OAKLANDS CATHOLIC SCHOOL

AND

SIXTH FORM COLLEGE

With delegated responsibility from the Edith Stein Catholic Academy Trust

IMAGERY POLICY

APPROVED BY ETHOS AND STRATEGY COMMITTEE	**June 2023**
INSPECTED AND SCUTINISED BY SLT	**May 2023**
REVISED	**May 2023**
MEMBER OF STAFF RESPONSIBLE	**DIRECTOR OF BUSINESS AND FINANCE**
STATUTORY / NON-STATUTORY	**NON-STATUTORY**

Community Unity Opportunity

Policy Amendments

Version Date	Section / Page	Amendments
May 2023	5.4 / Page 4	Change to CCTV footage retention and removal to a dedicated folder if required
March 2023	1.2 / Page 2 10.1 / Page 7 11.1 / Page 7 12.0 / Page 8	Changes made to reflect the very rare use of Skype and the additional control measures if it is used
February 2023	6.2 / Page 5	Update to CCTV locations
	6.2 / Page 5	Update to named locations
January 2022	1 / Page 2	Insertion of links to referenced documents
	1.2 / Page 2	Update to reference to Data Protection Act 2018
	4.2 / Page 3	Insertion of hyperlink to the ICO document “In the picture: A data protection code of practice for surveillance cameras and personal information”
	4.4 / Page 3	Change to text relating to CCTV signage
	6.2 / Page 5	Update to CCTV locations
June 2021	Throughout	Removal of LessonBox, as no longer used. Replace with “classroom video recording”
		Removal of Skype, as no longer used and replace with “Microsoft Teams”
		Inclusion of “Zoom”
	8.1 / Page 6	Clarification of year for Data Protection Act.

"The eye is the lamp of the body. If your eyes are healthy, your whole body will be full of light"'
Matthew 6:22

1.0 Introduction

1.1 Oaklands Catholic School and Sixth Form College is committed to providing a caring, friendly and safe environment for all of our students and staff so that teaching and learning can take place in a positive and secure atmosphere. The School is also committed to complying with the General Data Protection Regulations ("GDPR") and other Data Protection legislation. This Policy supports these objectives and should be read in conjunction with the School's Data Protection Policy and General IT Policy.

1.2 This Policy divides into four sections:

- Policies for all types of images including Closed Circuit Television (CCTV), classroom video recording and Microsoft Teams.
- Classroom video recording can be used to assist Teachers either as part of their initial training or as part of their Continued Professional Development (CPD).
- The school has a number of CCTV cameras permanently installed around the site. The school's CCTV is registered with the Information Commissioner under the terms of the Data Protection Act 2018. The Data Protection Act 2018 covers the use of CCTV and associated images. This policy outlines the school's use of CCTV and how it complies with the Act.
- The use of Microsoft Teams, part of the Office365 suite of online services, and Zoom are used by the school, to enable video conferencing and real-time collaboration with others over the internet. The use of these two programmes have mostly negated the use of Skype in school.

2.0 General Use of Images

2.1 This section applies to CCTV, classroom video recording, Microsoft Teams and Zoom.

2.2 There has never been and will not be any intention on the part of Senior Leadership Team, Governors or any other body, to use the video technology for the purposes of staff performance management. Neither will any footage be used as evidence in staff disciplinary hearings or during any capability proceedings.

3.0 Classroom Video Recording

3.1 This section only applies to the use of classroom video recording in the School.

3.2 The Information Commissioners Office (ICO - the body responsible for data protection) approves using classroom video recording for the purposes of teacher training and development. It is legal for schools to film children in the classroom for the purposes of teaching and learning training and development as long as they follow the ICO guidelines.

3.3 Classroom video recording will not form part of lesson observation for performance management.

3.4 Classroom video recording equipment can be booked through the School's "RoomBooker" website. It will be set up in the requested location by the IT Support team. The equipment is then under the FULL control of the classroom teacher, who can start/stop recording as required. It is the teacher's responsibility to familiarise themselves with the basic operation of the equipment. If a support tutor is also working in the room, they must give their verbal permission prior to any recording. The teacher may delegate control of the recording to a third party if they wish (usually for technical support). They may also delegate full control of the editing of the recording to another if they see fit.

3.5 Under normal circumstances, teachers, other staff and students will be recorded when the cameras are recording. During such times, there remains the possibility that any visitor to the classroom (parent, Governor, other visitor) is also recorded. These recordings can be considered in the same way as CCTV recording: the same general signage will apply.

3.6 Recordings are supplied to the member of staff on a special laptop, which is locked down so that recordings may not be moved, copied or otherwise distributed. The laptop must be returned to the IT Support Office within 5 working days. Recordings will be deleted either on the return of the laptop, or at the latest 20 days after recording. Only the teacher concerned may view the archived recordings unless he or she has given verbal or written authorisation otherwise. This does not affect a data subjects' statutory right to view data about them.

3.7 The School's IT Support Team, who may request third line support from the manufacturer as necessary, supports classroom video recording.

4.0 CCTV

4.1 This section only applies to the use of CCTV in the School.

4.2 The school complies with Information Commissioner's Office (ICO) document "In the picture: A data protection code of practice for surveillance cameras and personal information" (Version 1.2 or later) to ensure it is used responsibly and safeguards both trust and confidence in its continued use. The Code of Practice can be viewed at the following link.

4.3 The School uses CCTV video footage and static images to:

- Maintain a safe environment, helping to ensure the welfare of staff, students and visitors
- Deter criminal acts against persons and property
- Assist the School leadership team when investigating an issue in School.
- Assist the Police in identifying persons who have committed an offence.

4.4 Signage indicating the use of CCTV is sited near the public entrance to the White House and several locations around the school.

4.5 The system is a closed digital system and comprises of a number of fixed cameras. Sound is not recorded.

4.6 The School owns and operates the CCTV system. The Headteacher and Governors determine its deployment. The introduction of, or changes to, CCTV monitoring will be subject to consultation with the Headteacher.

4.7 The CCTV system continually records on a loop and recoding in some areas is motion activated. Footage is automatically overwritten by new footage. Depending on the motion activity in the area covered by a specific camera, footage is retained in the CCTV system for approximately 20 days.

4.8 Monitoring of a small number of cameras takes place in Reception area during office hours, where live footage is viewable by the Receptionist and other members of staff in that area. Footage is not visible for members of the public or students.

4.9 All authorised operators and employees with access to images are aware of and follow this Policy when accessing the recorded images. All employees are aware of the restrictions in relation to accessing and distribution of recorded images.

5.0 Accessing CCTV Footage

5.1 Any member of staff may ask any member of the Senior Leadership Team (SLT) for permission to view CCTV footage. The requestor must indicate in general the location and approximate time of the footage they wish to review.

5.2 It is up to the discretion of the Senior Leader whether to grant permission to review footage. The decision of the Senior Leader to sponsor the review of CCTV footage will depend on the nature and severity of the incident in question, and the likely chance of identification of any individual(s) being identified as a result. If granted, the Senior Leader must inform IT Support, who will arrange with the requesting member of staff a time to review the footage with them, and will document the request.

5.3 If an incident has been recorded on CCTV and needs to be kept as evidence, a short extract of video footage or still images may be exported from the CCTV system. This evidence is documented by IT Support, and placed in a secure area of the school network. IT Support will inform the requester and sponsor when the footage is available and where it can be reviewed as necessary. Video evidence is only viewable using approved software. It cannot be played on standard software, such as VLC Player.

5.4 Evidence will be deleted at the end of teach term by IT Support unless the Sponsor specifically requests that it be kept for a longer period. It will then be up to the Sponsor to ensure the footage is moved into a dedicated folder and is deleted when no longer required.

5.5 The Sponsor may also request that individuals on exported footage be anonymised by blanking faces or other features. This can be a time consuming process and should only be requested in exceptional circumstances.

5.6 Further disclosure of CCTV evidence must always be consistent with the purpose(s) for which the system was established. For example, the School may show images to the Police or to individuals who are the subject of the surveillance and their Parents/Carers. The school will ensure that disclosure is fair to the individuals concerned and that privacy intrusion to any third party individuals will be minimal. Requests for further disclosure must be made to the Headteacher. The School will refuse any such request unless:

- There is a legal obligation, such as a court order or information access rights.
- Authorised personnel such as Law Enforcement Agencies and service providers make the request to the school where these would reasonably need access to support the School and its aims.
- There are reasonable grounds for further disclosure, such as the safeguarding of staff and/or students.

6.0 CCTV Camera Location

6.1 Cameras will be sited so they only capture images relevant to the purposes for which they are installed and care has been taken to ensure that reasonable privacy expectations are not violated. The school will ensure that the location of equipment is carefully considered to ensure that images captured comply with the Data Protection Act. The CCTV system has been designed for maximum effectiveness and efficiency. The school cannot however guarantee that every incident will be detected or covered and 'blind spots' may exist around the school site. The school will make every effort to position cameras so that their coverage is restricted to the school premises, which includes outdoor areas.

6.2 Camera locations are in the table below. Sample images of camera locations can be found at N:\08_StaffInformation\CCTV Positions

Location (EX = External, otherwise Internal)	
Blessed Fra (Angelico) Entrance (EX)	Music Lobby
Angelico Foyer	Music Bins (EX)
Bike Sheds #1 (EX)	St John Henry Newman (N) Boys and Girls Toilets
Bike Sheds #2 (EX)	N Block Lockers
Canteen #1	N Block Stairs
Canteen #2	N7 #1
Canteen Entrance (EX)	N7 #2
Chapel Approach (EX)	N8 #1
Chapel Entrance (EX)	N8 #2
Chapel Rear (EX)	N16
Hall #1	N Block Staffroom / Romero Playground (EX)
Hall #2	N Block / JP Block (EX)
Hall #3	Oaklands Way (EX) (from pole by Kolbe)
Hall #4	Romero Bag Store
St John Paul II (JP) 1st Floor Corridor #1	Health Suite Changing Rooms Entrance
JP 1st Floor Corridor #2	Romero Gym Entrance
JP 1st Floor Toilets	Romero Gym
JP 12	Romero Gym Entrance (EX)
JP 14 #1	Roundabout (EX)
JP 14 #2	Sixth Form Entrance
JP 15 #1	Slope Down (EX)
JP 15 #2	Slope Up (EX)
JP Entrance	Covered Walkway (EX)
JP Exit	Sports Hall Entrance (EX)
JP Ground Floor Corridor #1	Sports Hall Changing Rooms Entrance
JP Ground Floor Corridor #2	Sports Hall #1 (IN)
JP Ground Floor Toilets	Sports Hall #2 (IN)
JP Playground Rear	Sports Hall Basketball Court (EX)
JP / St Oscar (Romero) Playground	St Thomas More (T) Block Corridor #1
St Maximillian (Kolbe) Entrance (EX)	T Block Corridor #2
Kolbe Entrance	T Block Corridor #3
Kolbe Lockers	T Block Corridor #4
Kolbe Side (EX)	T Block Corridor #5
St Cecilia (Music) Practice Room #1	T Block Lockers
Music Practice Room #2	T Block Boys and Girls Toilets
Music Practice Room #3	White House Rear Entrance (EX)
Music Practice Room #4	White House Reception
Lower Playground (EX)	White House Reception Entrance (EX)
Music Entrance (EX)	

7.0 Covert Monitoring

7.1 The school may in exceptional circumstances set up covert monitoring. For example:

i) Where there is good cause to suspect that an illegal or unauthorised action(s), is taking place, or where there are grounds to suspect serious misconduct;

ii) Where notifying the individuals about the monitoring would seriously prejudice the reason for making the recording.

7.2 In these circumstances authorisation must be obtained from the Headteacher or in his absence one of the Deputy Headteachers. Covert monitoring must cease following completion of an investigation.

8.0 Subject Access Request (SAR)

8.1 Individuals have the right to request access to CCTV footage relating to themselves under the Data Protection Act 2018.

8.2 All requests should be made in writing to the Headteacher. Individuals submitting requests for access will be asked to provide sufficient information to enable identification. For example, date, time and location.

8.3 The school will respond to requests within 40 calendar days of receiving the written request.

8.4 The school reserves the right to refuse access to CCTV footage where this would prejudice the legal rights of other individuals, this includes sharing images of third parties where they have not agreed to the release of images, or jeopardise an ongoing investigation.

9.0 Complaints

9.1 Complaints and enquiries about the operation of CCTV within the school should be directed to the Data Protection Officer in the first instance.

10.0 Microsoft Teams and Zoom

10.1 Microsoft Teams and Zoom are internet/telephony video applications that use peer-to-peer (P2P) network protocols to enable users to establish internet-based voice and video communication to other users. This may be used internally around the School, or externally, for example to St. Johns.

11.0 Reasons for Concern

11.1 Whilst Microsoft Teams and Zoom are fairly safe to use, Skype is not. If third party computers are connected to a fast Internet feed, there is a high risk that the computer will become a “Supernode” that starts to route large amounts of Internet traffic (that is a lot of other people’s video/conversations, not just your own). This could have service implications for not only the local computer but also the wider School network. Additionally, due to the closed nature of the Skype protocols, there are concerns as to the security and privacy implications of the use of Skype. For this reason, Skype is not to be used without the express permission of the Head of IT, see Section 12.0.

12.0 Restrictions on the use of Skype at Oaklands

12.1 The School does recognise the potential benefits of Skype and therefore allows Skype to be installed on machines connected to the school network provided the following conditions are met/understood:

- Skype should only be used where there is a clear academic or business purpose.
- Skype should only be installed by the IT Support Team.
- Skype must be set to not load automatically on start up.
- Skype is only running whilst the user is at the computer to receive or make calls.

12.2 Should a computer on which Skype is installed use an excessive amount of bandwidth the user must contact IT Support immediately. IT Support may disconnect the computer from the network.

13.0 Photographs

13.1 Whilst photographs are a form of imagery they should be treated in the same way as any other element of documented personal data whether held in hard copy or electronically. Personal data held in documented form is covered under the School's Data Protection Policy.

14.0 Further Information

14.1 Further information on the use of Imagery at the School can be provided by the Data Protection Officer via email: data.protection@oaklandscatholicschool.org