Date ratified at Full Directors' Meeting **17 July 2023**	Review Resources Committee

St John the Baptist

Catholic Multi Academy Trust

POLICY ON THE USE OF CCTV SYSTEMS

THE TRUST MISSION STATEMENT

Inspired by the life of Christ we provide an exceptional education in our Catholic schools which enables our children:

- to fully embrace all possibilities
- to flourish
- to develop their faith

and therefore to choose a path that enables them to be a positive influence upon our world.

'Prepare the Way' *The Gospel of St Mark 1:3*

St John the Baptist Catholic Multi Academy Trust
Company No: 7913261
Registered Office: Surrey Street, Norwich NR1 3PB

IN TRAN
communication for all

If you need this document in large print, audio, Braille, alternative format or in a different language please contact the Company Secretary on 01603 611431 and we will do our best to help.

Section 37 of the Data Protection Act

The Data Protection Act requires that all CCTV installations designed to provide either crime prevention, crime detection or to enhance the safety of people on site, must comply with the requirements of the Act.

These are that:

1. Data must be processed fairly and lawfully.
2. Data can only be obtained for lawful purposes.
3. Data shall be adequate, relevant and not excessive
4. Data shall be accurate and kept up to date.
5. Data shall be kept secure and not be kept for longer than is necessary.
6. Data shall be processed in accordance with the rights of individuals under the Act.
7. Appropriate measures shall be taken to prevent unauthorised or unlawful processing of data against accidental loss, destruction or damage.
8. Personal data will not be transferred to a country outside European Economic Area.

This policy should be read in conjunction with the Data Protection Policy.

1. Data must be processed fairly & lawfully

- Cameras are sited in such a way that they only monitor those spaces which are intended to be covered by the equipment.

- Signs are placed so that students / staff and the public are aware they are entering a zone which is covered by surveillance equipment.

- The purpose of the use of CCTV is displayed – e.g. "Images are being monitored for the purposes of prevention and detection of crime."

- Contact details regarding the CCTV scheme (Site Management) are displayed.

2. Data can only be obtained for lawful purposes

- Disclosure of images to third parties is permissible only in limited and prescribed circumstances. Examples of third parties are:
    - Law enforcement agencies if the recorded image would assist in a specific criminal inquiry
    - Prosecution agencies
    - Relevant legal representatives
    - The media, but only in exceptional circumstances if it is decided that the public's assistance is needed in order to assist in the identification of victim, witness or perpetrator in relation to a criminal incident.

- Data obtained can only be used for the prevention or detection of criminal activity, or the apprehension and prosecution of offenders.

- If data used for the above purposes contains images of unrelated parties, these images will be disguised in such a way that they cannot be identified.

- Access to recorded images is restricted to only those who need to have access to achieve the purpose of using the equipment. This access is documented with the following information:
    - The identity of the data subject or third party to whom disclosure was made.
    - The date of disclosure.
    - The reason for allowing disclosure.
    - The extent of the information disclosed.
    - The name and signature of the managed or designated member of staff allowing the disclosure.

- Approved list of St John the Baptist Catholic MAT staff who have access to CCTV footage at their site of work:
  - Site Team (Site Managers, Facilities Managers and Facilities Officers) - site of work only.
  - Headteachers (which includes Executive Headteachers and Heads of School), members of Leadership Teams, Pastoral Team and Designated Safeguarding Officers - site of work only.
  - The CEO and members of the Executive Team - CCTV at any SJB CMAT site
  - Authorised staff members (office staff if required by job role)
  - Authorised Facilities Management at all sites for system maintenance.
  - All other staff must request in writing to their Headteacher, who will decide upon / approve / monitor requests.

3. <u>Data shall be adequate, relevant and not excessive</u>

- Cameras are sited so that they do not record more information than is necessary for the purpose for which they were installed.

- Staff may suggest positions for cameras, especially where staff personal safety may be enhanced by their strategic location

4. <u>Data shall be accurate and kept up to date.</u>

- Any personal information which is recorded and stored must be accurate.

- A documented procedure is kept which ensures that the accuracy of the system features are checked and if necessary amended or altered.

5. <u>Data shall be kept secure and not be kept longer than is necessary</u>

- The Site Manager / Facilities Manager or Authorised Office Staff are responsible in liaison with Headteacher for nominating a named person to carry out the following procedures:

  - Checking that the equipment performs properly.
  - Ensuring any special features are accurate (e.g. time display).
  - Reporting immediately if equipment is faulty or damaged.
  - Putting in place service contract for maintenance and servicing of CCTV cameras and system.

- The firmware / software for the cameras and other components of the CCTV system should be updated regularly in accordance with the manufacturer's advice. The maintenance company should be requested to confirm this is being done.
- If schools use their data network or wireless connection for CCTV, the cameras, CCTV recording equipment and traffic passing in between will have to be password secured against unauthorised access by other network users. If possible, ideally network cameras/system will be on dedicated individual secure part of network (e.g., a VLAN).

- Recorded data will normally be kept for a maximum of 30 days and then overwritten unless necessary for procedures in relation to staff conduct and then will be kept only as long as necessary until matters are concluded.

6. Data shall be processed in accordance with the rights of individuals under the Act

- They have the right to be provided with a copy of the information held about them.

- They have the right to prevent processing which is likely to cause damage or distress.

- They have rights in relation to decision taking.

7. Appropriate measures shall be taken to prevent unauthorised or unlawful processing of data against accidental loss, damage or destruction.

- It is required that appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of data and against accidental loss, damage or destruction.

- System should be protected by means of password to limit data access. If possible, systems should be also protected by physical access control.

- System should be locked when not in use.

- Monitor screens should be turned off when not being viewed where possible.

- In order to achieve this there is a need to assess any harm that might result from the processing, damage, loss, or destruction of this data.

- The nature of the data to be processed should be considered and where it contains details of inappropriate/unnecessary material it must be processed with greater care.

8. **<u>Personal data will not be transferred to a country outside the European Economic Area (EEA)</u>**.

- This principle places limitations on the ability to transfer personal data to countries and territories outside of the EEA.

- Data will not be made available to the public via internet or website.