 



**CCTV Policy**

**February 2023**

Our Lady of Lourdes Catholic Multi-Academy Trust - Company Number: 7743523

Registered Office: 1st Floor, Loxley House, Riverside Business Park, Tottle Road, Nottingham NG2 1RT

**Contents**

1 Policy statement

2 Purpose of CCTV

3 Description of System

4 Siting of Cameras

5 Privacy Impact Assessment

6 Management & Access

7 Storage and Retention of Images

8 Disclosure of Images to Data Subjects

9 Disclosure of Images to Third Parties

10 Review of Policy and CCTV System

11 Misuse of CCTV systems

12 Complaints relating to this policy

ANNEX Definition of terms

**Trust Mission Statement**

We are a partnership of Catholic schools and our aim is to provide the very best Catholic education for all in our community and so improve life chances through spiritual, academic and social development.

We will achieve this by:

* Placing the life and teachings of Jesus Christ at the centre of all that we do
* Following the example of Our Lady of Lourdes by nurturing everyone so that we can all make the most of our God given talents
* Working together so that we can all achieve our full potential, deepen our faith, and know that God loves us
* Being an example of healing, compassion, and support for the most vulnerable in our society

*Psalm 138: 7 (GNT)*

*When I am surrounded by troubles, you keep me safe.*
*You oppose my angry enemies and save me by your power.*

**Guidance Note for School Leaders/Site Managers:**

**A key element in the assessment of lawful use of CCTV systems is the privacy impact assessment (PIA) conducted in relation to those systems setting out the justification for the system and its compliance with data protection legislation.**

**If the Trust/School has not conducted such an assessment then this must be conducted now, and this template policy amended to take account of the outcome of that assessment.**

**The Trust/School should do this with an open mind, including considering whether any existing cameras should be** **removed or the system modified in any way.**

**The completed impact assessment template (see page 9) should be forwarded to the Trust DPO for sign-off/approval.**

* **Highlighted sections of the policy should be completed as appropriate for each setting**
* **The Headteacher should designate named staff members to access / view the CCTV images**
* **The designated manager of the CCTV system should retain the log of access to viewed images (this log should be available as part of the GDPR annual audit)**
* **The designated manager of the CCTV system should retain the log of disclosures to third parties (this log should be available as part of the GDPR annual audit)**

**CCTV POLICY**

1. **Policy Statement**
	1. [Trust/School] uses Close Circuit Television (“CCTV”) within the premises of the [Trust/School]. The purpose of this policy is to set out the position of the [Trust/School] as to the management, operation and use of the CCTV at the [Trust/School].
	2. This policy applies to all members of our Workforce, visitors to the [Trust/School] premises and all other persons whose images may be captured by the CCTV system.
	3. This policy takes account of all applicable legislation and guidance, including:
		1. General Data Protection Regulation (“GDPR”)
		2. *[Data Protection Act 2018]* (together the Data Protection Legislation)
		3. CCTV Code of Practice produced by the Information Commissioner
		4. Human Rights Act 1998
	4. This policy sets out the position of the [Trust/School] in relation to its use of CCTV.
2. **Purpose of CCTV**
	1. The [Trust/School] uses CCTV for the following purposes:
		1. To provide a safe and secure environment for pupils, staff, and visitors
		2. To prevent the loss of or damage to the [Trust/School] buildings and/or assets and assist with any related financial claims/recovery
		3. To assist in the prevention of crime and assist law enforcement agencies in apprehending offenders
3. **Description of system**
	1. A HikVision IP based system with 11 Fixed CCTV cameras without sound recording. cameras have been sited to avoid capturing images which are not necessary for the purposes of the CCTV system. Installed cameras include a mixture of fully functional (PTZ), day / night vandal proof domes and internal audio capable camera
4. **Siting of Cameras**
	1. All CCTV cameras will be sited in such a way as to meet the purpose for which the CCTV is operated. Cameras will be sited in prominent positions where they are clearly visible to staff, pupils and visitors.
	2. Cameras will not be sited, so far as possible, in such a way as to record areas that are not intended to be the subject of surveillance. The [Trust/School] will make all reasonable efforts to ensure that areas outside of the [Trust/School] premises are not recorded.
	3. Signs will be erected to inform individuals that they are in an area within which CCTV is in operation.
	4. Cameras will not be sited in areas where individuals have a heightened expectation of privacy, such as changing rooms or toilets. Cameras should not be sited in classrooms.
5. **Privacy Impact Assessment**
	1. Prior to the installation of any CCTV camera, or system, a privacy impact assessment will be conducted by the [Trust/School] to ensure that the proposed installation is compliant with legislation and ICO guidance.
	2. The [Trust/School] will adopt a privacy by design approach when installing new cameras and systems, taking into account the purpose of each camera to avoid recording and storing excessive amounts of personal data.
6. **Management and Access**
	1. The CCTV system will be managed by the Head Teacher
	2. On a day-to-day basis the CCTV system will be operated by the site manager
	3. The viewing of live CCTV images will be restricted to the Site manager, office Manager and SLT
	4. Recorded images which are stored by the CCTV system will be restricted to access by Site manager, office Manager and SLT
	5. **No other individual will have the right to view or access any CCTV images unless in accordance with the terms of this policy as to disclosure of images.**
	6. The CCTV system is checked daily by the Site Manager to ensure that it is operating effectively
7. **Storage and Retention of Images**
	1. Recorded images are stored only for a period of 31 days unless there is a specific purpose for which they are retained for a longer period.
	2. The [Trust/School] will ensure that appropriate security measures are in place to prevent the unlawful or inadvertent disclosure of any recorded images. The measures in place include:
		1. CCTV recording systems being located in restricted access areas;
		2. The CCTV system being encrypted/password protected;
		3. Restriction of the ability to make copies to specified members of staff
	3. A log of any access to the CCTV images, including time and dates of access, and a record of the individual accessing the images, will be maintained by the [Trust/School].

*[Unless the CCTV records a specific incident then it is unlikely to be justifiable to retain any recorded images for more than, say, 28 days.]*

1. **Disclosure of Images to Data Subjects**
	1. Any individual recorded in any CCTV image is a data subject for the purposes of the Data Protection Legislation and has a right to request access to those images.
	2. Any individual who requests access to images of themselves will be considered to have made a subject access request pursuant to the Data Protection Legislation. Such a request should be considered in the context of the [Trust’s/School’s] Subject Access Request Policy.
	3. When such a request is made the site Manager, office Manager and SLT will review the CCTV footage, in respect of relevant time periods where appropriate, in accordance with the request.
	4. If the footage contains only the individual making the request, then the individual may be permitted to view the footage. This must be limited to that footage which contains only images of the individual making the request. The site Manager, office Manager and SLT must act appropriately to ensure that the footage is restricted in this way.
	5. If the footage contains images of other individuals, then the [Trust/School] must consider whether:
		1. The request requires the disclosure of the images of individuals other than the requester, for example whether the images can be distorted so as not to identify other individuals;
		2. The other individuals in the footage have consented to the disclosure of the images, or their consent could be obtained; or
		3. If not, then whether it is otherwise reasonable in the circumstances to disclose those images to the individual making the request.
		4. Consider providing stills from the CCTV with third parties having been redacted.
	6. **A record must be kept, and held securely, of all disclosures which sets out:**
		1. When the request was made;
		2. The process followed by the Site manager in determining whether the images contained third parties;
		3. The considerations as to whether to allow access to those images;
		4. The individuals that were permitted to view the images and when; and
		5. Whether a copy of the images was provided, and if so to whom, when and in what format.

(Please note that this CCTV disclosure log should be available to view at the annual GDPR Audit)

*[Please note that when a subject access request is made then, unless an exemption applies (such as in relation to third party data that it would be unreasonable to disclose) then the requester is entitled to a copy in a permanent form. We have referred only to “access” as opposed to a “permanent copy” as the [Trust/School] may consider it preferable in certain circumstances to seek to allow access to images by viewing in the first instance without providing copies of images. If an individual agrees to viewing the images only then a permanent copy does not need to be provided.* *However if a permanent copy is requested then this should be provided unless to do so is not possible or would involve disproportionate effort.]*

1. **Disclosure of Images to Third Parties**
	1. The [Trust/School] will only disclose recorded CCTV images to third parties where it is permitted to do so in accordance with the Data Protection Legislation.
	2. CCTV images will only be disclosed to law enforcement agencies in line with the purposes for which the CCTV system is in place.
	3. If a request is received from a law enforcement agency for disclosure of CCTV images, then the Site manager must follow the same process as above in relation to subject access requests. Detail should be obtained from the law enforcement agency as to exactly what they want the CCTV images for, and any particular individuals of concern. This will then enable proper consideration to be given to what should be disclosed, and the potential disclosure of any third-party images.
	4. The information above must be recorded in relation to any disclosure – this record should be available to view in during the annual GDPR Audit.
	5. If an order is granted by a Court for disclosure of CCTV images, then this should be complied with. However very careful consideration must be given to exactly what the Court order requires. If there are any concerns as to disclosure, then the Data Protection Officer should be contacted in the first instance and appropriate legal advice may be required.
2. **Review of Policy and CCTV System**
	1. This policy will be reviewed every 2 years.
	2. The CCTV system and the privacy impact assessment relating to it will be reviewed every 2 years.

*[The privacy impact assessment (PIA) relating to the system should be reviewed regularly to ensure that the use of any CCTV system continues to be justified and is compliant with legal requirements. The [Trust/School] should ensure that it has procedures in place to ensure that the CCTV system is regularly reviewed.]*

1. **Misuse of CCTV systems**
	1. The misuse of CCTV system could constitute a criminal offence.
	2. Any member of staff who breaches this policy may be subject to disciplinary action.
2. **Complaints relating to this policy**
	1. Any complaints relating to this policy or to the CCTV system operated by the [Trust/School] should be made in accordance with the [Trust/School] Complaints Policy.

|  |  |
| --- | --- |
| Date Reviewed | February 2023 |
| Next Review Date | February 2025 |
| Reviewer | Trust Audit & Risk Committee / OLoL Trust Exec Board / School |
| Author | Browne Jacobson template – edited by Tamer Robson & Will Ottewell & OLoL Schools |

**CCTV PRIVACY IMPACT ASSESSMENT TEMPLATE**

1. Who will be captured on CCTV?

|  |
| --- |
| Pupils, staff, parents / carers, volunteers, Governors and other visitors including members of the public etc. |

1. What personal data will be processed?

|  |
| --- |
| Facial Images, behaviour |

1. What are the purposes for operating the CCTV system? Set out the problem that the [Trust/School] is seeking to address and why the CCTV is the best solution, and the matter cannot be addressed by way of less intrusive means.

|  |
| --- |
| * To provide a safe and secure environment for pupils, staff and visitors
* To prevent the loss of or damage to St Patrick’s Catholic Primary School buildings and/or assets
* To assist in the prevention and detection of crime and assist law enforcement agencies in apprehending offenders
 |

1. What is the lawful basis for operating the CCTV system?

|  |
| --- |
| Legal obligation, legitimate interests of the organisation to maintain health and safety and to prevent and investigate crime |

1. Who is/are the named person(s) responsible for the operation of the system?

|  |
| --- |
| Jane Smedley Mark Holmes |

1. Describe the CCTV system, including:
	1. how this has been chosen to ensure that clear images are produced so that the images can be used for the purpose for which they are obtained;
	2. siting of the cameras and why such locations were chosen;
	3. how cameras have been sited to avoid capturing images which are not necessary for the purposes of the CCTV system;
	4. where signs notifying individuals that CCTV is in operation are located and why those locations were chosen; and
	5. whether the system enables third party data to be redacted, for example via blurring of details of third-party individuals.

|  |
| --- |
| * Digital high-definition IP cameras have been chosen to provide the highest quality of footage.

 * Cameras are placed within the school grounds to cover designated areas. Where cameras can record outside the school grounds, such as the front entrances and bus stops, the cameras are angled such that they minimise viewing neighbouring properties. Care is taken to minimise any loss of privacy by ensuring that cameras do not view external windows or entrances etc.

 * CCTV notices are displayed in key locations around the school including receptions. Visitors sign in using electronic signing in (Inventry) and a message is displayed to visitors to inform them that CCTV is in operation. This ensures that all visitors to the site are aware of CCTV in operation.

 * Footage recorded is done so in full detail. No footage is edited to redact the identity of those recorded.
 |

1. Set out the details of any sharing with third parties, including processors

|  |
| --- |
| Police, individuals making subject access requests, Data is stored on-premises with remote access by Site Manager. |

1. Set out the retention period of any recordings, including why those periods have been chosen

|  |
| --- |
| Recordings are kept for 31 days by default unless the footage is saved for evidence of an incident. This gives sufficient time to identify issues and investigate fully but reduces the risk of unnecessary data being kept. |

1. Set out the security measures in place to ensure that recordings are captured and stored securely

|  |
| --- |
| Data is recorded on a server kept in a secure server room. It is encrypted using industry standard encryption. |

1. What are the risks to the rights and freedoms of individuals who may be captured on the CCTV recordings?

|  |
| --- |
| * There is a minimal risk of CCTV being accessed unlawfully by means of a malicious attack on the school IT systems.
*
* There is minimal risk of CCTV being accessed by neglect of the SLT members regarding access to mobile devices (passkey protected) and/or desktop machines being left logged on.
*
* Data is kept for a maximum of 31 days to reduce risk of storing data unnecessarily.
*
* Risk of data loss when sharing with third parties.
 |

1. What measures are in place to address the risks identified?

|  |
| --- |
| * Antivirus and Firewall installed and maintained regularly on site
* Passkey used on mobile devices
* Data transferred to third parties will be carried out using encrypted devices and/or email of footage using encrypted email services provided by Microsoft O365. This is to reduce the risk of footage being lost in transit. Furthermore, this is only carried out in a minimal number of cases.
 |

1. Have parents and pupils where appropriate been consulted as to the use of the CCTV system? If so, what views were expressed and how have these been accounted for?

|  |
| --- |
| Parents and pupils have been informed of CCTV being used on site by means of signage. No concerns have been raised. |

1. When will this privacy impact assessment be reviewed?

|  |
| --- |
| Every two years |

**Approval:**

This assessment was approved by the Data Protection Officer:

DPO Jane Smedley Headteacher Jane Smedley

Date 24.3.23 Date 24.3.23