CCTV Policy

Version 2

This policy applies to all NCLT institutions.

CONTENTS

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 and all corresponding documentation follows the guidelines of the UK General Data Protection Regulation (UK GDPR) as informed by the Data Protection Act 2018, as well as advice and guidance of the Information Commissioner's Office (ICO).

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 The CCTV system is owned by NCLT with a small number of external cameras at Wingfield academy being owned by EQUANS. External companies 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:

- **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.
- **The Act** - The Data Protection Act 2018 which controls how personal information is used by organisations, businesses or the government.
- **UK GDPR** - The UK General Data Protection Regulation 2018, tailored by the Data Protection Act 2018. The UK GDPR and all applicable laws relating to the collection and use of personal data and privacy and any applicable codes of practice issued by a regulator.
- **ICO** - Information Commissioner's Office.
- **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).
- **DPM** - Data Privacy Manager, the Trust appointed manager who oversees and manages all areas of policy and data protection related guidance and support and acts as the main point of contact for data subjects and the Information Commissioner's Office (ICO).
- **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.
- **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.
- **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.

- **Data controller** - A controller determines the purposes and means of processing personal data. In most cases, the Trust would identify itself as the data controller.
- **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.
- **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.
- **Third party** - means a natural or legal person, public authority, agency or body other than the data subject or controller.
- **Scheme -** the provisions, equipment and documents which are installed or used as part of the Trust's CCTV system.
- **Images** – still images or video footage.
- **Trust Authorised User** – This will be users who can access the CCTV system on their site. The Data Privacy Manager will maintain this list liaising with the Principal on each site to confirm each user.

3.0 Purpose of CCTV

3.1 The systems at each site comprises a number of fixed and dome cameras located internally and externally around the site. All cameras at our Trust sites are monitored from within the site to which they belong. At our Wingfield site, cameras can be viewed on site and can also be viewed by the Trust's preferred monitoring company.

3.2 The Trust has taken the measure of installing CCTV 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.**

3.3 Any person wishing to enquire about the use of NCLT CCTV systems, outside of the above mentioned purposes, should use the electronic form available on the NCLT Trust website.

3.4 The system does not include the capability to record sound.

4.0 Statement of Intent

4.1 The Scheme is registered with the Information Commissioner under the terms of the UK GDPR and will seek to comply with the requirements both of the Act and the ICO's Code of Practice.

4.2 The Trust will treat the Scheme and all information, documents and recordings obtained and used, as data which is protected by the Act.

4.3 Cameras will be used to monitor activities within the Trust sites and its car parks and other public areas to identify criminal activity actually occurring, anticipated, or perceived, and for the purpose of securing the safety and well being of all Trust staff and students, together with its visitors.

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, their property or a specific group of individuals, without senior authorisation being obtained. 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 Materials or knowledge secured as a result of CCTV 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 The planning and design has endeavoured to ensure that the Scheme will give maximum effectiveness and efficiency but it is not possible to guarantee that the system will cover or detect every single incident taking place in the areas of coverage.

4.8 Warning signs, as required by the Code of Practice of the Information Commissioner, have been placed at all access routes to areas covered by the Trust CCTV.

4.9 The Principal/Headteacher reserves the right to request direct access if footage is required to safeguard students or staff. The approval form will be completed as soon as possible after access to ensure all access to the system is clearly audited.

5.0 CCTV Image Requests

5.1 The Trust is committed to ensuring that any images which are captured through the Scheme, are only used for the purposes outlined in this policy.

5.2 Any use of CCTV images or footage will be subject to regular analysis by the Trust, using the NCLT CCTV Request Form in Appendix A. The form will help to identify the reason for the request, who is making the request, the date/time the request refers to and the date the system was accessed. This will ensure the Trust are only providing access in line with the reasons outlined in 3.2 of this policy. The form in Appendix A will advise the further steps in 5.3 if data is planned to be shared outside the organisation.

5.3 Where a request is made to access the data stored within the Scheme, the NCLT CCTV Request Process should be followed **at all times**. See Appendix B. If the access involves the downloading and/or sharing of still images, please refer to 5.6.

5.4 The Trust is committed to meeting the obligations of Article 15 of the UK GDPR and the Act, in respect of providing access to images or footage captured by the Scheme, as part of any Subject Access Request by a data subject. All Subject Access Requests involving CCTV images should be made in writing to the Trust DPM via Data.Protection@nclt.ac.uk. For further information regarding how the Trust deals with Subject Access Requests, please refer to the NCLT Data Protection Policy.

5.5 In some circumstances, at the discretion of the most senior member of staff on site at the time of a request, images may be shared with other third parties such as insurance companies, neighbouring businesses, for purposes other than those stated above in section 3.2. In these circumstances images will normally be released where satisfactory documentary evidence is produced showing that they are required for legal proceedings or in response to a Court Order. In any such case, the Trust will record the reason for the sharing of the data on its central records, along with the name of the authorising senior staff member. In the vast majority of cases senior members of staff will liaise with the DPO or DPM to seek advice on release.

5.6 The Trust will in most cases restrict the printing of any still images. Where an approved request by the DPM is made to download still images, these should only be shared via electronic format such as email, USB storage device or via an online cloud based storage. All sharing of data should be done via encrypted processing. NCLT Authorised Users are required to ensure encryption is used.

5.7 Requests by the Police can only be actioned under section 29 of the Data Protection Act 2018 and should be recorded on the force specific document and signed by a senior police officer.

5.8 Where CCTV request involves a member of staff the DPM will ensure these are treated with the highest level of privacy ensuring that the number of staff used in the process is minimised.

6.0 Operation of the System

6.1 The Scheme will be administered and managed by each of the Principals/Headteachers and the Authorised Users. The DPM will have oversight and approve the system usage requests in accordance with the principles and objectives expressed in this policy.

6.2 The day-to-day management of the system will be the responsibility of the authorised users on site during the day.

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 and in particular that the equipment is properly recording and that cameras are functional.

6.5 Additional access to the CCTV facilities will be granted to a small number of authorised individuals in the performance of their day to day duties. The additional users will have limited access. The DPM will keep a list of the Authorised Users for each Trust site. Further information about users can be requested via Data.Protection@nclt.ac.uk

6.6 Emergency procedures will be used in appropriate cases to call the Emergency Services.

6.7 The Trust will not conduct any covert surveillance using the Scheme, 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 the DPM and recorded on Section 4 of the NCLT CCTV Request Form, which is then recorded centrally by the DPM.

6.8 Active monitoring will only take place in areas of Trust sites where there is limited staff supervision. Active monitoring is only carried out by staff who have been given authority to do so as part of their role, by the Principal or Headteacher of any Trust site. All active monitoring is only conducted on static monitors which restricts the user's ability to record or capture any images. The DPM will maintain a list of staff who can carry out active monitoring.

6.9 All Trust receptions have monitors installed which allows active monitoring of external cameras, the monitors do not allow for the operation of the cameras, these may cover

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

7.0 Footage Storage and Retention

7.1 In order to maintain and preserve the integrity of the data, all data captured using the Scheme is stored securely within the site to which the cameras operate. Access to the storage is limited to a small number of authorised staff. The DPM will maintain a list of staff who have access to this storage.

7.2 All data captured through the scheme is stored in 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 CCTV 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 on site 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 authorised applicants. A copy of this record can be requested via email to Data.Protection@nclt.ac.uk

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 Scheme

9.1 The Scheme is maintained by the Trust approved maintenance contractor with annual performance checks carried out as part of the contract and ad hoc works carried out when required.

9.2 Performance monitoring, including random operating checks, may be carried out by the Trust DPO or DPM.

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

Internal CCTV Request Form

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

External CCTV Request Form

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

Appendix B

NCLT CCTV Request Process

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 – Request Submission

Any request to view or access NCLT CCTV content, should be made in the first instance by completing the appropriate request form.

Internal Request – The form will advise the person within the Trust to contact data.protection@nclt.ac.uk if any data is planned to be shared outside the organisation.

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

External signage on the Trust sites will share an initial point of contact on site. When contact is made they will be sent the link to the CCTV external form.

Step 2 – Request Verification

The Data Privacy Manager will receive a notification through email or the external form that data is requesting to be shared.

The Data Privacy Manager will review the contents and approve or reject the application.

If the request for use is under special circumstances, then the Data Privacy Manager will refer the request to the Data Protection Officer for approval.

In some circumstances the request may require additional verification to ensure the data can be accessed in line with the NCLT policy and/or Data Protection legislation. In this instance the authorised user will provide details of the request to the Trust Data Privacy Manager for authorisation.

If the request is denied, then reasons for this decision will be shared

Step 3 – Access Granted

Once the request has been verified the Authorised user must ensure that any images which are to be shared are not excessive and only contain a minimal amount of data. They must also ensure that any faces of third parties not involved in the request, are either 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.

PLEASE NOTE THE SUPPLYING OF STILL IMAGES IN PRINTED FORMAT, IS PROHIBITED UNLESS AUTHORISED BY SLT OR THE TRUST DPM/DPO.

Requests which from part of a Subject Access Request (SAR) under UK GDPR, 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.

Any requests from 'competent authorities' require additional recording, further advice on dealing with this type of request should be requested by contacting the DPM/DPO.

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

Audit Prompt	Response
Name of policy	CCTV Policy
Author of document:	Andy Woodcock and Andy Dye
Responsible Senior Manager:	Andy Woodcock

Briefly describe the aims, objectives and purpose of the policy.	To ensure the CCTV cameras are effectively used in the Trust and there is a clear process for requests for access and sharing of footage.
Who does the policy apply to: • Staff • Learners (please indicate which groups) • Members of the general public (please specify)	All the three areas covered in the bullet points. This policy governs the use of CCTV which include the site perimeters.
Will the policy affect members of the target audience equally? If no, please indicate the specific groups targeted by the policy. In targeting the policy at a specific group of people will members of other groups be disadvantaged? If yes, how will this be addressed? What information has been gathered about the diversity of the target audience? Attach details of information considered. How has this diversity been taken into account in writing the policy?	Yes No The target audience will be all staff, learners and member of the general public who are recorded on the CCTV systems in the Trust. The policy is written to ensure that there is no change in process to request of use of the system or how the CCTV system is administered. If surveillance was requested in special circumstances this will be considered on a case by case basis by the trust data protection officer. We are not expecting these requests to happen but have ensured that these are planned for in the policy.
Does this policy contain visual images? If yes, are these technical or cultural in nature? If cultural, do they reflect diversity? If yes, please indicate how.	No
Please indicate how this policy supports the trust/college in its General Equality Duty to: • Eliminate unlawful discrimination, harassment and victimisation (A). • Advance equality of opportunity between people who share a protected characteristic and those who do not (B). • Foster good relations between people who share a protected characteristic and those who do not (C).	Ensure that there are clear processes that ensure consistency of operations and requests for access across the trust.
Please indicate any negative impacts identified in relation to the protected characteristics listed	

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 a person's disability may hinder them completing the form online the contact details for the data privacy manager are available to support. This could involve completing the 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 / **Low**
Please record who this audit has been completed by (if by committee/work group please indicate and get lead person to sign off):	Name : Andy Woodcock Job Title : Chief Operating Officer Date : 09.03.2024