



NMAT SURVEILLANCE POLICY (Non-Statutory)

Approved by:	NMAT Board of Trustees	Date: October 2023
Last reviewed on:	October 2023	
Next review due by:	October 2025	
Responsible	Executive Principal	

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 UK General Data Protection Regulation (UK GDPR) and the Data Protection Act 2018 (DPA), and the Information Commissioner's Office's (ICO) surveillance code of practice.

UK GDPR queries about this policy should be directed to the Trust's Governance Professional and Compliance Lead or queries about the use of surveillance in NMAT academies should be directed to the Trust's Chief Operating Officer.

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; However, should the need arise for the use of covert surveillance in the future all appropriate requirements will be followed).

CCTV

The Trust operates 'Closed Circuit Television' (CCTV) systems in order to:

- (a) prevent crime and protect buildings and assets from damage, disruption, vandalism and other crime;
- (b) ensure the personal safety of staff, students, visitors and other members of the public and to act as a deterrent against crime;
- (c) support law enforcement bodies in the prevention, detection and prosecution of crime;
- (d) assist in day-to-day management, including ensuring the health and safety of staff, students and others; and
- (e) assist in the effective resolution of disputes which arise in the course of student behavioural or expulsion action or in the course of staff disciplinary or grievance proceedings.

This policy will be kept under regular review in light of legal developments and best practice.

Planning CCTV Systems Any new implementation of CCTV systems will employ the concept of ‘privacy by design and default’ 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, where practicable, the system must record with sufficient resolution to perform its task.
- iv. The system must also have a set retention period (the typical retention period is 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 ‘properly’ 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 Trust 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 Trust. This role is performed by the IT Network Manager in NMAT academies.

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 will include the purpose for the system (e.g. the prevention or detection of crime and monitoring of the ‘behaviour policy’), the details of the organisation operating the system and who to

This policy will be kept under regular review in light of legal developments and best practice.

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.

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 where there is evidence to suggest 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 employees 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 Data Protection 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.
- Appropriate authorisation from the Line Manager than the one requesting the recording, or if this is not possible, the Head of School.

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 annually 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.

E-Safety Monitoring

This policy will be kept under regular review in light of legal developments and best practice.

The Trust operates 'e-safety monitoring software systems in order to (prevent misuse of systems and to ensure system users are compliant with the Acceptable Use Policy (AUP). This is considered to be a form of non-covert surveillance processing. The Trust uses Smoothwall as a web filter and security device, together with ABTutor (Nunthorpe) for teaching staff to monitor what students have on screen.

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:

GDPR Sentry Limited
Unit 434 Birch Park
Thorp Arch Estate
Wetherby
West Yorkshire
LS23 7FG



Tel: 0113 8042035
info@gdprsentry.com

To contact the DPO, emails can also be sent via the Trust Governance Lead by emailing S. Javed-Sarwar on sjaved-sarwar@nunthorpe.co.uk

Records of Processing

The Trust has a duty under Article 30 of the UK 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. This should detail each separate surveillance system in use.

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) available through HR.

This policy will be kept under regular review in light of legal developments and best practice.