

CCTV POLICY



St. Vincent's Catholic Primary School

Together through Christ we grow and learn

Approved by: Marina Coleman
Normunds Cukermanis

Last reviewed on: October 2019

Next review due by: End of October 2020

Contents

1. Data Protection	Error! Bookmark not defined.
2. Policy Statment.....	2
3. Camera Set Up	Error! Bookmark not defined.
4. Purpose of CCTV.....	3
5. Covert Monitoring.....	3
6. Storage and Retention	3
7. Access to CCTV Footage.....	4
8. Disclosure of Images to Data Subjects (Subject Access Requests)	4
9. Disclosure of Images to Third Parties.....	4
10. Complaints	4

1. Data Protection:

Any personal data processed in the delivery of this policy will be processed in accordance with the school Data Protection Policy and can be found in the Record of Data Processing.

2. Policy Statement

St. Vincent's Catholic Primary School uses Close Circuit Television ("CCTV") within the premises of the school. The purpose of this policy is to set out the operation, use, storage and disclosure of CCTV at the School.

This policy applies to all data subjects whose image may be captured by the CCTV system. It works in concurrence with the School's Data Protection Policy, Record of Data Processing and Data Retention schedule.

The policy considers applicable legislation and guidance, including but not limited to;

- General Data Protection Regulation (GDPR)
- Data Protection Act (DPA) 2018
- CCTV Code of practice as produced by the Information Commissioner Office (ICO)
- Human Rights Act 1998.

The CCTV system is **owned and operated by the school** and the deployment is determined by the Senior Leadership Team, with consultation from the Board of Governors and Data Protection Officer (DPO).

The school will:

- Notify the ICO of its use of CCTV as part of its registration.
- Complete a Data Privacy Impact Assessment if amendments are to be made to the deployment or use of CCTV.
- Treat the system and all information processed on the CCTV system as data which is processed under DPA 2018/GDPR.
- Not direct cameras outside of school grounds onto private property, an individual, their property or a specific group of individuals. The exception to this would be if authorization was obtained for Direct Surveillance as set up by the Regulatory of Investigatory Power Act 2000.
- Display Warning signs will be positioned clearly in prominent places.

Specifically, at all external entrances of the school site where CCTV is use and covers external areas. These signs will include information on how to contact the school regarding information or access to the CCTV footage.

- There is no guarantee that this system will or can cover and detect every single incident taking place in the areas of coverage.

- CCTV footage will not be used for any commercial purposes.

3. Camera Setup

The CCTV system is comprised of **20** cameras which record day and night covering the **Internal & External** areas of the School. **Their coverage also extends past the school boundaries to public areas.**

Cameras will be placed so they only capture images relevant for the purposes for which they are installed, and all care will be taken to ensure that reasonable privacy expectations are not violated.

CCTV is not sited in classrooms and will not be used in such, except in exceptional circumstances.

Members of staff on request can access details of CCTV camera locations.

4. Purpose of CCTV

The School uses CCTV for the following purposes:

- To provide a safe and secure environment for the workforce and visitors.
- To protect the school buildings and assets.
- To assist in the prevention and detection of criminal activity.
- Assist law enforcement agencies in apprehending suspected offenders.

5. Covert Monitoring

The school retains the right in exceptional circumstances to set up covert monitoring. For example;

- Where there is good cause to suspect illegal or serious unauthorized action(s) are taking place, or where there are grounds to suspect serious misconduct.
- Where notifying the individuals about the monitoring would seriously prejudice the reason for making the recording.

In these circumstances' authorisation must be obtained from the Head Teacher and Chair of Governors.

Covert monitoring will cease following the completion of an investigation.

6. Storage and Retention

Recorded data will not be retained for longer than is necessary, while retained the integrity of the recordings will be maintained to ensure their evidential value and to protect the rights of people who images have been recorded.

All Data will be stored securely;

The monitor to view CCTV footage will be kept School office, Head Teachers office, Deputy Head office, Hall, ICT room, ICT cupboard

Recordings will be kept for **10 days**. These will be stored in/on **DVR Hard drive**.

We do not backup footage.

7. Access to CCTV Images

The ability to view live and historical CCTV footage is only to be provided at designated locations and by authorised persons.

Specific live monitoring is limited to **4 cameras**

Direct Access to recorded footage is limited to only the Premises Manager and the Head Teacher.

Only in exceptional circumstances would any other individuals be allowed to view footage, the reasons and details for these circumstances would be recorded for posterity.

8. Disclosure of Images to Data Subjects (Subject Access Requests)

Any individual recorded in any CCTV image is considered a data subject and therefore has the right to request access to those images.

These requests will be considered a Subject Access Request and should follow the schools Subject Access Request process as detailed in the St. Vincent's Data Protection Policy October 2018.

9. Subject access requests and other rights of individuals

9.1 Subject access requests

Individuals have a right to make a 'subject access request' to gain access to personal information that the school holds about them. This includes:

- *Confirmation that their personal data is being processed*
- *Access to a copy of the data*
- *The purposes of the data processing*
- *The categories of personal data concerned*
- *Who the data has been, or will be, shared with*
- *How long the data will be stored for, or if this isn't possible, the criteria used to determine this period*
- *The source of the data, if not the individual*
- *Whether any automated decision-making is being applied to their data, and what the significance and consequences of this might be for the individual*

Subject access requests must be submitted in writing, either by letter, email or fax to the DPO. They should include:

- *Name of individual*
- *Correspondence address*
- *Contact number and email address*
- *Details of the information requested*

If staff receive a subject access request they must immediately forward it to the DPO.

9.2 Children and subject access requests

Personal data about a child belongs to that child, and not the child's parents or carers. For a parent or carer to make a subject access request with respect to their child, the child must either be unable to understand their rights and the implications of a subject access request, or have given their consent.

Children below the age of 12 are generally not regarded to be mature enough to understand their rights and the implications of a subject access request. Therefore, most subject access requests from parents or carers of pupils at our school may be granted without the express permission of the pupil. This is not a rule and a pupil's ability to understand their rights will always be judged on a case-by-case basis.

9.3 Responding to subject access requests

When responding to requests, we:

- *May ask the individual to provide 2 forms of identification*
- *May contact the individual via phone to confirm the request was made*
- *Will respond without delay and within 1 month of receipt of the request*
- *Will provide the information free of charge*
- *May tell the individual we will comply within 3 months of receipt of the request, where a request is complex or numerous. We will inform the individual of this within 1 month, and explain why the extension is necessary*

We will not disclose information if it:

- *Might cause serious harm to the physical or mental health of the pupil or another individual*
- *Would reveal that the child is at risk of abuse, where the disclosure of that information would not be in the child's best interests*
- *Is contained in adoption or parental order records*
- *Is given to a court in proceedings concerning the child*

If the request is unfounded or excessive, we may refuse to act on it, or charge a reasonable fee which takes into account administrative costs.

A request will be deemed to be unfounded or excessive if it is repetitive, or asks for further copies of the same information.

When we refuse a request, we will tell the individual why, and tell them they have the right to complain to the ICO.

When such a request is made, the footage will be reviewed in accordance with the request.

If the footage contains only the data subject making the request, then the individual may be permitted to view the footage.

This will be strictly limited to the footage of the data subject making the request and the specific reason for the request.

If the footage contains images of other data subjects, then the school will consider if;

- The request requires the disclosure of the images of data subjects other than the requester, and if these additional data subjects can be anonymized from the footage.
- The other individuals in the footage have consented to the disclosure of the images or if their consent could be obtained.
- If not, then either it is reasonable in the circumstances to disclose those images to the data subject making the request.

The School reserves the right to refuse access to the CCTV footage where this would prejudice the legal rights of other data subjects or jeopardize an ongoing investigation.

9. Disclosure of Images to Third Parties

The School will only disclose record CCTV footage to third parties where there is a lawful basis to do so.

Third parties acting on behalf of a data subject will be handled in accordance with the Subject Access Request Policy.

CCTV footage will only be disclosed to law enforcement agencies in line with the purpose for which the CCTV system is in place.

If a request is received from a law enforcement agency for the disclosure of footage then the school will follow the Subject Access Request process, obtaining the reasoning for wanting to obtain the footage and any data subjects of concern.

This will give help enable proper consideration of the extent of what can be disclosed. This information will be treated with the upmost confidentiality.

If an order is granted by a court for the disclosure of CCTV images then this should be complied with. However, consideration must be given to exactly what the court requires.

In all instances, if there are any concerns as to what should or should not be disclosed then the DPO should be contacted and further legal sought as per requirements.

10. Complaints

We take any complaints about our collection and use of personal information very seriously.

If you think that our collection or use of personal information is unfair, misleading or inappropriate, or have any other concern about our data processing, please raise this with us in the first instance.

To make a complaint, please contact our data protection officer. Our DPO is John Pearson Hicks and is contactable via john.pearson-hicks@london.anglican.org

Alternatively, you can make a complaint to the Information Commissioner's Office:

- Report a concern online at <https://ico.org.uk/concerns/>
- Call 0303 123 1113
- Or write to: Information Commissioner's Office, Wycliffe House, Water Lane, Wilmslow, Cheshire, SK9 5AF



Appendix 1 Subject Access Request Log

St. Vincent's Catholic Primary School

Subject Access Record Log

Name of data subject		
Name of person making the request and relationship to data subject if different (e.g. parents / carers making a subject access request on behalf of a child who does not have the capacity to exercise their own rights, trade union representative, solicitor on behalf of a client)		
Contact details of requester (email / telephone etc.)		
Has the DPO been notified?	Y N	
Date data request received		
Date acknowledgment sent		
Deadline for responding to the request		
Name of person dealing with request		
Do you have sufficient proof / information to be assured of the requester's identity?	Y N	
If a parent has made request on behalf of their child, have you established whether the child has the capacity to exercise their own rights in relation to their personal data (age 13+)?	Y N	
Are there any court orders in place which would restrict the parent's ability to access the personal data?	Y N	
What personal data have they requested?		
Do you need to clarify the request? Should the requester be asked to refine their request?	Y N	

St. Vincent's Catholic Primary School regularly reviews and updates all Acceptable Use documents to ensure that they are consistent with the school Online Safety and Safeguarding Policies. We attempt to ensure that all students have good access to digital technologies to support their teaching and learning and we expect all our students to agree to be responsible users to help keep everyone safe and to be fair to others.