OFFICIAL POLICY FOR

CCTV Policy (Statutory)

POLICY STATEMENT

THIS POLICY SETS OUT HOW NUNTHORPE MULTI-ACADEMY TRUST LIMITED ("WE", "OUR", "US") USES CCTV AND OTHER SURVEILLANCE SYSTEMS AT OUR SITES.

We believe that CCTV and other surveillance systems have a legitimate role to play in helping to maintain a safe and secure environment for all our staff, students and visitors. However, we recognise that this may raise concerns about the effect on individuals and their privacy and as such this Policy is intended to address such concerns. Any images recorded by surveillance systems are Personal Data, which must be Processed in accordance with data protection laws, including the General Data Protection Regulation ((EU) 2016/679) ("**GDPR**"). We are committed to complying with our legal obligations and ensuring that the legal rights of Data Subjects are recognised and respected.

This policy is intended to assist staff in complying with their own legal obligations when working with Personal Data. In certain circumstances, misuse of information generated by CCTV or other surveillance systems could constitute a criminal offence.

1. DEFINITIONS

For the purposes of this CCTV Policy, the following terms have the following meanings:

CCTV means fixed and domed cameras designed to capture and record images of individuals and property.

Data is information which is stored electronically or in certain paper-based filing systems and may include Personal Data. In respect of CCTV, this generally means video images. It may also include static pictures such as printed screen shots.

Data Controllers means the person or organisation that determines when, why and how to process Personal Data. We are the Data Controller of all Personal Data used in multi-academy trust for our own commercial and educational purposes.

Data Processors means the person or organisation that is not a Data User that Processes Personal Data on our behalf and in accordance with our instructions (for example, a supplier which handles Personal Data on our behalf).

Data Users are those of our employees whose work involves Processing Personal Data. This will include those whose duties are to operate CCTV cameras and other surveillance systems to record, monitor, store, retrieve and delete images. Data users must protect the data they handle in accordance with this Policy and our Privacy Standard and Privacy Policy.

Data Subjects means a living, identified or identifiable individual about whom we hold Personal Data as a result of the operation of our CCTV (or other surveillance systems).

Personal Data means any information identifying a Data Subject or information relating to a Data Subject that we can identify (directly or indirectly) from that data alone or in combination with other identifiers we possess or can reasonably access. This will include video images of Data Subjects.

Processing means any activity that involves the use of Personal Data. It includes obtaining, recording or holding the 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 transmitting or transferring Personal Data to third parties.

Surveillance systems means any devices or systems designed to monitor or record images of individuals or information relating to individuals. The term includes CCTV systems as well as any technology that may be introduced in the future such as automatic number plate recognition (ANPR), body worn cameras, unmanned aerial systems and any other systems that capture information of identifiable individuals or information relating to identifiable individuals.

2. ABOUT THIS POLICY

We currently use CCTV cameras to view and record individuals in and around the public areas of our sites. This Policy outlines why we use CCTV, how we will use CCTV and how we will process Personal Data recorded by CCTV cameras to ensure we are compliant with data protection law and best practice. This policy also explains how to make a subject access request in respect of personal data created by CCTV.

We are committed to complying with all our legal obligations under the GDPR. The images of individuals recorded by CCTV cameras in the workplace are Personal Data and therefore subject to the GDPR. We are a Data Controller and we have registered our use of CCTV with the Information Commissioner. We also seek to comply with best practice suggestions from the Information Commissioner's Office (**ICO**) (including its code of conduct for surveillance cameras and personal information (2017 Version 1.3)), as they may be updated or otherwise amended from time to time.

This Policy covers all employees, workers, contractors, agency workers, consultants, directors, members, governors, trustees, past or present students and may also be relevant to visiting members of the public.

This Policy is non-contractual and does not form part of the terms and conditions of any employment or other contract. We may amend this Policy at any time without consultation. The Policy will be regularly reviewed to ensure that it meets legal requirements, relevant guidance published by the ICO and industry standards.

A breach of this Policy may, in appropriate circumstances, be treated as a disciplinary matter. Following investigation, a breach of this Policy may be regarded as misconduct leading to disciplinary action, up to and including dismissal.

3. PERSONNEL RESPONSIBLE

The Executive Principal has overall responsibility for ensuring compliance with relevant legislation and the effective operation of this Policy. Day-to-day management responsibility for deciding what information is recorded, how it will be used and to whom it may be disclosed has been delegated to the Director of Finance & Operations. Day-to-day operational responsibility for CCTV cameras and the storage of data recorded is the responsibility of individual academy IT Team Managers.

4. REASONS FOR THE USE OF CCTV

We currently use CCTV in and around the public areas of our sites as outlined below. We believe that such use is necessary for legitimate business purposes, including:

(a) to prevent crime and protect buildings and assets from damage, disruption, vandalism and other crime;

(b) for the personal safety of staff, students, visitors and other members of the public and to act as a deterrent against crime;

(c) to support law enforcement bodies in the prevention, detection and prosecution of crime;

(d) to assist in day-to-day management, including ensuring the health and safety of staff, students and others; and

(e) to 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 list is not exhaustive and other purposes may be or become relevant.

5. MONITORING

CCTV monitors the main entrance, some external areas and internal public areas 24 hours a day and this data is continuously recorded.

Camera locations are chosen to minimise viewing of spaces not relevant to the legitimate purpose of the monitoring. As far as practically possible, CCTV cameras will not focus on private homes, gardens or other areas of private property.

Staff using surveillance systems will be given appropriate training to ensure they understand and observe the legal requirements related to the processing of relevant Personal Data.

6. HOW WE WILL OPERATE ANY CCTV

Where CCTV cameras are placed in the workplace (such as classrooms and staffrooms), we will ensure that signs are displayed at the entrance of the surveillance zone to alert individuals that their image may be recorded. Such signs will contain details of the purpose for using the surveillance system and who to contact for further information, where these things are not obvious to those being monitored.

We will ensure that live feeds from cameras and recorded images are only viewed by approved members of staff whose role requires them to have access to such Personal Data. This may include HR staff involved with disciplinary or grievance matters. Recorded images will only be viewed in designated, secure offices.

7. USE OF DATA GATHERED BY CCTV

In order to ensure that the rights of individuals recorded by the CCTV system are protected, we will ensure that Personal Data gathered from CCTV cameras is stored in a way that maintains its integrity and security. This may include encrypting the Personal Data, where it is possible to do so.

Given the large amount of Data generated by surveillance systems, we may store video footage using a cloud computing system. We will take all reasonable steps to ensure that any cloud service provider maintains the security of our information, in accordance with data protection laws (including GDPR) and industry standards.

We may engage Data Processors to process Personal Data on our behalf. We will ensure that there are contractual safeguards in place to protect the security and integrity of the Personal Data.

8. RETENTION AND ERASURE OF DATA GATHERED BY CCTV

Data recorded by the CCTV system may be stored digitally using a cloud computing system. This will then be overwritten (or otherwise erased permanently and securely) four weeks after recording. However, where images are

being recorded for crime prevention purposes, Data may be kept long enough only for incidents to come to light. We will maintain a comprehensive log of when Data is deleted.

At the end of their useful life, any physical matter such as tapes or discs will be disposed of as confidential waste. Any still photographs and hard copy prints will be disposed of as confidential waste.

9. USE OF ADDITIONAL SURVEILLANCE SYSTEMS

Prior to introducing any new surveillance system, including placing a new CCTV camera in any workplace location, we will carefully consider if they are appropriate by carrying out a data privacy impact assessment (**DPIA**).

A DPIA is intended to assist us in deciding whether new surveillance cameras are necessary and proportionate in the circumstances and whether they should be used at all or whether any limitations should be placed on their use.

Any DPIA will consider the nature of the problem that we are seeking to address at that time and whether the surveillance camera is likely to be an effective solution, or whether a better solution exists. In particular, we will consider the effect a surveillance camera will have on individuals and therefore whether its use is a proportionate response to the problem identified.

No surveillance cameras will be placed in areas where there is an expectation of privacy (for example, in changing rooms or bathrooms) unless, in very exceptional circumstances, it is judged by us to be necessary to deal with very serious concerns.

10. COVERT MONITORING

We will never engage in covert monitoring or surveillance (that is, where individuals are unaware that the monitoring or surveillance is taking place) unless, in highly exceptional circumstances, there are reasonable grounds to suspect that criminal activity or extremely serious malpractice is taking place and, after suitable consideration, we reasonably believe there is no less intrusive way to tackle the issue.

In the unlikely event that covert monitoring is considered to be justified, it will only be carried out with the express authorisation of the Executive Principal. The decision to carry out covert monitoring will be fully documented and will set out how the decision to use covert means was reached and by whom. The risk of intrusion on innocent workers and students will always be a primary consideration in reaching any such decision.

Only limited numbers of people will be involved in any covert monitoring.

Covert monitoring will only be carried out for a limited and reasonable period of time consistent with the objectives of making the recording and will only relate to the specific suspected illegal or unauthorised activity.

11. ONGOING REVIEW OF CCTV USE

We will ensure that the ongoing use of existing CCTV cameras is reviewed at least every 12 months to ensure that their use remains necessary and appropriate, and that any surveillance system is continuing to address the needs that justified its introduction.

12. REQUESTS FOR DISCLOSURE

We may share Personal Data with other academies in our trust where we consider that this is reasonably necessary for any of the legitimate purposes set out above in paragraph 5.

No images from our CCTV cameras will be disclosed to any other third party, without express permission being given by the Head of School and our review of our associated obligations under the GDPR. Personal Data will not normally be released unless satisfactory evidence that it is required for legal proceedings or under a court order has been produced.

In other appropriate circumstances, we may allow law enforcement agencies to view or remove CCTV footage where this is required in the detection or prosecution of crime.

We will maintain a record of all disclosures of CCTV footage.

No images from CCTV will ever be posted online or disclosed to the media.

13. SUBJECT ACCESS REQUESTS

Data Subjects may make a request for disclosure of their Personal Data and this may include CCTV images (**data subject access request**). A data subject access request is subject to the statutory conditions from time to time in place and should be made in writing, in accordance with our Privacy Standard and Privacy Policy.

In order for us to locate relevant footage, any requests for copies of recorded CCTV images must include the date and time of the recording, the location where the footage was captured and, if necessary, information identifying the individual.

We reserve the right to obscure images of third parties when disclosing CCTV data as part of a subject access request, where we consider it necessary to do so.

14. COMPLAINTS

Any questions about this policy or any concerns about our use of CCTV should be forwarded to Nunthorpe Multi Academy Trust's (NMAT) Complaints Manager in the first instance.

Where this is not appropriate or matters cannot be resolved informally, our formal grievance procedure should be followed.

15. REQUESTS TO PREVENT PROCESSING

We recognise that Data Subjects may wish to exercise their right to object to Processing and their right to erasure of Personal Data. For further information regarding this, please contact the NMATs Complaints Manager.