CCTV Policy

July 2019

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

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 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

1.1 [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].

1.2 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.

1.3 This policy takes account of all applicable legislation and guidance, including:

1.3.1 General Data Protection Regulation ("GDPR")

1.3.2 *[Data Protection Act 2018]* (together the Data Protection Legislation)

1.3.3 CCTV Code of Practice produced by the Information Commissioner

1.3.4 Human Rights Act 1998

1.4 This policy sets out the position of the [Trust/School] in relation to its use of CCTV.

2 Purpose of CCTV

2.1 The [Trust/School] uses CCTV for the following purposes:

2.1.1 To provide a safe and secure environment for pupils, staff and visitors

2.1.2 To prevent the loss of or damage to the [Trust/School] buildings and/or assets

2.1.3 To assist in the prevention of crime and assist law enforcement agencies in apprehending offenders

2.1.4 [INSERT AS REQUIRED]

3 Description of system

3.1 [Set out a description of the system, including the number of cameras, the technical capabilities of the cameras, whether these have sound recording capabilities, whether these cameras move or are fixed – from point 6 of the attached Privacy Impact Assessment document]

4 Siting of Cameras

4.1 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.

4.2 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.

4.3 Signs will be erected to inform individuals that they are in an area within which CCTV is in operation.

4.4 Cameras will not be sited in areas where individuals have a heightened expectation of privacy, such as changing rooms or toilets. *[If cameras are to be sited in classrooms then this should be stated together with justification supported by a privacy impact assessment.]*

5 Privacy Impact Assessment

5.1 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.

5.2 The [Trust/School] will adopt a privacy by design approach when installing new cameras and systems, taking into account the purpose of each camera so as to avoid recording and storing excessive amounts of personal data.

6 Management and Access

6.1 The CCTV system will be managed by [INSERT AS APPROPRIATE – THIS SHOULD BE AN INDIVIDUAL WITH APPROPRIATE SENIORITY].

6.2 On a day to day basis the CCTV system will be operated by [INSERT AS APPROPRIATE – THIS SHOULD BE AN INDIVIDUAL WITH APPROPRIATE TECHNICAL ABILITIES].

6.3 The viewing of live CCTV images will be restricted to [INSERT AS APPROPRIATE – THIS COULD BE AN INDIVIDUAL OR A GROUP OF INDIVIDUALS, BUT THERE MUST BE JUSTIFICATION FOR WHY SUCH INDIVIDUALS REQUIRE THE ABILITY TO VIEW FOOTAGE].

6.4 Recorded images which are stored by the CCTV system will be restricted to access by [INSERT AS APPROPRIATE – THIS SHOULD REFELCT THE POSITION AS IN 6.3 ABOVE].

6.5 **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.**

6.6 The CCTV system is checked [DAILY/WEEKLY/MONTHLY] by [INSERT AS APPROPRIATE] to ensure that it is operating effectively

7 Storage and Retention of Images

7.1 Any images recorded by the CCTV system will be retained only for as long as necessary for the purpose for which they were originally recorded.

7.2 Recorded images are stored only for a period of [INSERT NUMBER OF DAYS] unless there is a specific purpose for which they are retained for a longer period.

7.3 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:

7.3.1 CCTV recording systems being located in restricted access areas;

7.3.2 The CCTV system being encrypted/password protected;

7.3.3 Restriction of the ability to make copies to specified members of staff

7.3.4 [INSERT AS APPROPRIATE]

7.4 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.]

8 Disclosure of Images to Data Subjects

8.1 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.

8.2 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.

8.3 When such a request is made the [INSERT INDIVIDUAL(S) WITH ACCESS TO CCTV – as set out in 6.3] will review the CCTV footage, in respect of relevant time periods where appropriate, in accordance with the request.

8.4 If the footage contains only the individual making the request then the individual may be permitted to view the footage. This must be strictly limited to that footage which contains only images of the individual making the request. The [INSERT INDIVIDUAL WITH ACCESS TO CCTV – as set out in 6.3] must take appropriate measures to ensure that the footage is restricted in this way.

8.5 If the footage contains images of other individuals then the [Trust/School] must consider whether:

8.5.1 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;

8.5.2 The other individuals in the footage have consented to the disclosure of the images, or their consent could be obtained; or

8.5.3 If not, then whether it is otherwise reasonable in the circumstances to disclose those images to the individual making the request.

8.6 **A record must be kept, and held securely, of all disclosures which sets out:**

8.6.1 When the request was made;

8.6.2 The process followed by [INSERT INDIVIDUAL WITH ACCESS TO CCTV] in determining whether the images contained third parties;

8.6.3 The considerations as to whether to allow access to those images;

8.6.4 The individuals that were permitted to view the images and when; and

8.6.5 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.]

9 Disclosure of Images to Third Parties

9.1 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.

9.2 CCTV images will only be disclosed to law enforcement agencies in line with the purposes for which the CCTV system is in place.

9.3 If a request is received from a law enforcement agency for disclosure of CCTV images then [INSERT INDIVIDUAL WITH ACCESS TO CCTV] 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.

9.4 The information above must be recorded in relation to any disclosure – this record should be available to view in during the annual GDPR Audit.

9.5 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.

10 Review of Policy and CCTV System

10.1 This policy will be reviewed ANNUALLY.

10.2 The CCTV system and the privacy impact assessment relating to it will be reviewed ANNUALLY.

[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.]

11 Misuse of CCTV systems

11.1 The misuse of CCTV system could constitute a criminal offence.

11.2 Any member of staff who breaches this policy may be subject to disciplinary action.

12 Complaints relating to this policy

12.1 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 Issued	June 2019
Date of Review	June 2020
Reviewer	Karen Rich / OLoL Trust / School
Author	Browne Jacobson template – edited by Karen Rich & 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.]

2 What personal data will be processed?

[Facial Images, behaviour, sound, etc.]

3 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.

[Prevention or detection of crime etc.]

4 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]

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

6 Describe the CCTV system, including:

a. 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;

b. siting of the cameras and why such locations were chosen;

c. how cameras have been sited to avoid capturing images which are not necessary for the purposes of the CCTV system;

d. where signs notifying individuals that CCTV is in operation are located and why those locations were chosen; and

e. whether the system enables third party data to be redacted, for example via blurring of details of third party individuals.

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

[Police, subject access, etc. Careful consideration should be given to whether any provider is used in relation to the CCTV system and the access they might have to images. Will those processors send this data outside of the EEA, for example for storage in a cloud based system?]

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

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

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

For example:

- Is it fair to record them in the way proposed?
- How is the amount of data processed to be minimised?
- What are the risks of the system being accessed unlawfully?
- What are the potential data breach risks?
- What are the risks during any transfer of recordings, or when disclosed to third parties such as the police?

11 What measures are in place to address the risks identified?

12 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?

13 When will this privacy impact assessment be reviewed?

Approval:

This assessment was approved by the Data Protection Officer:

DPO ……

Date …….