



PRINCIPLES FOR USE OF CCTV AT LEARN@ ACADEMIES

**“ALL DIFFERENT,
ALL EQUAL,
ALL ACHIEVING TOGETHER”**

Sources:

<https://www.gov.uk/government/publications/surveillance-camera-code-of-practice>

https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/368115/Leaflet_v6_WEB.pdf

https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/409290/12_principles_diagram_v3.pdf

Introduction

In its use of Closed Circuit Television (CCTV) Learn@ MAT is committed to striking a balance between protecting all members of its school community – including pupils, staff, parents and carers, visitors and neighbours – whilst also protecting an individual's legitimate expectation of privacy, where the location must be considered along with the activity being recorded. For example, there is less entitlement to privacy where an individual's behaviour is seriously anti-social or even criminal.

Learn@ MAT has based its eleven principles for the use of CCTV at its Academies on principles set out in the Surveillance Camera Commissioner's Code of Practice. These principles will underpin the CCTV Policies of all Learn@ Academies.

Learn@ MAT Academies will not use CCTV to monitor staff, students or visitors without their knowledge unless:

- We suspect they're breaking the law
- Letting them know about it would make it hard to detect the crime.

Covert monitoring will always be a last resort. It will only take place as part of a specific investigation and it will stop when the investigation is over. Any proposal to carry out covert monitoring must be authorised by senior management. The Headteacher should normally obtain such authorisation from the Learn@ MAT CEO, and the CEO should normally inform the Academy Council and the Learn@ Trust Board before any covert monitoring begins.

Principles for use of Closed Circuit Television (CCTV) by Learn@ Academies

Learn@ MAT expects its Academies to adopt the following principles for the use of CCTV on their premises:

1. Use of a CCTV system must always be for a specified purpose, which is in pursuit of a legitimate aim and necessary to meet an identified, pressing need.
2. The use of a CCTV system must take into account its effect on individuals and their privacy, with regular reviews to ensure its use remains justified.
3. There must be as much transparency in the use of a CCTV system as possible, including a published contact point for access to information and complaints.
4. There must be clear responsibility and accountability for all CCTV system activities including images and information collected, held and used.

5. Clear rules, policies and procedures must be in place before a CCTV system is used, and these must be communicated to all who need to comply with them.
6. No more images and information should be stored than that which is strictly required for the stated purpose of a CCTV system, and such images and information should be deleted once their purposes have been discharged.
7. Access to retained images and information should be restricted and there must be clearly defined rules on who can gain access and for what purpose such access is granted; the disclosure of images and information should only take place when it is necessary for such a purpose or for law enforcement purposes.
8. CCTV operators should consider any approved operational, technical and competency standards relevant to a system and its purpose and work to meet and maintain those standards.
9. CCTV images and information should be subject to appropriate security measures to safeguard against unauthorised access and use.
10. There should be effective review and audit mechanisms to ensure legal requirements, policies and standards are complied with in practice, and regular reports should be published.
11. When the use of a CCTV system is in pursuit of a legitimate aim, and there is a pressing need for its use, it should then be used in the most effective way to support safety and law enforcement with the aim of processing images and information of evidential value.

Here are some questions to help our Learn@ Academies consider whether they comply with the principles for the use of CCTV on their premises:

Principle	
Use of a CCTV system must always be for a specified purpose, which is in pursuit of a legitimate aim and necessary to meet an identified, pressing need.	<p>What's your system for?</p> <p>Do you review its use?</p>
The use of a CCTV system must take into account its effect on individuals and their privacy, with regular reviews to ensure its use remains justified.	<p>Have you carried out a privacy impact assessment?</p> <p>Do you publish your privacy impact assessment?</p>
There must be as much transparency in the use of a CCTV system as possible, including a published contact point for access to information and complaints.	<p>Do you have signage in place to say a CCTV system is in use?</p> <p>Is there a published point of contact with which people can raise queries or complaints?</p>
There must be clear responsibility and accountability for all CCTV system activities including images and information collected, held and used.	<p>Who's responsible for your system?</p> <p>Are all staff aware of their responsibilities?</p>
Clear rules, policies and procedures must be in place before a CCTV system is used, and these must be communicated to all who need to comply with them.	<p>Do you have clear policies and procedures in place?</p> <p>Do your staff know what your policies and procedures are?</p>
No more images and information should be stored than that which is strictly required for the stated purpose of a CCTV system, and such images and information should be deleted once their purposes have been discharged.	<p>How long do you keep images/information?</p> <p>How do you make sure images/information is deleted once its no longer needed?</p>
Access to retained images and information should be restricted and there must be clearly defined rules on who can gain access and for what purpose such access is granted; the disclosure of images and information should only take place when it is necessary for such a purpose or for law enforcement purposes.	<p>Do you have a policy on who has access to the stored information?</p> <p>Do you have a policy on disclosure of information?</p>

<p>CCTV operators should consider any approved operational, technical and competency standards relevant to a system and its purpose and work to meet and maintain those standards.</p>	<p>Do you follow any recognised operational or technical standards?</p> <p>Who maintains your system?</p>
<p>CCTV images and information should be subject to appropriate security measures to safeguard against unauthorised access and use.</p>	<p>Do you make sure that the images captured by your system are recorded securely?</p> <p>Are only authorised people given access to the images?</p> <p>Who are the authorised people?</p> <p>Do all staff know the authorised people?</p>
<p>There should be effective review and audit mechanisms to ensure legal requirements, policies and standards are complied with in practice, and regular reports should be published.</p>	<p>Do you evaluate your system regularly to make sure it's still required?</p> <p>Could there be an alternative solution to a CCTV system?</p>
<p>When the use of a CCTV system is in pursuit of a legitimate aim, and there is a pressing need for its use, it should then be used in the most effective way to support safety and law enforcement with the aim of processing images and information of evidential value.</p>	<p>Can the criminal justice system use the images and information produced by your CCTV system?</p> <p>Do you have a policy on data storage, security and deletion?</p>

LEARN@ MAT CCTV PRIVACY IMPACT ASSESSMENT



Learn@ MAT Academies should carry out a documented privacy impact assessment before installing a new CCTV system or making significant changes to an existing CCTV system. They should consider the following when completing a Privacy Impact Assessment:

- What is the Academy's purpose for using CCTV images? What are the issues/problems it is meant to address?
- Is the system necessary to address a pressing need, such as staff and student safety or crime prevention?
- Are the CCTV cameras intended to operate on the outside of the premises only?
- Are external CCTV cameras justified under the circumstances?
- Are external CCTV cameras proportionate to the problem they are designed to deal with?
- Is it intended that CCTV cameras will operate inside the Academy buildings?
- Are internal CCTV cameras justified under the circumstances?
- Are internal CCTV cameras proportionate to the problem they are designed to deal with?
- What are the benefits to be gained from their use?
- Can CCTV systems realistically deliver these benefits? Can less privacy-intrusive solutions, such as improved lighting, achieve the same objectives?
- Does the Academy need images of identifiable individuals, or could the system use other images, which are not capable of identifying the individual?
- Will the proposed system deliver the desired benefits now and remain suitable in the future?
- What future demands may arise for wider use of images and how will they be addressed?
- Is the Academy the data controller for the entire CCTV? If not, is the Academy satisfied that the external contractor who operates the system complies with the Data Protection Acts with regard to the processing of images of staff, students and visitors to the Academy captured on any CCTV systems under its management?

- What are the views of those who will be under CCTV surveillance?
- What could be done to minimise intrusion for those whose images may be captured, particularly if specific concerns have been expressed?
- How have staff, students and visitors been assured by the Academy that they will not be routinely monitored and that the CCTV system will only be used for the stated purposes?
- Does the Academy's policy on the use of CCTV make it clear that staff (teaching and non-teaching) will not be monitored for performance or conduct purposes?
- Have the views of staff and students been taken into account regarding the location of cameras?
- Can the location of each internal camera be justified in accordance with the overall purpose for the use of the CCTV system?
- Has appropriate signage been put up at the location of each internal camera indicating that recording is taking place and outlining the purpose of such a recording?
- Who will have access to the system and CCTV footage?
- What security measures are in place to protect the CCTV system and recorded footage to ensure that no one can tamper with them?
- Are the people who will have authorised access to the system and recorded CCTV footage clear about their responsibilities?
- Are the camera monitors kept out of view of staff, students and visitors and is access to the camera monitors restricted to a limited number of staff on a 'need to know' basis?
- Is the room(s) which houses the camera monitors and the CCTV system securely locked when unattended?
- Does the Academy have a procedure in place to ensure that CCTV footage is erased or deleted as soon as the retention period (40 working days) has expired?
- Does the Academy have a procedure in place for handling requests for access to CCTV footage from the Police?
- Will appropriate notices be in place to ensure that individuals know that they are being monitored?
- Does the Academy have a data protection policy? Has it been updated to take account of the introduction of a CCTV system?
- Does the Academy have a procedure in place to handle access requests seeking a copy of footage recorded by the CCTV system (within the statutory timeframe of forty days)?
- Has the right of access been communicated to staff, students and visitors?
- Has the Academy communicated its policy on the use of CCTV to staff, students and visitors and how has this been done?
- How are new students and new staff informed of the Academy's policy on the use of CCTV?

Author	Andrea Wills	Date	November 2019
Approved	Audit Finance and Resources Committee	Review	Two year cycle or where there is a change to the law or circumstances
Last Updated	November 2019	Next Review	November 2021
Review Body	Audit Finance and Resources Committee	Status	Statutory