

CCTV Policy

Version 3

This policy applies to all NCLT schools and colleges.



Wingfield Academy



CONTENTS

Paragraph Number	Heading	Page Number
1.0	Introduction	3
2.0	Definitions	3
3.0	Purpose and Presence of CCTV Systems	4
4.0	Statement of Intent	4
5.0	Access to and Downloading of Recorded Images	5
6.0	Operation of CCTV Systems	6
7.0	Images Storage and Retention	7
8.0	Breach of this Policy	7
9.0	Assessment of the Scheme	7
10.0	Complaints	7
Appendix	A – Request Forms	8
	B – CCTV Request Process and Protocol	9
	Equality Impact Assessment	11

1.0 Introduction

- 1.1 This policy sets out to provide information and guidance on the management, operation and use of Closed-Circuit Television (CCTV) and associated recording systems which are in place across all New Collaborative Learning Trust ('NCLT' or the 'Trust') sites.
- 1.2 The information contained within this policy follows the guidelines of the data protection laws.
- 1.3 This policy and its contents are subject to a 3-year review; however, can be reviewed at any time should a valid reason arise and through consultation with all stakeholders and the Trust Chief Operating Officer (COO) and the Trust Data Protection Officer (DPO).
- 1.4 A number of CCTV systems are owned and operated by NCLT at its establishments. A CCTV system, comprising a small number of external cameras and recorder, is operated at Wingfield Academy by our PFI partner, EQUANS. Suitable retained contractors service and maintain the cameras within the Trust.

2.0 Definitions

- 2.1 The following are definitions as defined under the relevant data protection legislation:
 - **Authorised User** – individuals authorised by the Headteacher/Principal to access the CCTV system on their site in performance of their day to day duties. The Data Privacy Manager will maintain this list liaising with the Principal on each site to confirm each user.
 - **Data Controller** - A controller determines the purposes and means of processing personal data. In most cases, the Trust is a data controller.
 - **Data processors** - includes any person or organisation who processes personal data on behalf of a data controller. Employees of data controllers are excluded from this definition, but it does include suppliers who handle personal data on our behalf.
 - **Data Protection Laws**- The Data Protection Act 2018 and UK General Data Protection Regulations. The term 'Data Protection Laws' includes all applicable laws relating to the collection and use of personal data and privacy and codes of practice issued by the regulator.
 - **Data subjects** - includes all living individuals about whom the Trust holds personal data. A data subject need not be a UK national or resident. All data subjects have legal rights in relation to their personal data.
 - **DPIA** – Data Privacy Impact Assessment is a document comprising a checklist, which is used to assess the risk associated with collecting, processing and storing personal data of data subjects, for a particular purpose/project.
 - **DPM** - Data Privacy Manager
 - **DPO** - Data Protection Officer, assists the Trust to monitor internal compliance, inform and advise on data protection obligations and acts as a point of contact for data subjects and the Information Commissioner's Office (ICO).
 - **ICO** - Information Commissioner's Office.
 - **Images** – still images or video footage.
 - **Personal data** - refers to any information relating to a living, identifiable person who can be directly or indirectly identified in particular by reference to an identifier.

- **Processing** - is any activity that involves the use of personal data. It includes obtaining, recording or holding data, or carrying out any operation or set of operations on the data including organising, amending, retrieving, using, disclosing, erasing or destroying it. Processing also includes transferring personal data to third parties.
- **PTZ camera** – a pan-tilt-zoom camera
- **CCTV system** - the Trust's CCTV equipment including its cameras and recording device.
- **Special Category Data** - includes information about a person's racial or ethnic origin, political opinions, religious or similar beliefs, trade union membership, physical or mental health or condition, sexual life and/or sexual orientation, genetics, and biometric information (where it is used for ID purposes). Special category data is personal data that is more sensitive, and so requires more protection.
- **The Act** - The Data Protection Act 2018, which mandates how personal information is used by Data Controllers and Data Processors.
- **Third party** - means a natural or legal person, public authority, agency or body other than the data subject or controller.
- **Trust** - New Collaborative Learning Trust (NCLT)
- **Trust staff** - Any Trust employee or contractor who has been authorised to access any of the Trust's personal data and will include employees, consultants, contractors, and temporary staff hired to work on behalf of the Trust.

3.0 Purpose and Presence of CCTV Systems

- 3.1 The Trust has taken the measure of installing CCTV Systems across all sites to assist with the overall security management of our colleges and schools. The CCTV system is primarily in use for the following reasons:
- **To monitor and maintain the physical security of each NCLT site.**
 - **To protect the security of all NCLT property and assets.**
 - **To positively manage the personal safety of staff, students and visitors and reduce the fear of crime.**
 - **To assist law enforcement agencies with the prevention and detection of crime.**
- 3.2 The systems at each site comprises a number of fixed and PTZ cameras located internally and externally around the site and the recording equipment. All cameras at our Trust sites are monitored from within the site to which they belong. Cameras can be viewed on site and by the Trust's contracted monitoring company for premises security.
- 3.3 The CCTV system do not record sound.

4.0 Statement of Intent

- 4.1 The Trust is registered with the Information Commissioner as a Data Processor and will seek to comply with the data protection laws and the ICO's recommendations on the operation of CCTV systems.
- 4.2 The Trust recognises personal data processed in connection with the CCTV System is protected by the Act.
- 4.3 Cameras will be used to monitor activities within the Trust sites, its car parks and other public areas to identify criminal activity actually occurring, anticipated, or perceived, consistent with paragraph 3.2.
- 4.4 Staff have been instructed that static cameras are not to focus on private homes, gardens and other areas of private property.
- 4.5 Unless an immediate response to events is required, staff must not direct cameras at an individual(s), third-party property, without senior authorisation. This should be signed off by DPO or NCLT SLT, allowing the directed use of cameras to take place. A record of these special circumstances requests will be held centrally in accordance with the Regulation of Investigatory Powers Act 2000.
- 4.6 Personal data or knowledge secured as a result of CCTV system operation will not be used for any commercial purpose. Data will only be released to the media for use in the investigation of a specific crime and with the written authority of the Police. Data will never be released to the media for purposes of entertainment.
- 4.7 Visible signs showing that CCTV is in operation have been placed to the entrances at all Trust establishments operating CCTV.

5.0 Access to and Downloading of Recorded Images

Access within NCLT

- 5.1 The Trust is committed to ensuring that any recorded images are only used for the purposes outlined in this policy.
- 5.2 The Principal/Headteacher is permitted to authorise employees familiar with the requirements of this policy to access CCTV images pursuant to a purpose set out in paragraph 3.2. A record of access should be completed at the time, using the NCLT CCTV Form provided in Appendix A. The form provides for a record of: who required access; the image's date/time; the access date; and, the reason for access (consistent with paragraph 3.2).

Release of images to others in permitted circumstances

- 5.3 The Trust is committed to meeting the obligations of Article 15 of the UK GDPR (Data Subjects' Right of Access to their personal Data), in relation to images/footage captured by the CCTV System. All Subject Access Requests involving CCTV images should be made in writing to Data.Protection@nclt.ac.uk.

- 5.4 Where the Trust receives a request for the release of images and there is a lawful basis, under the UK Data Protection Laws, to sharing the personal data, it will disclose the images. The process set out in Appendix B will be followed when considering requests.
- 5.5 The Trust will record the reason for the sharing of the data on its central records.
- 5.6 The Trust will in most cases avoid disclosing physical images. Where an approval is given by the Central Services Data Protection Team, still images should only be shared via a secure O365 share using encrypted files.
- 5.7 On the receipt of a request from the Police and other agencies, NCLT may be able to release information under Schedule 2, Part 1 of the Data Protection Act (DPA) 2018. The police and other agencies do not have an automatic right of access to the information. The Act states public bodies may assess the merits of requests and decide whether or not to apply the exemption (not to inform the data subject of the release of their personal information). Requests must be made from the police/the agency on their specific document and signed by a senior police officer/suitably designated official.
- 5.8 Where CCTV information/image request involves a member of NCLT staff, the Central Services Data Protection Team will ensure these are treated with the highest level of privacy ensuring that the number of staff involved in the process is minimised.

6.0 Operation of CCTV Systems

- 6.1 The CCTV System will be administered and managed by each of the Principals/ Headteachers and their authorised users. The Central Services Data Protection Team will monitor the use of the CCTV *Internal Access Form* in regard to the principles and objectives expressed in this policy.
- 6.2 The day-to-day management of each Establishment's system will be the responsibility of the Headteacher's/ Principal's authorised users.
- 6.3 The CCTV system will be operated 24 hours each day, every day of the year.
- 6.4 The Site Supervisor/Caretaker will check and confirm the efficiency of the system on a twice-weekly basis to ensure the equipment is recording properly and cameras are functional.
- 6.5 Each establishment will keep a list of the Authorised Users. Further information about users can be requested via Data.Protection@nclt.ac.uk
- 6.6 The Trust will not conduct any covert surveillance using the CCTV System, unless instructed or requested to do so by the Police or other competent authority, as defined by the ICO. Where a request is made, it must be authorised by a member of the Central Services Data Protection Team and recorded on the NCLT CCTV External Request Form.
- 6.7 All Trust receptions have a static monitors for the active monitoring of external cameras. These static monitors do not permit the movement/adjustment of the cameras. These monitors may cover:

- Car park entrance/exit barriers
- Main building entrance doors (via intercom)

6.8 Active monitoring of further areas will only take place at Trust sites where there is limited staff supervision of students. Active monitoring is only carried out by staff authorised by the Headteacher/Principal. All active monitoring is only conducted on static monitors.

7.0 Images, Storage and Retention

7.1 In order to maintain and preserve the integrity of the data, all images captured using the CCTV System is stored securely within the site to which the cameras operate. Access to the storage is limited to a small number of authorised staff.

7.2 All captured images are stored on secure hard drives, which have restricted user access. The system will hold the recordings for a maximum period of 60 days before being automatically deleted. Any data downloaded from the system should be stored in the Trust shared IT area by authorised users. Each site will have their own folder so they can only store and access the footage from only their site and on others sites in the Trust. The data in this area is backed up on a regular basis. Once the data has been processed or shared as part of a request, it should be deleted from all areas.

7.3 When downloading CCTV images, users will ensure the files are clearly marked for storage using an agreed format, which ensures they can be easily identified.

7.4 CCTV Request Forms used for the purposes outlined in section 5 of this policy, will be stored for a maximum of 2 years from the date of the request.

7.5 The Trust will keep an electronic record of the release of data to the Police or other permitted requestors.

8.0 Breach of this Policy (including breaches of security)

8.1 Any breach of this policy by Trust staff will be investigated in line with Trust policy which could result in appropriate disciplinary action.

9.0 Assessment of the CCTV System

9.1 The CCTV system is maintained by the Trust approved contractor(s) providing periodic performance and maintenance checks and ad hoc works required.

9.2 Performance monitoring, including random operating checks, may be carried out by the Central Services Data Protection Team.

10.0 Complaints

10.1 Any complaints about the Trusts' CCTV system should follow the Trust Complaints Policy available on the New Collaborative Learning Trust Website.

Appendix A – Request Forms

CCTV Form – Internal Access

<https://forms.office.com/e/bZVhX0ELzk>

External CCTV Request Form – see Appendix B

<https://forms.office.com/e/SPRzqzr62g>

Appendix B

NCLT CCTV – Request for the Release of images to a third-party

The timeframes below are given as a guide only, as some requests may be more detailed and complex than others, resulting in the process being longer than expected. We will aim to complete the process as efficiently as possible.

Step 1 – External Request Submission

The Central Services Data Protection Team will receive a notification by email or the external form that data is requesting to be shared.

Any external person or company requiring access will complete the CCTV external form on the NCLT website.

Step 2 – Request Verification

The identity of the applicant will be verified by the Central Services Data Protection Team before proceeding.

Step 3 – Request Determination

The Central Services Data Protection Team will review the contents and determine the application.

If the request is denied, the reasons will be given to the applicant.

If the application is approved only the a minimal amount of data may be shared. The faces/identity of any third parties which cannot be lawfully disclosed must be redacted or cut out.
(Support with this may be required from IT/Marketing/Data Protection staff)

The Authorised user must then share the information securely, in the agreed format.

THE RELEASE OF FOOTAGE OR STILL IMAGES, INCLUDING PRINTED OR ELECTRONIC FORMAT, IS PROHIBITED UNLESS AUTHORISED BY CENTRAL SERVICES DATA PROTECTION TEAM.

Requests which from part of a Subject Access Request (SAR) under Data Protection Laws have a strict timescale of 30 days to complete. In most cases the Trust DPM will be involved at the start of this process with respect to a SAR and will provide a guide to the timescales involved. If anyone has any queries related to SAR's please contact the Trust DPM/DPO immediately.

Equality Impact Assessment (EIA)

The completion of this document is a requirement for all existing and proposed New Collaborative Learning Trust (NCLT) policies, major procedures, practices and plans (hereafter referred to as policies) as well as whenever looking at policy updates.

The Equality Act 2010 sets out our legal duty to undertake equality analysis of all trust/college policies. Completion of this EIA is the first step in meeting this duty. Please send the completed EIA (together with a copy of the related policy/draft policy document) to the Trust Director for Human Resources who will review the document and may refer to the Equality and Diversity Committee as necessary to advise on any follow up action that might be required.

Completion of the Equality Impact Assessment is part of the Specific Equality Duties (SED) required of the trust. Over arching the specific duties is the General Equality Duty (GED) required of everyone. Please bear the GED and SED in mind when undertaking this audit.

General Equality Duty

- Eliminate unlawful discrimination, harassment and victimisation and other conduct prohibited by the Act.
- Advance equality of opportunity between people who share a protected characteristic and those who do not.
- Foster good relations between people who share a protected characteristic and those who do not.

Specific Equality Duties Relevant to EIA are to provide:

- Sufficient information to demonstrate compliance with the general duties; including effects policies have on people.
- Evidence that analysis of this information has been undertaken.
- Details of information considered during analysis.
- Details of engagement (consultation) that has taken place.

Protected Characteristics are:

- | | |
|------------------------------|----------------------|
| • Age | • Race |
| • Disability | • Religion or Belief |
| • Gender Reassignment | • Sex |
| • Marriage/Civil Partnership | • Sexual Orientation |
| • Pregnancy/Maternity Leave | |

Audit Prompt	Response
Name of policy	CCTV Policy
Author of document:	Richard Wheatcroft
Responsible Senior Manager:	Richard Wheatcroft

below, or how you have arrived at the view that there are not negative impacts in relation to these characteristics: Age Disability Gender Reassignment Marriage/Civil Partnership Pregnancy/Maternity Leave Race Religion or Belief Sex Sexual Orientation	There should be no negative impacts on the identified characteristics as the processes involved are consistent. If an individual requires support to access our services/respond to requests for information this will be provided consistent with Equality law. This could involve completing an enquiry form on their behalf.
Is the policy free from discrimination on the grounds of: • Additional Learning Needs • Economic Needs • Social Needs	Yes
Please indicate who the policy has been considered by and/or who has been consulted about the policy. Where applicable include: • Staff/student consultative groups • Trade unions • Equality and Diversity, Health and Safety and Safeguarding Committee • Other committees/working groups (specify) • Senior Management Team • Trust Executive Team • Board of Directors • External group / Advisory group (specify)	The trust executive will review the policy Key trust leaders/managers have been involved in the creation of the process. Through the process of request access to the system there is a single point of contact the Data Privacy manager who will ensure requests are consistently approved or rejected based on consistent criteria. The Data Privacy Manager will refer to the Data Protection Officer where 'Special circumstances' requests are made or a request needs further consideration.
Can you identify any further consultations that might be necessary to ensure no adverse impact? If yes, please specify.	No
	No

Can you identify any differential or adverse impact the policy might have that is not already recorded? If yes, please specify.	
How would you assess the overall impact of this policy on equality? Please circle.	High / Medium / <u>Low</u>
Please record who this audit has been completed by (if by committee/work group please indicate and get lead person to sign off):	Name : Richard Wheatcroft Job Title : Chief Operating Officer Date : December 2024