John Taylor MAT
CCTV Statement & Relevant Procedures

John Taylor Multi Academy Trust (JTMAT) is committed to safeguarding and promoting the safe use of Close Circuit Television (CCTV). Each school within the Trust has a separate approach to CCTV that will form part of its own procedures which can be found on the school's individual website. This statement outlines the approach schools should take when installing, using and reviewing CCTV. The statement is based on the ICO's code of practice for surveillance cameras and will:

- Help schools using CCTV comply with the Data Protection Act (DPA) and the General Data Protection Regulation (GRPR);
- Contribute to the efficient deployment and operation of a camera system;
- Mean that information captured is usable and can meet its objectives in practice;
- Reduce reputational risks by staying within the law and avoiding regulatory action and penalties;
- Re-assure those whose information is being captured; and
- Help schools to follow guidance in the Protection of Freedoms Act.

JTMAT Adopted CCTV Principles from the ICO Code of Practice

- Use of a surveillance camera system must always be for a specified purpose which is in pursuit of a legitimate aim and necessary to meet an identified pressing need.
- The use of a surveillance camera system must take into account its effect on individuals and their privacy, with regular reviews to ensure its use remains justified.
- There must be as much transparency in the use of a surveillance camera system as possible, including a published contact point for access to information and complaints.
- There must be clear responsibility and accountability for all surveillance camera system activities including images and information collected, held and used.
- Clear rules, policies and procedures must be in place before a surveillance camera system is used, and these must be communicated to all who need to comply with them.
- No more images and information should be stored other than that which is strictly required for the stated purpose of a surveillance camera system, and such images and information should be deleted once their purposes have been discharged.
- 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.
- Surveillance camera system 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.
- Surveillance camera system images and information should be subject to appropriate security measures to safeguard against unauthorised access and use.
- 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.

Expectations & Guidance

- The Trust will register with the Information Commissioners (ICO) and pay the appropriate fee on behalf of schools. You can search the register here https://ico.org.uk/ESDWebPages/Search.
- The Trust will ensure privacy statements are updated and relevant.
- The use of conventional cameras (not CCTV) by the Trust and its schools is not covered in this statement as these are governed by the DPA, GDPR and the Trust's own policies and procedures.

- If installing or extending CCTV a privacy impact assessment should be undertaken looking at the pressing need of the system is intended to address and whether its proposed use has a lawful basis and is justified, necessary and proportionate.

  A privacy impact assessment will be undertaken by each school's local governing body (LGB) in conjunction with the Trust GDPR Lead and Data Protection Officer to ensure compliance.

  When conducting a privacy impact assessment, the following should considered and documented at a minimum:
    - How practicable is it to take copies of a recording off your system when requested?
    - Can it provide information in a suitable format without losing image quality or date and time information?
    - Can the aims of the system be better achieved without using CCTV?
    - What is the lawful basis for processing this information?
    - How easy it is to locate and an extract information?
- Cameras should be sited and image capture restricted to ensure that they do not view areas not of interest, for example a person's private property. In areas where people have a heightened expectation of privacy, such as changing rooms, cameras should only be used in the most exceptional circumstances where it is necessary to deal with very serious concerns. This decision would be joint with between the headteacher/head of school and the local governing body.
- Schools should establish who has responsibility for the control of information, for example deciding what has to be recorded, how the information is to be recorded, how the information should be used and to whom it may be disclosed. The Trust recommends this responsibility lie with the headteacher or head of school in consultation with the Trust's GDPR Lead and Data Protection Officer (DPO) and information when disclosed is on a 'read only' format e.g. CD/DVD.
- If an organisation provides any processing services (such a remote monitoring of a system) a written contract should be obtained clearly defining;
    - The responsibilities of each party (the school and the contracted provider)
    - Information is processed in accordance to your instructions
    - What guarantees are available around security, storage and the use of properly trained staff
- Each school will have a CCTV procedure to determine how and why they use CCTV systems including;
    - Clearly defined and specific purposes for the collection and use of the information
    - Who, by name, has responsibility for the control of the information and making decisions about how it can be used.
    - Documented procedures based on this document, for how information should be handled. This should include guidance on disclosures and record keeping.
    - How and when proactive audits are a carried out.
    - What regular maintenance regime has been set up to ensure the system continues to provide the information required.
    - How recorded material is stored in order to protect the integrity of the data
    - A clearly defined retention period. There is no prescribed minimum or maximum retention period defined within legislation. The retention period should reflect the school's purpose.
    - Recorded images should be viewed in an appropriate secure location.
    - A map highlighting the location and the direction the camera faces.
    - How people are informed of CCTV usage. These signs should be displayed at the entrance of any CCTV zone, with further signs reinforcing this message within the zone. If audio recording is being used this should be stated clearly on any signage.
- Viewing of live images should be restricted to the operator and any authorised person where it is necessary for them to see it.
- CCTV and other surveillance systems should not normally be used to record conversations as this is considered to be more privacy intrusive than purely visual recording. Audio recording should only be used where;
    - You have identified a need or issue which can be characterised as a pressing social need and can evidence that this need must be addressed.

    - The school has considered other, less privacy intrusive, methods of addressing the need.
    - Having reviewed other less privacy intrusive methods, concluded that these would not appropriately address the need and the only way is through the use of audio recording.
    - The audio quality is sufficient to achieve the stated aim.
    - Data subjects are made aware in a clear and concise manor that audio recording is taking place.
- If a school has setup a live streaming camera available to the public so they can for example, view school events or other activities, you should ensure appropriate steps have been taken to either prevent identification of individuals and/or consent has been provided.
- If a school has two systems, some of the above will need to be duplicated if they differ significantly from one another e.g. Analogue vs Digital (IP)

Disclosure of Information

Please see the following sources of supporting information;

- JTMAT Policies (https://jtmat.co.uk/policies)
- JTMAT Privacy Centre (https://jtmat.co.uk/privacy)
- Information Commissioners' Office (https://ico.org.uk/)

Disclosure of information from surveillance systems must be controlled and consistent with the purpose(s) for which the system was established. For example, it can be appropriate to disclose surveillance information to a law enforcement agency when the purpose of the system is to prevent and detect crime, but it would not be appropriate to place them on the internet in most situations. It would not be appropriate to disclose information about identifiable individuals to the media without obtaining prior consent.

NOTE: Even if a system was not established to prevent and detect crime, it would still be acceptable to disclose information to law enforcement agencies if failure to do so would be likely to prejudice the prevention and detection of crime.

Any other requests for information should be approached with care as wider disclosure may be unfair to the individuals concerned.

Subject Access Requests (SARs)

Individuals whose information is recorded have a right to be provided with that information. When disclosing surveillance images of individuals, particularly when responding to subject access requests, each school will need to consider whether the identifying features of any of the other individuals in the image need to be obscured.

Where information of third parties is also shown with the information of the person who has made the access request, you must consider whether you need to obscure this information taking into account the considerations discussed. If there is a risk to these individuals rights and freedoms their identity should not be disclosed.

Please see the JTMAT Privacy Centre (https://jtmat.co.uk/privacy) for more information.

Freedom of Information (FOI)

If you receive a request for surveillance system information, you should consider:

- Is the information personal data of the requester? If so, then that information is exempt from the FOIA and FOISA. Instead this request should be treated as a data protection subject access request as explained above.
- Is the information personal data of other people? If it is, then the information can only be disclosed if this would not breach the data protection principles.

In practical terms, if individuals are capable of being identified either directly or indirectly from the relevant surveillance system, then it is personal information about the individual concerned. It is generally unlikely that this information can be disclosed in response to a freedom of information request as the requester could potentially use the information for any purpose and the individual concerned is unlikely to expect this. This may be unfair processing in contravention of the DPA.

Please see the JTMAT Privacy Centre (https://jtmat.co.uk/privacy) for more information.