Ribbleton Avenue
Methodist Junior School

"Brighter futures built with Ambition, Courage and Respect; filled with Love, Hope and Faith"

CCTV Policy

CCTV Policy

"Brighter futures built with Ambition, Courage and Respect; filled with Love, Hope and Faith"

---

1. Policy overview

Ribbleton Avenue Methodist Junior School uses Closed Circuit Television (CCTV) to help create a safe and secure environment for pupils, staff, visitors and school property.

This policy explains:

- why CCTV is used
- how it is managed and operated
- how privacy is protected
- how images are accessed, stored and disclosed

This policy applies to **all pupils, staff, volunteers, visitors and contractors** whose image may be captured by the CCTV system.

---

2. Legal framework

This policy complies with the following legislation and guidance:

- **UK General Data Protection Regulation (UK GDPR)**
- **Data Protection Act 2018**
- **Human Rights Act 1998**
- **Information Commissioner's Office (ICO) CCTV Code of Practice**
- **Freedom of Information Act 2000 (where applicable)**

CCTV images are regarded as **personal data** and are processed in accordance with data protection law.

---

3. Lawful basis for processing

The lawful basis for processing CCTV images is:

- **UK GDPR Article 6(1)(e): Public Task**
  Processing is necessary for the performance of a task carried out in the public interest, namely safeguarding children, maintaining security and preventing crime.

Where appropriate, **legitimate interests** may also apply (Article 6(1)(f)), balanced carefully against individuals' rights and freedoms.

---

4. Purpose of CCTV use

CCTV is used for the following purposes:

- To safeguard pupils, staff and visitors
- To protect school buildings, equipment and assets
- To deter and detect crime, vandalism and antisocial behaviour
- To assist with investigations of incidents and serious breaches of behaviour

CCTV is **not** used for:

- routine staff performance management
- teaching observation
- commercial purposes

---

5. Transparency and privacy

5.1 **Signage**
Clear and prominent CCTV signs are displayed at:

- all site entrances
- locations where cameras operate

Signs state that CCTV is in operation, the purpose of monitoring, and who controls the system.

5.2 **Privacy notices**
Information about CCTV is included in the school's **Privacy Notices** for pupils, parents, staff and visitors.

---

6. Siting and use of cameras

- Cameras are positioned to capture images **relevant and necessary** for the stated purposes.
- Cameras **are not installed** in toilets, changing rooms or other areas where there is a strong expectation of privacy.
- CCTV is **not routinely used in classrooms**.
- Cameras do not record audio.

Camera locations are reviewed regularly to ensure continued proportionality and compliance.

---

7. Covert monitoring

Covert CCTV monitoring will **only be considered in exceptional circumstances**, such as where:

- there is reasonable suspicion of serious criminal activity or safeguarding risk; and
- informing individuals would prejudice the investigation.

Any covert monitoring must:

- be **authorised in writing** by the Headteacher and Chair of Governors
- involve the **Data Protection Officer (DPO)**
- be **time-limited and specific**
- never be used to assess professional competence or capability

Covert monitoring will **never** take place in private areas (e.g. toilets).

---

8. Data Protection Impact Assessment (DPIA)

A **Data Protection Impact Assessment (DPIA)** has been completed for the CCTV system and is reviewed:

- annually
- when the system is significantly changed
- if risk levels increase

The DPIA identifies risks to privacy and sets out appropriate mitigation.

---

9. Storage and retention of images

- CCTV footage is stored securely on the school's system.
- Routine recordings are retained for **no longer than 7 days**.
- Footage required for investigation or legal purposes may be retained longer and will be clearly logged with a defined review date.
- All retained data is protected against unauthorised access, alteration or deletion.

---

10. Access to CCTV images

Access to live or recorded footage is **strictly limited** to authorised personnel:

- Headteacher
- Senior Leadership Team members
- Site / Premises Manager (where necessary)
- Safeguarding staff where relevant

Access is logged and monitored. Staff may only access footage as part of their official duties.

---

11. Subject Access Requests (SARs)

Any individual whose image may be captured has the right to request access to their personal data.

- Requests should be made in writing to the **Headteacher or Data Protection Officer**.
- The school will verify identity and request sufficient information (date, time, location).
- Requests are handled in line with the school's **Subject Access Request Policy**.
- Third-party images will be redacted or withheld unless lawful to disclose.
- Requests may be refused if disclosure would prejudice safeguarding or a lawful investigation.

---

12. Disclosure to third parties

CCTV images may be disclosed to third parties only where legally permitted, including:

- Law enforcement agencies
- Safeguarding partners
- Courts or regulatory bodies

All disclosures are:

- necessary and proportionate
- formally recorded
- made in accordance with data protection legislation

---

13. Use in school procedures

CCTV footage may be used as evidence in:

- behaviour investigations
- safeguarding concerns
- disciplinary or grievance procedures

Any use will comply with data protection principles and the school's internal policies.

---

14. Complaints

Complaints or concerns regarding CCTV should be raised with:

- the **Headteacher**, or
- the **Data Protection Officer**

Individuals may also raise concerns with the **Information Commissioner's Office (ICO)** if unresolved.

---

15. Governance and review

- **Data Controller:** Governing Body
- **Operational responsibility:** Headteacher
- **Data Protection Officer:** Mandy Gaitens (SBM)

This policy is reviewed **annually** or sooner if:

- legislation changes
- the CCTV system changes materially
- an incident indicates review is necessary

Appendix A – Internal Storage
Log of stored CCTV images (specific footage stored for longer than standard period)

Date Stored	Who by	Image/file Reference	Reason for retention	Please state the format these images are being stored (e.g. CD ROM/Hard Drive/Flash drive)	Please state the date the footage was erased , by whom and why.	Signed off by Data Protection Officer Date.

Appendix B – External Requests
Subect Access & Third Party Request Disclosure Log

NB: Please follow the Subject Access Request Policy procedures before disclosing any data

Date request received and from whom (name & organisation)	Date referred to DPO	Subject Access Request or Third Party Request	State the reason (if third party)	Date & nature of disclosure (viewing or copy of image)	Images viewed/sent (state location, date,time of original image/s and internal image reference)	The outcome if applicable