NICHOLAS CHAMBERLAINE SCHOOL

CCTV Policy

Date: September 2026
Review Due: September 2027

Reviewed Annually

NICHOLAS CHAMBERLAINE SCHOOL

Contents

Background..... 3

Justification for use of CCTV..... 4

Data Protection Impact Assessments..... 4

Location of Cameras..... 4

Covert Surveillance..... 5

Notification..... 5

Storage and Retention..... 5

Access..... 6

Subject Access Requests (SARs)..... 7

Complaints..... 7

Staff Training..... 7

Responsibilities..... 8

Policy Review and Approval..... 8

1. Background

1.1 Nicholas Chamberlaine School uses closed circuit television (CCTV) images for the prevention, identification and reduction of crime and to monitor the school buildings in order to provide a safe and secure environment for pupils, staff and visitors, and to prevent the loss or damage to school property.

1.2 CCTV surveillance at the School is intended for the purposes of:

- protecting the school buildings and school assets, both during and after school hours;
- promoting the health and safety of staff, pupils and visitors;
- preventing bullying;
- reducing the incidence of crime and anti-social behaviour (including theft and vandalism);
- supporting the Police in a bid to deter and detect crime;
- assisting in identifying, apprehending and prosecuting offenders; and
- ensuring that the school rules are respected so that the school can be properly managed.

1.3 The system comprises of 64 fixed (non-PTZ) cameras.

1.4 The CCTV system is owned and operated by the school and the deployment of which is determined by the school's leadership team. The system is standalone and operated by the School.

1.5 The CCTV is monitored centrally from the ICT Support office, Head's office, Student Services office and Head's PA PC. A list of staff members with direct monitoring access is available on request. Footage is recorded on 3 NVR devices with equipment stored securely in the ICT Support Office.

1.6 The school's CCTV Scheme is registered with the Information Commissioner under the Data Protection Act 2018 and the UK General Data Protection Regulation (UK GDPR).This policy outlines the school's use of CCTV and how it complies with the Act.

1.7 All authorised operators and employees with access to images are aware of the procedures that need to be followed when accessing the recorded images. All operators are trained in their responsibilities under the CCTV Code of Practice. All employees are aware of the restrictions in relation to access to, and disclosure of, recorded images

1.8 The school complies with Information Commissioner's Office (ICO) CCTV Code of Practice to ensure it is used responsibly and safeguards both trust and confidence in its continued use.

1.9 The use of the CCTV system will be conducted in a professional, ethical and legal manner and any diversion of the use of CCTV security technologies for other purposes is prohibited by this policy e.g. CCTV will not be used for monitoring employee performance.

1.10 CCTV monitoring of public areas for security purposes will be conducted in a manner consistent with all existing policies adopted by the school, including Equality & Diversity Policy, Dignity at Work Policy, Codes of Practice for dealing with complaints of Bullying & Harassment and Sexual Harassment and other relevant policies, including the provisions set down in equality and other educational and related legislation.

2. Justification for Use of CCTV

2.1 The use of CCTV to control the perimeter of the school buildings for security purposes has been deemed to be justified by the leadership team. The system is intended to capture images of intruders or of individuals damaging property or removing goods without authorisation or of antisocial behaviour.

2.2 CCTV systems will not be used to monitor normal teacher/student classroom activity in school.

2.3 In other areas of the school where CCTV has been installed, e.g. hallways, stairwells and hand washing areas in the student toilets, the school has demonstrated that there is a proven risk to security and/or health & safety and that the installation of CCTV is proportionate in addressing such issues that may have arisen prior to the installation of the system.

3. Data Protection Impact Assessments

3.1 Where new CCTV systems or cameras are to be installed, the School will carry out a full Data Protection Impact Assessment identifying risks related to the installation and ensuring full compliance with data protection legislation. This may involve the need for consultation with staff, parents and local residents. This process will include consultation with the Griffin Schools Trust Data Protection Officer (DPO) to ensure full compliance with UK GDPR requirements.

3.2 Where existing CCTV systems are in operation as of August 2024, the school will endeavour to carry out a full Data Protection Impact Assessment on any upgrade or replacement of the system.

4. Location of Cameras

4.1 Cameras will be sited so they only capture images relevant to the purposes for which they are installed and care will be taken to ensure that reasonable privacy expectations are not violated.

4.2 The School will ensure that the location of equipment is carefully considered to ensure that images captured comply with the Data Protection Act. The school will make every effort to position cameras so that their coverage is restricted to the school premises, which may include outdoor areas.

4.3 CCTV will only be used in teaching areas where there is a significant amount of expensive equipment that could be vandalised or stolen, such as in IT suites.

4.4 Use of CCTV to monitor areas where individuals would have a reasonable expectation of privacy would be difficult to justify. Nicholas Chamberlaine School has endeavoured to select locations for the installation of CCTV cameras which are least intrusive to protect the privacy of individuals. A full list of where the school cameras are and their use are listed on the DPIA form and available on our website or via the main office.

4.5 Cameras placed so as to record external areas are positioned in such a way as to prevent or minimise recording of passers-by or of another person's private property.

4.6 CCTV Video Monitoring and Recording of Public Areas may take place for the following purposes:

- Protection of school buildings and property: Building perimeters, entrances and exits, lobbies and corridors, special storage areas, office locations, receiving areas for goods/services
- Monitoring of Access Control Systems: Monitor and record restricted access areas at entrances to buildings and other areas
- Verification of Security Alarms: Intrusion alarms, exit door controls, external alarms • Video Patrol of Public Areas: Parking areas, Main entrance/exit gates, Traffic Control
- Criminal Investigations (carried out by police): Robbery, burglary and theft surveillance

5. Covert Surveillance

5.1 Nicholas Chamberlaine School will not engage in covert surveillance.

6. Notification

6.1 A copy of this CCTV Policy will be provided on request to staff, students, parents and visitors to the school and will be made available on the school website.

6.2 The location of CCTV cameras will also be indicated and adequate signage will be placed at each location in which a CCTV camera(s) is sited to indicate that CCTV is in operation.

6.3 Adequate signage will also be prominently displayed at the entrance to Nicholas Chamberlaine School property. Signage shall include the name and contact details of the data controller as well as the specific purpose(s) for which the CCTV camera is in place in each location.

Appropriate locations for signage will include:

- at entrances to premises, i.e. external doors and school gates
- reception area
- at or close to each corridor entrance

7. Storage and Retention

7.1 Footage is typically retained for up to 31 days. However, due to system capacity, some footage may be stored for longer periods. Retention beyond 31 days will only occur where necessary for operational, security, or safeguarding purposes, and such footage will be securely deleted once no longer required. Any extended retention must be authorised by the Head of School.

7.2 The images/recordings will be stored in a secure environment with a log of access kept.

7.3 Access will be restricted to authorised personnel. Supervising the access and maintenance of the CCTV System is the responsibility of the Head. The Head may delegate the administration of the CCTV System to another staff member.

7.4 In certain circumstances, the recordings may also be viewed by other individuals in order to achieve the objectives set out above. When CCTV recordings are being viewed, access will be limited to authorised individuals on a need-to-know basis.

7.5 Recorded footage will be stored in a secure environment with a log of access kept. Access will be restricted only to authorised personnel. All NVRs and monitoring devices are password-protected and stored securely. Access to footage is restricted to authorised users only and monitored by the Head of School and IT and Network Manager.

8. Access

8.1 Recorded footage and the monitoring equipment will be securely stored in a restricted area. Unauthorised access to that area will not be permitted at any time. The area will be locked when not occupied by authorised personnel. A log of access to footage will be maintained.

8.2 Access to the CCTV system and stored images will be restricted to authorised personnel only.

8.3 When accessing images two authorised members of staff must be present. A written record of access will be made. Records of access will be kept.

8.4 A record of the date of any disclosure request along with details of who the information has been provided to (the name of the person and the organisation they represent), why they required it and how the request was dealt with will be made and kept, in case of challenge.

8.5 Data will be provided to those requests authorised in a permanent format where possible. If this is not possible the data subject will be offered the opportunity to view the footage.

8.6 In relevant circumstances, CCTV footage may be accessed:

- By the police where Nicholas Chamberlaine School (or its agents) are required by law to make a report regarding the commission of a suspected crime; or
- Following a request by the police when a crime or suspected crime has taken place and/or when it is suspected that illegal/anti-social behaviour is taking place on Nicholas Chamberlaine School property, or
- To the HSE and/or any other statutory body charged with child safeguarding; or
- To assist the Head in establishing facts in cases of unacceptable student behaviour, in which case, the parents/guardians will be informed; or
- To data subjects (or their legal representatives), pursuant to a Subject Access Request or
- To individuals (or their legal representatives) subject to a court order.
- To the school insurance company where the insurance company requires same in order to pursue a claim for damage done to the insured property.

9. Subject Access Requests (SAR)

9.1 Individuals have the right to request access to CCTV footage relating to themselves under the Data Protection Act.

9.2 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.

9.3 The school will respond to requests within 30 calendar days of receiving the request, in line with UK GDPR and the Trust's Subject Access Request Policy.

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

9.5 A record of the date of the disclosure along with details of who the information has been provided to (the name of the person and the organisation they represent) and why they required it will be made.

9.6 In giving a person a copy of their data, the school provide a still/series of still pictures or a disk with relevant images. However, other images of other individuals will be obscured before the data is released.

9.7 Where footage contains images relating to 3rd parties, the school will take appropriate steps to mask and protect the identities of those individuals.

9.8 Where a parent requests to view CCTV footage, the school will determine whether the footage contains images of other identifiable individuals. In such cases, the footage will not be shared or copied. Instead, the Head may arrange a controlled on-site viewing of the relevant segment, or where appropriate, ask a nominated school governor to review the footage and provide an impartial summary of the findings. This ensures the privacy of all individuals is protected while allowing parental concerns to be addressed.

10. Complaints

10.1 Complaints and enquiries about the operation of CCTV within the school should be directed to the Head in the first instance.

11. Staff Training

11.1 Staff authorised to access the CCTV system will be trained to comply with this policy. Staff will understand that all information relating to the CCTV images must be handled securely.

11.2 Staff will receive appropriate training to enable them to identify and handle different requests according to regulations.

11.3 Staff misuse of surveillance system information will lead to disciplinary proceedings.

12. Responsibilities

12.1 The Head (or nominated deputy) will:

- Ensure that the use of CCTV systems is implemented in accordance with the policy set down by Nicholas Chamberlaine School
- Oversee and co-ordinate the use of CCTV monitoring for safety and security purposes within Nicholas Chamberlaine School
- Ensure that all existing CCTV monitoring systems will be evaluated for compliance with this policy
- Ensure that the CCTV monitoring at Nicholas Chamberlaine School is consistent with the highest standards and protections
- Review camera locations and be responsible for the release of any information or recorded CCTV materials stored in compliance with this policy
- Maintain a record of access (e.g. an access log) for the release of material recorded or stored in the system
- Ensure that recorded footage is not duplicated in any way
- Ensure that the perimeter of view from fixed location cameras conforms to this policy both internally and externally
- Give consideration to both students and staff feedback/complaints regarding possible invasion of privacy or confidentiality due to the location of a particular CCTV camera or associated equipment
- Ensure that all areas being monitored are not in breach of an enhanced expectation of the privacy of individuals within the school and be mindful that no such infringement is likely to take place
- Co-operate with the Health & Safety Officer of Nicholas Chamberlaine School in reporting on the CCTV system in operation in the school
- Ensure that external cameras are non-intrusive in terms of their positions and views of neighbouring residential housing and comply with the principle of "Reasonable Expectation of Privacy"
- Ensure that monitoring footage are stored in a secure place with access by authorised personnel only
- Ensure that digital recordings or images are stored for a period not longer than 31 days and are then erased unless required as part of a criminal investigation or court proceedings (criminal or civil).
- Ensure that when a zoom facility on a camera is being used, there is a second person present with the operator of the camera to guarantee that there is no unwarranted invasion of privacy
- Ensure that camera control is solely to monitor suspicious behaviour, criminal damage etc. and not to monitor individual characteristics
- Ensure that camera control is not infringing an individual's reasonable expectation of privacy in public areas

12.2 This policy has been reviewed with due regard to the Equality Act 2010 to ensure it does not disadvantage any protected group.

13. Policy review and approval

This policy will be reviewed annually by the Head and Griffin Schools Trust Data Protection Officer and approved by the Local Governing Body.