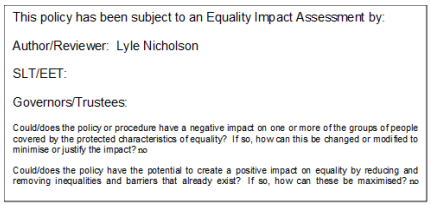
Surveillance Policy


This policy has been subject to an Equality Impact Assessment by:

Author/Reviewer: Lyle Nicholson

SLT/EET:

Governors/Trustees:

Could/does the policy or procedure have a negative impact on one or more of the groups of people covered by the protected characteristics of equality? If so, how can this be changed or modified to minimise or justify the impact? no

Could/does the policy have the potential to create a positive impact on equality by reducing and removing inequalities and barriers that already exist? If so, how can these be maximised? no

Introduction

This policy is concerned with the use and governance of surveillance technology, and the processing of Personal Data which has been collected by using surveillance technology. The policy is written in accordance with various Data Protection legislation, which includes but is not limited to the General Data Protection Regulation (GDPR) and the Data Protection Act 2018 (DPA), and the Information Commissioner's Office's (ICO) surveillance code of practice.

Queries about this policy should be directed to the Tees Valley Collaborative Trust's (the Trust) Data Protection Officer (Veritau Ltd SchoolsDPO@veritau.co.uk)

Scope

This policy applies to all Trust employees (both those employed directly by the Trust and those employed on behalf of the Trust by a local authority (or other such body), any authorised agents working on behalf of the Trust, including temporary or agency staff, governors, volunteers, and third party contractors.

This Policy will refer to all individuals within scope of the policy as 'employees'. Employees who are found to knowingly or recklessly infringe this policy may face disciplinary action.

Surveillance is the monitoring of behaviour, activities, or other changing information for the purpose of influencing, managing, directing, or protecting people. The Trust only uses surveillance in the context of CCTV and e-monitoring software.

The Trust does not operate covert surveillance technologies and therefore this policy does not cover the use of such technology.

CCTV

The purpose of the CCTV system is crime prevention and detection. This includes the apprehension and prosecution of offenders on the premises, ensuring security and safety of campus users, maintaining the security of the premises by preventing crime and enabling subsequent investigation.

Planning CCTV Systems

Any new implementation of CCTV systems will employ the concept of 'privacy by design' which will ensure that privacy implications to data subjects will be considered

before any new system is procured. The prescribed method for this is through the completion of a Data Protection Impact Assessment (DPIA).

The Trust has various statutory responsibilities to protect the privacy rights of data subjects. Therefore during this planning phase the Trust will consider:

i. The purpose of the system and any risks to the privacy of data subjects,

ii. That there are statutory requirements placed on the location and position of cameras. This means that cameras must be positioned to meet the requirement(s) of the intended purpose(s) and not exceed the intended purpose(s).

iii. The obligation to ensure that the CCTV system can meet its intended purpose(s) also means that the system specification must be such that it can pick up any details required for these aims. For example the system should record with sufficient resolution to perform its task.

iv. The system must also have a set retention period (one month) and, where appropriate, the Trust must also have the ability to delete this information prior than the set retention period in order to comply with the rights of data subjects.

v. That the Trust will need a level of access to the system and there will need to be the option to provide other agencies (such as law enforcement agencies) with specific footage if requested.

CCTV Privacy Notices

The processing of personal data requires that the individuals that the data relates to (in this case any individuals captured by the CCTV) are made aware of the processing. Therefore the use of CCTV systems must be visibly signed.
The signage must be clear enough that anyone entering the recorded area will be aware that they are being recorded.

Access to CCTV Recordings

CCTV footage will only be accessed to comply with the specified purpose. For example, if the purpose of maintaining a CCTV system is to prevent and detect crime then the footage must only be examined to investigate a criminal activity having taken place.

The CCTV system will have a nominated Information Asset Owner who will be responsible for the governance and security of the system. The Information Asset Owner will authorise officers to access CCTV footage either routinely or on an ad-hoc basis.

CCTV Footage Disclosures

A request by individuals for CCTV recordings that include footage of them should be regarded as a subject access request (SAR). For more information on the right of access for individuals captured on CCTV, refer to the Trust's Information Policy.

If the Trust receives a request from another agency (for example a law enforcement agency) for CCTV recordings, then it will confirm the following details with that agency:

i. the purpose of the request,

ii. that agency's lawful basis for processing the footage,

iii. confirmation that not receiving the information will prejudice their investigation,

iv. whether the Trust can inform the data subject of the disclosure, and if not, the reasons for not doing so.

The Trust will liaise with its appointed Data Protection Officer should it have any concerns about such requests.

Review of CCTV

CCTV systems must be reviewed biennially to ensure that systems still comply with Data Protection legislation and national standards. The Information Asset Owner should use the checklist included in Appendix 1 of this policy to complete this review. It is the responsibility of the Information Asser Owner to ensure reviews are completed and evidence of those reviews taking place are maintained.

Complaints

Complaints by individuals about the use of surveillance systems, or the way surveillance data is processed, should be treated as a data protection concern and the Trust's data protection officer should be made aware.

The Trust's Data Protection Officer is: SchoolsDPO@veritau.co.uk

Records of Processing

The Trust has a duty under Article 30 of the GDPR to ensure that all instances of data processing activity is recorded for regulatory inspection where required. The Trust maintains an information asset register in order to fulfil this requirement.

The Trust will ensure that the use of surveillance systems is recorded on their information asset register.

Related Documents

Employees who are responsible for planning, maintaining, or reviewing the implementation of a surveillance system are encouraged to read the following related documents prior to implementation:

- ICO Surveillance Code of Practice (External Link)
- The School's Data Protection Impact Assessment (DPIA) Template (available through Veritau)

Date of Last Approval/Revision	New policy
Review interval (years)	3 yearly
Responsible Officer	Director of Resources
Approval/review body	Executive Team
Date of next review	September 2024
Public File location	Tees Valley Collaborative Trust Sharepoint/ Websites/Staff Handbook

Appendix 1 – CCTV System Checklist

Tees Valley Collaborative Trust

Name and Description of Surveillance System:		
The purpose and requirements of the system are addressed by the system (i.e the cameras record the required information)	**YES**	**NO**
	Notes:	
The system is still fit for purpose and produces clear images of adequate resolution.	**YES**	**NO**
	Notes:	
Cameras are sited in effective positions to fulfil their task.	**YES**	**NO**
	Notes:	
Cameras are positioned so that they avoid capturing the images of persons not visiting the premises and/or neighbouring properties.	**YES**	**NO**
	Notes: One camera at PPC records the gate area. Some houses are close enough that their owners and visitors are recorded. Students pass these houses on arrival.	
There are visible signs showing that CCTV is in operation. These signs include: ▪ Who operates the CCTV, ▪ Their contact details, ▪ What the purpose of the CCTV is.	**YES**	**NO**
	Notes: New signage has been produced; deployment underway.	
CCTV recordings are securely stored and access limited.	**YES**	**NO**
	Notes: Recordings are only available to IT administrators and Site Services staff.	
The system has the	**YES**	**NO**

capability to transfer recordings to law enforcement or to fulfil a request for an individual's own personal information.	**Notes: Recordings can be exported to external drives when required.**	
The system has a set retention period. This retention period should only be long enough to fulfil the CCTV's purpose and not longer. Outside of this retention period information should be deleted	**YES**	**NO**
	Notes: 30 days is the recording limit. We may overwrite data before this period, but recordings over 30 days are automatically removed.	
The system users should be able to selectively delete information still inside the retention period to fulfil the right to erasure.	**YES**	**NO**
	Notes: There's no way to delete footage inside the retention period without deleting everything.	
All operators have been authorised by the Information Asset Owner and have sat their mandatory data protection training.	**YES**	**NO**
	Notes: Data protection training has been delivered several times. Further training is available to all users in KnowBe4	
This system has been declared on the corporate register of surveillance systems.	**YES**	**NO**
	Notes:	

Checklist Completed By: Name: Mark Russon Job Title: IT Manager Date: 12/02/2021	**Checklist Reviewed and Signed By (Information Asset Owner):** Name: Job Title: Date: