CCTV policy

June 2018

Published date: June 2018	Next review deadline: June 2020	Statutory	Executive Lead at ATT: Andy Gannon, Head of Corporate Affairs

Associated documents:	
Links to:	
• Data protection policy	

Our Vision – Transforming education: Transforming performance: Transforming lives

Putting children and young people at the heart of all that we do.

We will ensure that all our children and young people, regardless of their background, fulfil their educational potential. We will do this in safe, supportive and ambitious environments, ensuring we maximise life chances for them all.

Our values

- We will work inclusively within our communities, embracing the varied localities we serve while sharing our common vision and values.

- We will develop the very best leaders of the future, working to improve education and transform lives.

- We will adhere unwaveringly to the 'Nolan Principles' of Public Service, which is made clear in our commitment to Ethical Leadership.

Contents

Note

This policy may be used by any Academy in relation to any CCTV system operated by them. A key element in the assessment of lawful use of CCTV systems is the privacy impact assessment (PIA) conducted in relation to those systems setting out the justification for the system and its compliance with data protection legislation. If the Academy has not conducted such an assessment then this must be conducted now, and this template policy amended to take account of the outcome of that assessment. The Academy should do this with an open mind, including considering whether any existing cameras should be removed or the system modified in any way.

1 Policy Statement

1.1 The Nicholas Hamond Academy uses Close Circuit Television ("CCTV") within the premises of the Academy. The purpose of this policy is to set out the position of the Academy as to the management, operation and use of the CCTV at the Academy.

1.2 This policy applies to all members of our Workforce, visitors to the Academy premises and all other persons whose images may be captured by the CCTV system.

1.3 This policy takes account of all applicable legislation and guidance, including:

1.3.1 General Data Protection Regulation ("GDPR")

1.3.2 Data Protection Act 2018 (together the Data Protection Legislation)

1.3.3 CCTV Code of Practice produced by the Information Commissioner

1.3.4 Human Rights Act 1998

1.4 This policy sets out the position of the Academy in relation to its use of CCTV.

2 Purpose of CCTV

2.1 The Academy uses CCTV for the following purposes:

2.1.1 To provide a safe and secure environment for pupils, staff and visitors

2.1.2 To prevent the loss of or damage to the Academy buildings and/or assets

2.1.3 To assist in the prevention of crime and assist law enforcement agencies in apprehending offenders

3 Description of system

3.1 The installation is an Internet Protocol (IP), Power over Ethernet (PoE) system based on 42 x 4 megapixel Infra-Red (IR) internal dome cameras and 40 x 4 megapixel Infra-Red external dome cameras. Two 64 channel network Video Recorders (NVRs) provide the recording platform with internal data storage capacity to provide a 30 day archive. The NVRs have sufficient capacity to extend the system with additional cameras at a later date should current operational requirements change. The system has been installed on a totally separate network in order to eliminate any additional data strain on the academy's network.

4 Siting of Cameras

4.1 All CCTV cameras will be sited in such a way as to meet the purpose for which the CCTV is operated. Cameras will be sited in prominent positions where they are clearly visible to staff, pupils and visitors.

4.2 Cameras will not be sited, so far as possible, in such a way as to record areas that are not intended to be the subject of surveillance. The Academy will make all reasonable efforts to ensure that areas outside of the Academy premises are not recorded.

4.3 Signs will be erected to inform individuals that they are in an area within which CCTV is in operation.

4.4 Cameras will not be sited in areas where individual have a heightened expectation of privacy, such as changing rooms or toilets. Cameras are sited in ICT suites for security or equipment and safeguarding.

5 Privacy Impact Assessment

5.1 Prior to the installation of any CCTV camera, or system, a privacy impact assessment will be conducted by the Academy to ensure that the proposed installation is compliant with legislation and ICO guidance.

5.2 The Academy will adopt a privacy by design approach when installing new cameras and systems, taking into account the purpose of each camera so as to avoid recording and storing excessive amounts of personal data.

6 Management and Access

6.1 The CCTV system will be managed by the Regional Estates Manager.

6.2 On a day to day basis the CCTV system will be operated by the IT Manager and Site Supervisors.

6.3 The viewing of live CCTV images will be restricted to the IT Manager and Site Supervisors.

6.4 Recorded images which are stored by the CCTV system will be restricted to access by individual staff who request footage, authorising member of senior staff, the IT manager & Site Supervisors.

6.5 No other individual will have the right to view or access any CCTV images unless in accordance with the terms of this policy as to disclosure of images.

6.6 The CCTV system is checked monthly by the IT Manager and Site Supervisors to ensure that it is operating effectively

7 Storage and Retention of Images

7.1 Any images recorded by the CCTV system will be retained only for as long as necessary for the purpose for which they were originally recorded.

7.2 Recorded images are stored only for a period of 30 days unless there is a specific purpose for which they are retained for a longer period.

7.3 The Academy will ensure that appropriate security measures are in place to prevent the unlawful or inadvertent disclosure of any recorded images. The measures in place include:

7.3.1 CCTV recording systems being located in restricted access areas;

7.3.2 The CCTV system being encrypted/password protected;

7.3.3 Restriction of the ability to make copies to specified members of staff

7.4 A log of any access to the CCTV images, including time and dates of access, and a record of the individual accessing the images, will be maintained by the Academy.

[Unless the CCTV records a specific incident then it is unlikely to be justifiable to retain any recorded images for more than, say, 28 days.]

8 Disclosure of Images to Data Subjects

8.1 Any individual recorded in any CCTV image is a data subject for the purposes of the Data Protection Legislation, and has a right to request access to those images.

8.2 Any individual who requests access to images of themselves will be considered to have made a subject access request pursuant to the Data Protection Legislation. Such a request should be considered in the context of Academy Transformation Trust's Subject Access Request Policy.

8.3 When such a request is made the IT Manager and Site Supervisors will review the CCTV footage, in respect of relevant time periods where appropriate, in accordance with the request.

8.4 If the footage contains only the individual making the request then the individual may be permitted to view the footage. This must be strictly limited to that footage which contains only images of the individual making the request. The It manager and Site Supervisors must take appropriate measures to ensure that the footage is restricted in this way.

8.5 If the footage contains images of other individuals then the Academy must consider whether:

8.5.1 The request requires the disclosure of the images of individuals other than the requester, for example whether the images can be distorted so as not to identify other individuals;

8.5.2 The other individuals in the footage have consented to the disclosure of the images, or their consent could be obtained; or

8.5.3 If not, then whether it is otherwise reasonable in the circumstances to disclose those images to the individual making the request.

8.6 A record must be kept, and held securely, of all disclosures which sets out:

8.6.1 When the request was made;

8.6.2 The process followed by the IT Manager and Site Supervisors in determining whether the images contained third parties;

8.6.3 The considerations as to whether to allow access to those images;

8.6.4 The individuals that were permitted to view the images and when; and

8.6.5 Whether a copy of the images was provided, and if so to whom, when and in what format.

[Please note that when a subject access request is made then, unless an exemption applies (such as in relation to third party data that it would be unreasonable to disclose) then the requester is entitled to a copy in a permanent form. We have referred only to "access" as opposed to a "permanent copy" as the Academy may consider it preferable in certain circumstances to seek to allow access to images by viewing in the first instance without providing copies of images. If an individual agrees to viewing the images only then a permanent copy does not need to be provided. However if a permanent copy is requested then this should be provided unless to do so is not possible or would involve disproportionate effort.]

9 Disclosure of Images to Third Parties

9.1 The Academy will only disclose recorded CCTV images to third parties where it is permitted to do so in accordance with the Data Protection Legislation.

9.2 CCTV images will only be disclosed to law enforcement agencies in line with the purposes for which the CCTV system is in place.

9.3 If a request is received form a law enforcement agency for disclosure of CCTV images then the IT Manager and Site Supervisors must follow the same process as above in relation to subject access requests. Detail should be obtained from the law enforcement agency as to exactly what they want the CCTV images for, and any particular individuals of concern. This will then enable proper consideration to be given to what should be disclosed, and the potential disclosure of any third party images.

9.4 The information above must be recorded in relation to any disclosure.

9.5 If an order is granted by a Court for disclosure of CCTV images then this should be complied with. However very careful consideration must be given to exactly what the Court order requires. If there are any concerns as to disclosure then the Data Protection Officer should be contacted in the first instance and appropriate legal advice may be required.

10 Review of Policy and CCTV System

10.1 This policy will be reviewed every two years.

10.2 The CCTV system and the privacy impact assessment relating to it will be reviewed annually.

[The privacy impact assessment (PIA) relating to the system should be reviewed regularly to ensure that the use of any CCTV system continues to be justified and is compliant with legal requirements. The Academy should ensure that it has procedures in place to ensure that the CCTV system is regularly reviewed.]

11 Misuse of CCTV systems

11.1 The misuse of CCTV system could constitute a criminal offence.

11.2 Any member of staff who breaches this policy may be subject to disciplinary action.

12 Complaints relating to this policy

12.1 Any complaints relating to this policy or to the CCTV system operated by the Academy should be made in accordance with the Academy Complaints Policy.

CCTV PRIVACY IMPACT ASSESSMENT TEMPLATE

1 Who will be captured on CCTV?

[Pupils, staff, parents / carers, volunteers, Governors and other visitors including members of the public etc]

2 What personal data will be processed?

[Facial Images, behaviour, sound, etc]

3 What are the purposes for operating the CCTV system? Set out the problem that the Academy is seeking to address and why the CCTV is the best solution and the matter cannot be addressed by way of less intrusive means.

[Prevention or detection of crime etc]

4 What is the lawful basis for operating the CCTV system?

[Legal Obligation, legitimate interests of the organisation to maintain health and safety and to prevent and investigate crime]

5 Who is/are the named person(s) responsible for the operation of the system?

The IT Manager and Site Supervisors

6 Describe the CCTV system, including:

a. how this has been chosen to ensure that clear images are produced so that the images can be used for the purpose for which they are obtained;

b. siting of the cameras and why such locations were chosen;

c. how cameras have been sited to avoid capturing images which are not necessary for the purposes of the CCTV system;

d. where signs notifying individuals that CCTV is in operation are located and why those locations were chosen; and

e. whether the system enables third party data to be redacted, for example via blurring of details of third party individuals.

The system in place is suitable for its purpose. Cameras are sited in appropriate positions to allow for the best coverage of are4as bearing in mind sensitive /public areas. Signs are in position at the main entrance and exits to the site.

7 Set out the details of any sharing with third parties, including processors

All footage is stores locally to the academy site and shared with the appropriate Law Agencies if requested (following subject access procedure)

8 Set out the retention period of any recordings, including why those periods have been chosen

30 day archive being adequate time to obtain any footage required

9 Set out the security measures in place to ensure that recordings are captured and stored securely

Storage server is located in a secure room with limited access, electronic access is limited to selected named staff

10 What are the risks to the rights and freedoms of individuals who may be captured on the CCTV recordings?

For example: • Is it fair to record them in the way proposed? • How is the amount of data processed to be minimised? • What are the risks of the system being accessed unlawfully? • What are the potential data breach risks? • What are the risks during any transfer of recordings, or when disclosed to third parties such as the police?

11 What measures are in place to address the risks identified?

• Access to recorded footage is limited and predominately for safeguarding of all individuals • Data held for length of retention period only. Exported footage minimised as requests must contain a limited 'time frame' • Access to the system is password protected with regular updates, the system is physically secure and access is only available to limited named staff • Requests for footage must be authorised by a senior member of staff. Footage is then exported to a protected and secure area on the network. • Should any footage need to leave the site (Police request) then this is password protected.

12 Have parents and pupils where appropriate been consulted as to the use of the CCTV system? If so, what views were expressed and how have these been accounted for?

The Academy Trust & the academy considered the use of the system to be appropriate taking into account all the relevant security procedures in place.

13 When will this privacy impact assessment be reviewed?

June 2020

Approval:

This assessment was approved by the Data Protection Lead:

DPL Kate Winter

Date October 2019