Adopted:	July 2020
Next review:	July 2022
Approved by:	NSAT Trust Board
Responsibility of:	Data & Compliance Director

Northern Star Academies Trust Surveillance and CCTV Policy

Contents

1. Statement of Intent

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 Northern Star Academies Trust Data & Compliance Director or Data Protection Officer.

2. Scope

This policy applies to all pupils, Trust employees, any authorised agents working on behalf of the Trust, including temporary or agency staff, governors, volunteers, and third-party contractors and any other individual visiting an NSAT site.

Surveillance is the monitoring of behaviour, activities, or other changing information for the purpose of influencing, managing, directing, or protecting people. The Trust 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.

3. CCTV Purpose

The Trust and schools within the Trust may operate 'Closed Circuit Television' (CCTV) systems for the following purposes: -

- For the safety and security of the school and its pupils, staff, visitors, volunteers, governors, trustees and any other individual visiting a Trust site;
- To protect the school buildings and assets;
- To assist in reducing the fear of crime and for the protection of private property;
- To assist in the prevention of crime and assist law enforcement agencies in apprehending offenders;
- To assist in the investigation of accidents, incidents and near misses

4. 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. During the planning phase the Trust and School will consider:

- The purpose of the system and any risks to the privacy of data subjects.
- 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).
- 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 must record with sufficient resolution to perform its task.

- The system must also have a set retention period. The Trust has the ability to delete this information prior to the set retention period in order to comply with the rights of data subjects.
- 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. If a data subject is captured and recorded by the system, then that individual also has the right to request a copy of that footage under subject access provisions.

The school will ensure that a contract will be agreed between the Trust (as Data Controller) and the CCTV system provider. Consideration should also be given as to whether there are any joint data controller arrangements where the system is shared with another organisation. Data Processing clauses must be included within the written contract if the provider will be processing (e.g. monitoring, storing, accessing) the data on behalf of the school.

5. CCTV Privacy Notices

The processing of personal data requires that the individuals 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 will include the purpose for the system (e.g. the prevention or detection of crime), the details of the organisation operating the system and who to contact about the system (including basic contact details). The signage must be clear enough that anyone entering the recorded area will be aware that they are being recorded.

A more detailed Privacy Notice for the use of CCTV must be maintained with the intention of informing data subjects of their rights in relation to surveillance data. This will be available on the school (if applicable) and Trust websites.

6. Access to CCTV Recordings

CCTV footage will only be accessed to comply with the specified purpose and the footage will only be examined to meet one of the purposes described above.

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.

7. CCTV Footage Disclosures

A request by individuals for CCTV recordings that include footage of them is 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:

- the purpose of the request,
- that agency's lawful basis for processing the footage,
- confirmation that not receiving the information will prejudice their investigation,
- 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.

8. Review of CCTV

CCTV systems should be reviewed within the same timeline for the Information Security Policy 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.

9. E-Safety Monitoring

The Trust or School within the Trust may operate e-safety monitoring software systems in order to safeguard pupils and inform IT staff when any pupil searches for or looks at inappropriate or malicious content. Software is also used to ensure pupils are “on task” within lessons. This is considered to be a form of non-covert surveillance processing. Harrogate High School uses AB Tutor to monitor pupils within lessons and a Smoothwall firewall that monitors and reports on internet searches and activity when online. The use of E-Safety Monitoring software is included in the Privacy Notice for the school where relevant.

10. Planning E-Monitoring Systems

Any new implementation of 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:

- The purpose of the system and any risks to the privacy of data subjects,
- The system must be installed in a way which meets the requirement(s) of the intended purpose(s) and not exceed the intended purpose(s).
- The obligation to ensure that the 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.
- The system must also have a set retention period and, where appropriate, the Trust or school 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.
- That the Trust or school 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 system data if requested. If a data subject’s activity is captured and recorded by the system, then that individual also has the right to request a copy of that data under subject access provisions.
- The Trust of school will ensure that a contract will be agreed with the system provider. Consideration should also be given as to whether there are any joint data controller arrangements where the system is shared with another organisation. Data Processing clauses must be included within the written contract if the provider will be processing (e.g. monitoring, storing, accessing) the data on behalf of the Trust or school.

11.System Privacy Notices

The processing of personal data requires that the individuals that the data relates to (in this case any individuals whose activity is recorded by the system) are made aware of the processing. Therefore, the use of monitoring systems must be visibly signed.

A more detailed Privacy Notice for the use of the system will be maintained with the intention of informing data subjects of their rights in relation to surveillance data.

12.Access to Systems Data

System data will only be accessed to comply with the specified purpose. For example, if the purpose of maintaining the monitoring system is to safeguard children then the data must only be examined where there is evidence to a child is at risk.

The 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 the system data either routinely or on an ad-hoc basis.

13.Monitoring Data Disclosures

A request by individuals for system data that includes their activity should be regarded as a subject access request (SAR). For more information on the right of access for individuals refer to the Trust's Information Policy.

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

- the purpose of the request,
- that agency's lawful basis for processing the data,
- confirmation that not receiving the data will prejudice their investigation,
- whether the school 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.

14.Review of Systems

Systems must be reviewed in line with the Information Policy 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.

15.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 school's data protection officer should be made aware.

The Trust's Data Protection Officer is:

Schools Data Protection Officer
Veritau Ltd
County Hall
Racecourse Lane
Northallerton
DL7 8AL
schoolsDPO@veritau.co.uk

16. Records of Processing

The school 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 school maintains an information asset register in order to fulfil this requirement.

The school will ensure that the use of surveillance systems is recorded on their information asset register. This should detail each separate surveillance system in use.

17. 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 Trust's Data Protection Impact Assessment (DPIA) Template (available through Veritau)

Appendix 1 – Surveillance System Checklist

School Name:

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:	
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:	
CCTV recordings are securely stored and access limited.	**YES**	**NO**
	Notes:	

The system has the capability to transfer recordings to law enforcement or to fulfil a request for an individual's own personal information.	**YES**	**NO**
	Notes:	
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:	
The system users should be able to selectively delete information still inside the retention period to fulfil the right to erasure.	**YES**	**NO**
	Notes:	
All operators have been authorised by the Information Asset Owner and have sat their mandatory data protection training.	**YES**	**NO**
	Notes:	
This system has been declared on the corporate register of surveillance systems.	**YES**	**NO**
	Notes:	

Checklist Completed by: Name: Job Title: Date:	**Checklist Reviewed and Signed by (Information Asset Owner):** Name: Job Title: Date: