DATA PROTECTION & INFORMATION SYSTEMS

LEARNING TOGETHER
CORNWALL EDUCATION LEARNING TRUST

CCTV Policy

Author: Deputy Trust Lead
\Adopted by (body): Full Board Trustees

Collaborate	Ability to work effectively as a team
Empower	Ability to take initiative and problem solve in order to improve performance
Lead	To lead by example and achieve shared goals
Transformation	Ability to recognise a need for change and adapt accordingly

CELT Vision

Our vision is for our trust to be a learning organisation in the truest sense.

At the heart of our vision for education is a self-improving school-led system which has the best evidence-led practice and in which every child fulfils their potential. This is a learning community in which:

- Our leaders are driven by moral purpose. They are outwards focused and not afraid to take risks to achieve system transformation. The focus of policy is on continually improving the quality of teaching.
- Our teachers strive to be outstanding. They work across organisational boundaries to promote a collective sharing of knowledge, skills, expertise and experience in order to deepen pupil learning.
- The individual talents and strengths of our pupils are recognised and nurtured. A passion and curiosity for learning is sustained in every child from the moment they join us. A CELT pupil leaves our family of academies with a purpose, and the confidence to fulfil that purpose.
- Our parents are engaged in our learning community and actively work in partnership with us to raise the level of attainment and aspiration of every child.

CELT Mission

"Learning together to help every child achieve more."

We believe there is no limit to what every child can achieve, and that every child deserves the chance to fulfil their potential.

As a learning community we are on an ambitious journey. We want to deliver a model for education in the 21st century which instils curiosity and a love for learning in every child so that they develop into young adults who contribute to humanity, follow their passions, and think for themselves.

By learning and improving together – as part of a global learning community – we create much richer and more sustainable opportunities for rigorous transformation than can be provided by any one of our academies alone.

COLLABORATE
EMPOWER
LEAD
TRANSFORM

Should you require further information, please contact
The Governance Officer.
Cornwall Education Learning Trust (CELT), Atlantic Centre,
Trenance Leisure Park, Newquay, Cornwall TR7 2LZ

Telephone: 01637 800293 Email: ccarter@gov.celtrust.org
www.celtrust.org

Contents

Introduction	4
About this policy	5
Definition of data protection terms	6
The Data Protection Principles	7
and Privacy by Design	7
Responsibilities of the Trust	8
Responsibilities of the Data Protection Officer	9
Responsibilities of the headteacher	9
Purpose and justification	10
How Cornwall Education Learning Trust manages CCTV and surveillance	11
Security	12
Covert monitoring	13
Storage and retention of images	13
Subject Access Requests (SARs)	14
Access to and disclosure to other third parties	15
Complaints	15
History of Changes	15

1 Introduction

1.1. At Cornwall Education Learning Trust we take our responsibility towards the safety of staff, visitors and pupils very seriously. To that end, we use surveillance cameras to monitor any instances of aggression or physical damage to our Trust and its members.

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

- We comply with the 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 and their rights are being upheld.

1.3 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:

- Ensuring the security of our site
- Ensuring the safety of our staff, pupils and visitors
- Taking action to prevent a crime
- Using images of individuals that could affect their privacy

2 About this policy

2.1 This policy has been created with regard to the following statutory and non- statutory guidance:

- Home Office (2013) 'The Surveillance Camera Code of Practice'
- Information Commissioner's Office (ICO) (2014) 'CCTV Code of Practice'

2.2 This policy has due regard to legislation including, but not limited to, the following:

- The General Data Protection Regulation 2016
- The Data Protection Act 2018
- The Freedom of Information Act 2000
- The Protection of Freedoms Act 2012
- The Regulation of Investigatory Powers Act 2000

2.3 This policy operates in connection with the following Trust policies:

- Data Protection and Freedom of Information Policy

It also compliments local academy policies as should IT Acceptable Use.

3 Definition of data protection terms

3.1 For the purpose of this policy a set of definitions will be outlined, in accordance with the Surveillance Camera Code of Practice:

- CCTV – Closed Circuit Television is a system of cameras which stream an image to a central monitor, where activity can be recorded.

- Surveillance – monitoring the movements and behaviour of individuals; through CCTV.

- Overt surveillance – any use of surveillance for which authority 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.

Cornwall Education Learning Trust does not condone the use of covert surveillance when monitoring staff, pupils and/or volunteers.
Covert surveillance will only be operable in extreme circumstances.

4 The Data Protection Principles and Privacy by Design

4.1 Data collected from surveillance and CCTV will be:

1. Processed lawfully, fairly and in a transparent manner in relation to individuals.
2. Collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes.
3. Adequate, relevant, and limited to what is necessary in relation to the purposes for which they are processed.
4. Accurate and, where necessary, kept up to date.
5. Kept for no longer than is necessary for the purposes for which the personal data are processed.
6. 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.

4.2 The Trust will follow the ICO's guidelines on Privacy by Design – before planning installing and using a surveillance system, the Trust will:

- Consider whether the Trust can fulfil its requirements through a less privacy-intrusive system that does not include surveillance and recording.
- Carry out a Data Privacy Impact Assessment (DPIA) to assess security risks and how the rights of individuals will be upheld.
- Where the Trust identifies a high risk to an individual's interests, and it cannot be overcome, the Trust will consult the ICO before they use CCTV, and the Trust will act on the ICO's advice.

5 Responsibilities of the Trust

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

This responsibility will be delegated to the Executive Team, and to designated school leads as appropriate.

5.3 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.

6 Responsibilities of the Data Protection

6.1 As a Trust we are data controllers in law and are required to appoint a Data Protection Officer. Our DPO is Clare Ridehalgh and can be contacted at dataprotection@celtrust.org

6.2 The DPO is responsible for ensuring compliance with the Data Protection legislation and with this policy. Their responsibilities are laid out in the Data Protection policy, but in relation to CCTV and surveillance they include:

- Ensuring that all data controllers at the Trust and its Academies handle and process surveillance and CCTV footage in accordance with the 6 data protection principles.
- Ensuring that surveillance and CCTV footage is obtained in line with legal requirements.
- Supporting the Trust to complete a Data Privacy Impact Assessment when installing or replacing cameras (see paragraph 4.2).
- Reviewing the effectiveness of the current CCTV system and making recommendations if appropriate.
- Ensuring that surveillance and CCTV footage is destroyed in line with legal requirements when it falls outside of its retention period.
- Informing data subjects of how their data captured in surveillance and CCTV footage will be used by the Trust, their rights for the data to be destroyed and the measures implemented by the Trust to protect individuals' personal information.

7 Responsibilities of the headteacher

7.1 The headteacher has the following responsibilities:

- Meeting with the DPO to decide where CCTV is needed to justify its means.
- Liaising 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 Trust is using surveillance fairly and lawfully.
- Communicating any changes to legislation to all members of staff.

8 Purpose and justification

8.1 The Trust will only use surveillance cameras for the safety and security of the Trust and its staff, pupils and visitors.

8.2 Surveillance will be used as a deterrent for violent behaviour and damage to the Trust.

8.3 The Trust may share surveillance footage to assist the police in identifying persons who have committed an offence (see paragraph 13.1).

8.4 The Trust will only conduct surveillance as a deterrent and will not site cameras in general classrooms or any changing facility.

8.5 The Trust may place cameras in more specialist learning spaces, for example IT Suites, to ensure that those specialist areas are more closely monitored to ensure safe and appropriate use, and issues of misuse or vandalism are traceable.

8.6 The Trust may use surveillance data as part of disciplinary and grievance processes. This will be communicated to students and staff through the Trust Privacy Notices.

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

9 How Cornwall Education Learning Trust manages CCTV and surveillance

9.1 The Trust is registered as a data controller with the Information Commissioner's Office, which also covers the use of surveillance systems.

9.2 CCTV warning signs are clearly and prominently placed at all external entrances to Trust sites, including gates if coverage includes outdoor areas. The signs contain details of the purpose for using CCTV e.g. public safety or crime prevention.

9.3 In areas where CCTV is used, the Trust will ensure that there are prominent signs placed at both the entrance of the CCTV zone and within the controlled area.

9.4 The surveillance system is a closed digital system will not record audio by default, as audio recording may be considered an excessive intrusion of privacy.

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

9.6 The surveillance system will not be focused on individuals unless an immediate response to an incident is required.

9.7 The surveillance system will not be focused on private vehicles or property outside the perimeter of the Trust sites.

10 Security

10.1 Access to the surveillance system, software and data is strictly limited to authorised Trust staff and is password protected.

10.2 The Trust's authorised CCTV system users are:

- The Data Protection Officer, or local Data Protection Leads
- Headteachers (or delegates on the leadership teams)
- Designated Safeguarding Leads and Deputies
- IT Staff
- Estates Staff

10.3 Visual display of the CCTV systems across our Trust varies slightly depending upon their local site. The 'back end' systems (dedicated CCTV recording systems, or networked storage solutions) will be secured and only accessible by those above titled staff to keep the systems working.

Viewing of systems will often be available away from these secured back-end systems via software or web-based platform. The use of those systems will only be undertaken by the above titled staff, or at their direct request.
On occasion it may be necessary to request additional staff to view footage alongside the above titled staff to aid in identifying individuals as part of an investigation into behaviour or vandalism etc.

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

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

10.6 The headteacher and authorised staff will decide when to record footage, e.g. a continuous loop outside the grounds to deter intruders.

10.7 Any unnecessary footage captured will be securely deleted from the system. This will often be on a rotational basis (e.g. recordings on to a system which allows footage to automatically overwrite after a determined amount of days)

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

11 Covert monitoring

11.1 While the Trust does not condone the general or day to day use of covert recording, the Trust may, in exceptional circumstances, set up covert monitoring. For example:

- Where there is good cause to suspect that an illegal or unauthorised action(s), is taking place, or where there are grounds to suspect serious misconduct.
- Where notifying the individuals about the monitoring would seriously prejudice the reason for making the recording.

11.2 In these circumstances authorisation must be obtained from the Data Protection Officer.

11.3 Covert monitoring must cease following completion of an investigation.

11.4 Cameras sited for the purpose of covert monitoring will not be used in areas which are reasonably expected to be private, for example toilets.

11.5 The Human Rights and Employment Rights of all the people who use the Trust must be respected and covert monitoring must only be used as a last resort.

12 Storage and retention of images

12.1 Recorded data will not be retained for longer than is necessary. While retained, the integrity of the recordings will be maintained to ensure their evidential value and to protect the rights of the people whose images have been recorded.

12.2 The CCTV images will be kept for 30 days (in line with the purpose for recording this data) unless there is a current incident that is being investigated.

12.4 All retained data will be stored securely and will be listed on the Trust 's Data Asset Audit.

12.5 All retained data must be stored in a searchable system. Only a primary copy should be kept, and secondary copies should only be created in exceptional circumstances.

13 Subject Access Requests (SARs)

13.1 Individuals have the right to request access to video footage relating to themselves under the Data Protection Act 2018.

13.2 All requests should be made to the Headteacher or the Data Protection Officer. 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. Requests may be written or verbal.

13.3 The Trust will immediately indicate receipt and then respond within one calendar month of receiving the request.

13.4 The Trust reserves the right to refuse access to video footage where this would prejudice the legal rights of other individuals or jeopardise an ongoing investigation.

13.5 All attempts will be made to allow the viewing of the video. If others can be identified, the Trust will assess the risk to others from the video being viewed by the requester. If there is likely to be a risk of harm, the Trust may consider the following options where appropriate:

- Obtain the consent of others to share the video with the requester.
- Use video-editing software to blur the faces of others who can be identified from the video.
- Provide selected still images from the video and blur the identifiable faces.
- Provide a transcript or written description of the contents of the video.

13.6 If all options have been considered and the Trust still consider there to be a risk to others from the requester viewing the video, the Trust may decline the request to view the video (although relevant exemptions in the Data Protection Act 2018 will need to be identified by the Trust provided to the requester).

13.7 The Trust should not provide copies of the video to others unless instructed to do so in law or there is no risk to individuals who may be identifiable from the video.

14 Access to and disclosure to other third parties

14.1 There will be no disclosure of recorded data to third parties other than to authorised personnel such as the Police and service providers to the Trust where these would reasonably need access to the data (e.g. investigators) and with the correct authorisation.

14.2 Requests from third parties should be made in writing to the Headteacher or the Data Protection Officer. However, consideration must also be given to the following paragraph (14.3)

14.3 Consideration should always be given to the safeguarding and best interest of pupils. Data Protection should not be used as an excuse to prevent the viewing of images if there is an overwhelming need. All disclosures and the reasons for release should be recorded.

14.4 The data may be used within the Trust 's discipline and grievance procedures as required and will be subject to the usual confidentiality requirements of those procedures. This will be communicated to staff through the Trust Privacy Notices.

15 Complaints

15.1 Complaints and enquiries about the operation of CCTV within the Trust should be directed to the Headteacher or the Data Protection Officer in the first instance.

Review
This policy will be reviewed every two years.

Appendix History of Changes

Version	Author(s)	Date Produced	Amendments	Origin of Change
1.0	MW	April 2021		