:

- Be designed to take into account 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.
- Only keep images and information for as long as required.
- Restrict access to retained images and information with clear rules on who can gain access.
- 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 students, staff and volunteers, and law enforcement.

- Be accurate and well maintained to ensure information is up-to-date.

To comply with the requirements of the Protection of Freedoms Act 2012, the school will notify all parents of its intention to process students' biometric data, and emphasise that parents may object at any time to the processing of the information.

The school will ensure that students' biometric data is not taken or used as part of a biometric recognition system if students under the age of 18 object or refuse to participate in activities that involve the processing of their biometric data. The school is aware that a student's objection or refusal overrides any parental consent to the processing of data.

The Trust will ensure that information is included in its privacy notices that explains how biometric data is to be processed and stored, including the rights available to individuals in respect of the processing.

Reasonable alternative arrangements will be provided for students who do not use automated biometric recognition systems either because their parents have refused consent or due to the student's own refusal to participate in the collection of their biometric data.

The alternative arrangements will ensure that students do not suffer any disadvantage or difficulty in accessing services and premises. Likewise, such arrangements will not place any additional burden on parents whose children are not participating in such a system.

9. Access

Under the UK GDPR, individuals have the right to obtain confirmation that their personal information is being processed.

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

Individuals have the right to submit an SAR to gain access to their personal data in order to verify the lawfulness of the processing.

Individuals have the right to have personal data erased if:

- The data is no longer necessary for the original purpose it was collected for.
- They are relying on legitimate interests as a basis for processing, the individual objects to the processing of their data, and there is no overriding legitimate interest to continue the processing.
- The data has been processed unlawfully.
- There is a specific legal obligation.

There are certain exceptions where the right to erasure cannot be exercised, these include, but are not limited to:

- Where the processing is needed for the performance of a task in the public interest or an official authority.
- Certain research activities.
- Compliance with a specific legal obligation.

As an alternative to the right of erasure, individuals can limit the way their data is used if they have issues with the content of the data held by the school or they object to way it was processed.

Data can be restricted by either:

- Moving the data to another processing system.
- Making the data unavailable to users.
- Temporarily removing published data from a website.

The Trust will verify the identity of the person making the request before any information is supplied.

A copy of the information will be supplied to the individual free of charge; however, the Trust may impose a 'reasonable fee' to comply with requests for further copies of the same information. The individual will either be provided with a permanent copy of the information or allowed to view the information.

Where an SAR has been made electronically, the information will be provided in a commonly used electronic format.

Requests by persons outside the Trust for viewing or copying disks, or obtaining digital recordings, will be assessed by the Executive Headteacher/Headteacher, who will consult the DPO, on a case-by-case basis with close regard to data protection and freedom of information legislation.

Where a request is manifestly unfounded, excessive or repetitive, a reasonable fee will be charged.

All fees will be based on the administrative cost of providing the information.

All requests will be responded to without delay and at the latest, within one month of receipt.

In the event of numerous or complex requests, the period of compliance will be extended by no more than an additional 20 working days. The individual will be informed of this extension, and will receive an explanation of why the extension is necessary, within one month of the receipt of the request.

Where a request is manifestly unfounded or excessive, the Trust holds the right to refuse to respond to the request. The individual will be informed of this decision and the reasoning behind it, as well as their right to complain to the ICO and to a judicial remedy, within one month of the refusal.

In the event that a large quantity of information is being processed about an individual, the school will ask the individual to specify the information the request is in relation to.

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 Executive Headteacher/ 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 DPO and the Executive Headteacher/Headteacher.

The headteacher 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.

Approved by the Trustees on 28 January 2024

Next Review Due January 2025 (annually)

Appendix A - Data Protection Impact Assessment

Location of surveillance camera system: Robert Carre Trust (Carre's Grammar School and Kesteven & Sleaford High School)

Date of Assessment: October 2023

Review Date: October 2024

Persons Responsible

ICT Services Manager

Data Protection Manager

Director of Finance and Resources

GDPR and Data Protection Act 2018 and Surveillance Camera Code of Practice

1 What are the problems that you need to address in defining your purpose for using the surveillance camera system?

A CCTV System is installed consisting of internal and external cameras. Internal cameras monitor reception areas and computer suites. The CCTV system is for the purpose of providing site security and safeguarding for stakeholders and visitors.

2 Can surveillance camera technology realistically mitigate the risks attached to those problems?

External and reception cameras are required to achieve the appropriate level of safeguarding as highlighted by Health and Safety Advisors and indicated by OFSTED. Internal cameras within computer suites are for the purpose of equipment protection.

3 What other less privacy-intrusive solutions such as improved lighting have been considered?

Other appropriate measures are also in place to help maintain site security including lighting, gates (Paxton Net2), and fencing. CCTV is also required to deter those from entering the site with the intention of causing harm to our stakeholders and visitors, damage to the school's property, or theft of the school's property and/or contents. Internal cameras will deter those who intend to cause damage to school property or cause a safeguarding risk to others.

4 What is the lawful basis for using the surveillance camera system?

The lawful basis for using the surveillance camera system is that of Legitimate Interests.

5 Can you describe the information flows?

The CCTV system consists of AXIS POE network IP cameras, the model of which will depend on current models and availability. Additionally, AXIS Camera Station software will be used to securely assign differentiated access and provide a mechanism for secure storage of data.

CCTV footage can be live monitored by those authorised to do so. Footage is viewed, recorded, and retained in accordance with Trust policies. Footage automatically overwrites previously recorded data and is held for no longer than one month unless footage is saved securely for the purpose of ongoing investigations.

Data is saved securely to a networked server which is managed and maintained as part of the Trust's computer network to ensure data integrity.

6 What are the views of those who will be under surveillance?

Where necessary the installation is discussed with those working within an affected area. Personnel have accepted the requirement for this additional level of security and monitoring.

7 What are the benefits to be gained from using surveillance cameras?

We have a duty of care to ensure a safe working environment for stakeholders and visitors. The system enables us to deter and investigate any onsite incidents. The site, despite fencing, can and has been accessed in the past by persons not authorised to be on site, this causes a potential risk to stakeholders and visitors. The site has also been subject to damage and attempted unauthorised entry.

8 What are the privacy risks arising from this surveillance camera system?

Appropriate action is taken when situating and angling the cameras to ensure, as much as reasonably practicable, only the school site and assets are captured by the CCTV system. Appropriate signage is displayed alerting those entering the site that CCTV is in operation. Recording will be retained for no more than 1 month before being automatically overwritten, unless required for the purpose of ongoing investigations. Only those authorised to do so will have access to the CCTV software and will only be viewed by others for the strict purpose of assisting with an investigation. It has been assessed that there will be little impact on individuals being recorded and will only serve to ensure their safety whilst on the school site, there will be no use of CCTV in areas which can be deemed an intrusion, for example toilets or changing rooms.

9 Have any data protection by design and default features been adopted to reduce privacy intrusion? Could any features be introduced as enhancements?

Appropriate action is taken when situating and angling the cameras to ensure as much as reasonably practicable only the school site and assets are captured by the CCTV system. Privacy masks on the camera feeds are set as required/appropriate to minimise the risk of the school CCTV capturing residential properties surrounding the school, or sensitive areas, once the cameras are in their final positions.

10 What organisations will be using the surveillance camera images, and where is the controller responsibility under the GDPR and Data Protection Act 2018?

Robert Carre Trust central services staff; Estates Team, ICT Support Team, Senior Leadership, and pastoral staff during investigations.

Footage to be shared with government services, e.g., Police, when lawfully required to do so.

11 Do the images need to be able to recognise or identify individuals, or could the purpose be met using images in which individuals cannot be identified?

Footage must be clear enough to allow identification of individuals to aid in the investigation of safeguarding incidents, damage to school property and unlawful access to the school site.

12 How will you inform people that they are under surveillance and respond to any Subject Access Requests, the exercise of any other rights of data subjects, complaints or requests for information?

Signage is situated on entry to the school site, to alert all stakeholders and visitors to the use of CCTV on site. Location information, for the purpose of safeguarding or equipment damage investigations, is shared with staff through annual training.

Any Subject Access Requests are dealt with in accordance with Trust policies. Privacy notices are displayed on our school websites.

13 How will you know if the particular camera system/hardware/software/firmware being considered does deliver the desired benefits now and in the future?

Steps have been taken to ensure the chosen system is suitable for use and will meet any future requirements. The chosen AXIS solution is widely used and can provide the features required whilst ensuring live and recorded data is secure and protected from unauthorised access. Consideration is made regarding the placement of cameras, where it is not possible to physically angle a camera to avoid residential properties, or sensitive areas, it is possible to set masked areas within the camera software. Masking within the camera software ensures no image data is available either via live feed of recording, this feature cannot be overridden by an operator.

14 What future demands may arise for wider use of images and how will these be addressed?

Additional external cameras may be required to provide expanded site coverage or address future problem areas if they arise. Additional internal cameras may be required for the security of school property, if a new requirement is identified, or to ensure the safety and wellbeing of our stakeholders and visitors. Any additional cameras will be carefully considered, and this Impact Assessment reviewed.

15 Have you considered the extent to which your surveillance camera system may interfere with the rights and freedoms conferred under the European Convention on Human Rights?

The system is necessary to enhance site security and protect equipment whilst also providing a higher level of safeguarding to our stakeholders. There is a minimal impact on ECHR.

16 Do any of these measures discriminate against any particular sections of the community?

No areas of the school site are subject to a single section of our community, therefore there will be no discrimination.