JFS Policies **– CCTV – June 2025**

Headteacher	Chair of Governing Board
	
Dr David Moody	Mr Mark Hurst

Published Date	Staff	Review Date
June 2025	Dr David Moody	June 2026

This policy outlines the management, operation, and use of Closed Circuit Television (CCTV) systems at JFS School.

1. Purpose

The CCTV system is intended to:

- Promote a safe and secure environment for students, staff, and visitors.
- Prevent and reduce the risk of crime, vandalism, and anti-social behaviour.
- Support the school in safeguarding students and staff.
- Assist in the investigation of incidents and management of behaviour.
- Protect the school's premises and assets.

2. Scope

- This policy applies to all members of the school community, including staff, students, parents, contractors, and visitors. It covers the use of CCTV equipment installed across school property, including internal and external areas.

3. CCTV System Overview

- The CCTV system is owned by JFS School but is operating by the security team (SAFE 4 U LTD)
- Cameras are located in key areas where they do not infringe on personal privacy, such as corridors, entrances/exits, playgrounds, and car parks.
- Cameras are *not* located in private areas such as toilets, changing rooms, or staff rooms.
- Cameras are *not* located to provide access to the interior of private property outside of the school.
- CST – *Protecting Our Jewish Community* has remote access to some of the external cameras for security purposes

4. Responsibilities

- The Headteacher and designated Data Protection Officer (DPO) are responsible for overseeing the use of the CCTV system.
- Day-to-day management is delegated to the security team (SAFE 4 U LTD)

5. Data Protection and Privacy

- CCTV recordings are considered personal data under the Data Protection Act.
- JFS School is registered as a data controller with the Information Commissioner's Office (ICO).
- Clear signage is in place to inform individuals of the presence and purpose of CCTV monitoring.
- Data is collected fairly and used solely for the purposes set out in this policy.

6. Data Storage and Retention

- CCTV footage is password protected and stored securely with appropriate access controls.
- Recorded images are retained for a maximum of 2 months unless required longer for investigative purposes.
- After the retention period, footage is overwritten.

7. Access to Footage

- Individuals have the right to request access to footage in which they appear, under subject access request provisions.
- Requests must be made in writing to the DPO and may be subject to redaction to protect third-party identities.
- Access to live feeds and recorded footage is restricted to the security team at JFS. Under their supervision JFS Staff can view the CCTV footage.
- The Police can review the system without the supervision of the security team.
- During a major incident police will be given the authority to supervise the CCTV room.

8. Misuse of the CCTV System

- Misuse of the CCTV system, including unauthorised access or disclosure of footage, may result in disciplinary action and, where applicable, legal proceedings.

9. Monitoring and Review

- This policy is reviewed annually, or sooner if necessary, due to changes in legislation or school practices. The review will assess the ongoing necessity and effectiveness of CCTV usage.

10. Data Protection Act (2018)

The Seven principles of the Data Protection Act 2018 GDPR will be adhered to, and any future changes of legislation will be taken into account.

1) Lawfulness, fairness and transparency

The revised first principle of DPA 2018 mandates the organisations and controllers to be 100% transparent while seeking the individuals for data collection, processing and protection. They must deliver the data collection purposes in clear and plain language to address the data subjects' consent and individual rights on personal data collection.

2) Purpose limitation

This principle specifies that personal data must be used for the specific purpose the data subjects have given consent. The controller cannot use the data for processing outside the mentioned purpose. Unlike GDPR, DPA 2018 only gives leniency to store data beyond the defined data processing purpose in some cases, such as some historical, scientific, statistical or archiving purposes

3) Data minimization

The DPA 2018 conditions collect the necessary, relevant and not excessive amount of personal data for processing. The controller must not collect the data more than they need.

4) Accuracy

The controllers must verify that the data they process and collect is accurate and not misleading, incomplete or incorrect. At any point, the information is found inaccurate; it is the controller's responsibility to consider steps, i.e., erase or correct the data as soon as possible.

5) Storage limitation

The act makes it necessary for controllers not to keep personal data more than its requirement. They must notify the data subjects on how long they will hold the data. If any of the requirements are completed before its retention time, the controller should destroy or erase the data in such a situation. Controllers can only keep personal data for a long time if they need it for statistics, scientific, historical, and research purposes.

6) Integrity and confidentiality (Security)

The sixth DPA 2018 principle, also known as the security principle, ordered the organisations and controllers to have security controls and measures to protect the confidentiality or integrity of stored and processed personal data so no one can alter or steal the data subjects information. Read more about the CIA triad (confidentiality, integrity and availability) here. Regarding data protection, the controller must implement controls to prevent

- Unauthorised access to personal data
- Unauthorised processing of personal data
- Unlawful processing of personal data
- Accidental destruction, damage or loss to personal data

7) Accountability

This principle is relatively new in contrast with DPA 1998. With this newly added principle in DPA 2018, every organisation that stores or processes personal data must comply with regulatory obligations. To meet the legislation, controllers and businesses must design the data protection principles for secure usage of UK citizen's personal data.