CCTV Policy

Date Published	**June 2016**
Version	**2**
Last Approved Date	**23rd May 2018**
Review Cycle	**3 Years**
Review Date	**May 2021**

"Learning together; to be the best we can be"

1. Policy statement

1.1. Nexus Multi Academy Trust complies with the Data Protection Act 1998, General Data Protection Regulation (2018) and Information Commissioner's CCTV Code of Practice 2008 where it uses CCTV systems. This policy statement and the following guidance must be complied with at all times on all Nexus Multi Academy Trust premises including academies, residential homes, offices and depots.

1.2. Academy senior leaders must ensure that there is reasonable justification before CCTV is used.

1.3. The CCTV must not invade neighbours privacy when viewing perimeter fencing.

1.4. A designated person – typically the Headteacher or the school Business Manager/Officer - will have legal responsibility for each CCTV system.

1.5. The intended use of the CCTV will be documented and the system must not be used for anything other than this. For example, if the scheme is merely for site security (viewing perimeters) then images of individuals must not be taken.

1.6. The scheme must be notified to the Information Commissioners Office (ICO).

1.7. Each system must have procedures for administration, which will include:

- Ensuring notification on an annual basis;
- Ensuring the system is used in accordance with the notification;
- Procedures for handling images;
- Record keeping of access requests, use of images procedures and pro-active monitoring of the scheme to ensure compliance;
- Control of recorded material.

1.8. The CCTV system must be sited only to achieve what is documented in the scheme.

1.9. Permanent or movable cameras must not be used to view areas that are not of interest and not intended to be the subject of the scheme. There are areas where there is an expectation of heightened privacy and CCTV may only be used in very extreme cases and this must not be undertaken without correct notification to the ICO and the Headteacher or Business Manager.

1.10. The CCTV will only be used at relevant times.

1.11. The equipment used must be maintained to give reliable quality.

1.12. No sound recording technology is to be used.

1.13. Material must not be stored for longer than is necessary and must be deleted when no longer required.

1.14. Images must be viewed in a secure/restricted area with access only to authorised persons.

1.15. Images must not be released to third parties unless there is a lawful reason to do so (take advice from the Trust's legal advisors before sharing images).

1.16. Individuals who are recorded may request access to the images.

1.17. There must be adequate signage to let people know that surveillance is taking place. Where cameras are discreet, the notices must be more prominent. All staff working in buildings covered by CCTV must be made aware that images can be used for disciplinary purposes where necessary.

1.18. The CCTV systems must not be used to systematically monitor people. Authorisation under the Regulation of Investigatory Powers Act (RIPA) 2000 will be required if surveillance is to be used.

1.19. All staff who use the CCTV system must be trained and aware of this policy statement, the Data Protection Act 1998, the General Data Protection Regulation (2018) and the Information Commissioner's Office (ICO) CCTV Code of Practice.

2. Introduction

2.1. Closed Circuit Television (CCTV) is now a well-established and accepted practice in our lives. It is widely used in towns, shopping areas, hotels, schools and on the road networks. CCTV is generally supported by the public, but it does intrude into people's lives as they carry out their daily activities. This therefore means that responsible use, under guidelines, must be maintained to ensure that this 'intrusion' is legitimately carried out.

2.2. A code of practice for CCTV was issued in 2000 by the Information Commissioners Office (ICO) and this has since been replaced by the 2008 revised edition. The 2008 edition strengthens the 2000 code by taking into account the advancement of technology. The code is available at: www.ico.gov.uk/upload/documents/library/data_protection/detailed_specialist_guides/ico_cctvfinal_2301.pdf

2.3. The code has been developed to ensure operators of CCTV systems follow good practice guidelines and comply with the law, in particular the Data Protection Act 1998 (DPA). Information about individuals (including images) that is held by any organisation, including academies, is covered by the DPA. The DPA has a number of principles, which are legally enforceable and are briefly included within this document.

3. What is covered by the Code of Practice?

3.1. The 2008 code of practice covers CCTV systems which capture images of identifiable individuals, or information relating to individuals.

3.2. There are certain cases where the DPA is not applicable. These include:

- Householders who have CCTV for domestic use, e.g. to protect their properties.
- Images captured by individuals for personal (domestic) use on digital camera, mobile phones or camcorders.

3.3. Please note that any directed surveillance for law enforcement purposes is covered by the Regulation of Investigatory Powers Act (RIPA) 2000 and may require authorisation.

4. When to use CCTV

4.1. Prior to installing a CCTV system, which must comply with the DPA, you must consider whether it is necessary or whether there is an alternative solution. For example, if the CCTV is purely for security, improved fencing and lighting may be a better option and won't require compliance with the DPA.

4.2. The code requires organisations to conduct an assessment before installation, to establish the following:

- Who is legally responsible for the system?
- What will the system be used for and how will it benefit the organisation?
- Can other, less intrusive, alternatives be used, such as lighting or improved fencing?
- Does the scheme capture images of identifiable individuals?

4.3. The Information Commissioner's Office states that if you are establishing a large system or considering a use of CCTV which could give rise to significant privacy concerns you may wish to consider using its Privacy Impact Assessment handbook.
http://www.ico.gov.uk/upload/documents/pia_handbook_html_v2/index.html

4.4. CCTV is an established part of everyday life and a proven tool in the fight against bullying, vandalism, graffiti and theft. One of the most rapidly expanding areas of use is in the education sector. CCTV is often used for surveillance in schools to prevent crime.

4.5. Often, cameras are positioned to protect school premises and the general fabric of the building which helps to deter unwanted intruders from entering the academy's perimeter. This has been particularly useful during academy closures or holidays. Recently, there has been an increase in the use of CCTV not only for the purpose of protecting the academy but for the intention of monitoring pupils and staff for the purposes of health and safety.

4.6. Careful consideration should always be given to whether to use CCTV in the first instance; the fact that it is possible, affordable or has public support should not be the primary motivating factor. Academies should take into account what benefits can be gained and whether alternative solutions exist, and what effect it may have on individuals.

4.7. It would be strongly advisable to consult with staff, Local Governing Bodies, pupils and parents before installing any kind of CCTV system. It is recommended that the academy conducts a full consultation with all relevant parties. The consultation should include an explanation of all the purposes for which the CCTV cameras are being, or have been, installed and confirmation that they comply with the law as described in this policy.

4.8. Below is a list of common reasons why schools may consider installing CCTV:

- Improving safety for staff
- Tackle bullying
- Reduce damage by vandalism
- Tackle graffiti
- Reduce theft
- Deter the arsonist
- Prevent pupils carrying knives into school
- Eliminate boisterous activity in classrooms and general bad behaviour
- Prevent cheating in exams
- Improve safety and security during periods of extracurricular activity
- Protect the school and staff against malicious or ill-conceived compensation claims
- Use in staff disciplinary matters

4.9. If CCTV is to be used, privacy must be safeguarded by ensuring that cameras are not directed at areas where there is an expectation of privacy such as toilets / washrooms / changing rooms.

4.10. CCTV should always be used proportionally and with caution and where there are justifiable concerns that make it necessary for cameras to be fitted. Circumstances might be when persistent thefts have occurred or if it is suspected that persistent bullying is taking place. However, even in those circumstances, this should be time limited, proportional and all staff and pupils should be fully informed of the reason/s why the cameras are present.

4.11. Below is a list of situations where CCTV should not be used:

- Cameras should not be fitted in staff rooms unless required for security reasons when the rooms are not occupied. In this case, it should only be switched on during those periods.
- Schools must be careful not to include captured images of surrounding properties and gardens, as this will contravene data protection regulations.
- In no circumstances should CCTV be placed in such a way that it could capture images of pupils in areas where there is an expectation of privacy.

5. Legal Issues

5.1. CCTV images, videos and webcams of clearly identifiable people will be subject to the DPA and the Human Rights Act 1998 and must be dealt with in accordance with these Acts.

5.2. The Human Rights Act 1998 (HRA) gives individuals the right to respect for their private and family life, home and correspondence. The General Data Protection Regulation (2018) also enhances an individual's right to privacy and subject access request (where applicable). Public authorities may not interfere with this right except where necessary and in accordance with the law, in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others. In practice, this means that authorities can use CCTV but only after they have risk assessed the impact on others privacy, whether the scheme is necessary, and for what purpose the images will be used.

5.3. Principle 1 of the DPA requires that personal data is processed fairly and lawfully, i.e. that individuals are aware that images are being captured on CCTV, and of how that information will be used.

5.4. This means that signs, which are clearly visible and legible, should be displayed so that the public are aware they are entering an area where CCTV is in use. The signs should display details of the organisation responsible for the scheme, their contact details and the purpose of the CCTV system.

5.5. To ensure that images are only captured for the intended purpose of the scheme, the location of cameras must be carefully considered. The CCTV should be used only to monitor the intended spaces.

5.6. Owners and residents of domestic premises should be consulted if domestic premises border the intended area to be viewed.

5.7. Those operating the system must be fully trained, must be aware of what the scheme should be used for, and must only use the cameras and images for that purpose.

5.8. Principle 2 requires that personal data be obtained for a specific purpose. Therefore if you install CCTV for security purposes you would normally only use that information for that purpose and wouldn't use it, for example, for staff monitoring.

5.9. Principle 2 also requires an organisation to notify to the Information Commissioner the purposes they process data for. If you use a CCTV system which will obtain personal information (i.e. images of individuals), you must ensure that your notification to the ICO includes this.

5.10. Principle 3 of the DPA requires that personal data should be adequate, relevant and not excessive in relation to the purpose or purposes for which they are processed. This means that you should only collect the amount of data you need for the purpose the CCTV system has been installed for. You should collect no extra information and you need to ensure that the images will be adequate for their intended use.

5.11. Principle 4 of the DPA requires that information should be accurate and up to date. The quality of images must be maintained to ensure that data within them is accurate and adequate for the intended purpose. In order to achieve this:

- Equipment should be maintained, serviced and cleaned regularly to ensure it performs correctly and a maintenance log should be kept.
- Tapes (if used) / discs should be of good quality and should be updated when necessary.
- If the system records location of camera, date, time etc. these should be accurate.
- Cameras should be protected from vandalism or tampering.

5.12. Principle 5 of the DPA requires that information is held no longer than necessary for the intended purpose. Once a retention period has expired, images must be erased.

5.13. Principle 6 of the DPA gives individuals certain rights under the Act. Section 7 of the DPA gives individuals the right of access to any personal data an organisation holds about them. This includes CCTV images and they have a right to view those images or request a copy. If such a request is received in relation to the CCTV system, pass the details to the Headteacher.

5.14. Principle 7 of the DPA requires that information is held securely. Access to images, monitors and equipment should be by authorised staff only and copies of images should be stored securely.

6. Disclosure of CCTV Images

6.1. Access to, and the disclosure of, CCTV images and the disclosure of images to third parties should be restricted and carefully controlled to ensure the rights of individuals are protected.

6.2. All access should be documented (whether information is provided or refused), and disclosures must be limited to those allowed by law

6.3. There are some exemptions within the Data Protection Act which will allow images to be used for certain purposes: for example, in disciplinary matters or if a crime has been committed. However, you must take advice from the Trust's HR Advisor, or the Trust's legal advisor before disclosing information to third parties or to other organisations or before using information for other purposes.