All Saints' Church of England Primary School

GDPR – CCTV AND SURVEILLANCE POLICY

"Loving to Learn, learning to Love"

"A new command I give you, Love one another.

As I have loved you, so you must love one another."

John 13:34

Ratified by the Full Governing Body: 09.11.2021 Review date: Autumn 2022

Policy Contents

STATEMENT OF INTENT

We believe that CCTV and other surveillance systems have a legitimate role to play in helping to maintain a safe and secure environment for all our staff, students and visitors. However, we recognise that this may raise concerns about the effect on individuals and their privacy and as such this Policy is intended to address such concerns.

At All Saints' CE Primary School, we take our responsibility towards the safety of staff, visitors and pupils very seriously. To that end, we use surveillance cameras to monitor any instances of aggression or physical damage to our schools and its members. The purpose of this policy is to manage and regulate the use of the surveillance and CCTV systems at our schools and ensure that:

- We comply with the GDPR, effective as of 25 May 2018.
- The images that are captured are useable for the purposes we require them for.
- We reassure those persons whose images are being captured, that the images are being handled in accordance with data protection legislation.

This policy covers the use of surveillance and CCTV systems which capture moving and still images of people who could be identified, as well as information relating to individuals for any of the following purposes:

- Observing what an individual is doing
- Taking action to prevent a crime
- Using images of individuals that could affect their privacy

This Policy covers all employees, workers, contractors, agency workers, consultants, directors, members, governors, trustees, past or present students and may also be relevant to visiting members of the public.

This Policy is non-contractual and does not form part of the terms and conditions of any employment or other contract.

We may amend this Policy at any time without consultation.

This policy covers the main school and "the Hive".

Signed: …….. Date: ……

1. LEGAL FRAMEWORK

1.1 This policy has due regard to legislation including, but not limited to, the following:

- The Regulation of Investigatory Powers Act 2000
- The Protection of Freedoms Act 2012
- The General Data Protection Regulation
- The Freedom of Information Act 2000
- The Education (Pupil Information) (England) Regulations 2005 (as amended in 2016)
- The Freedom of Information and Data Protection (Appropriate Limit and Fees) Regulations 2004
- The School Standards and Framework Act 1998
- The Children Act 1989
- The Children Act 2004
- The Equality Act 2010

1.2 This policy has been created with regard to the following statutory and nonstatutory guidance:

- Home Office (2013) 'The Surveillance Camera Code of Practice'
- ICO (2017) 'Overview of the General Data Protection Regulation (GDPR)'
- ICO (2017) 'Guide to the General Data Protection Regulation'
- ICO (2017) 'In the picture: A data protection code of practice for surveillance cameras and personal information'

1.3 This policy operates in conjunction with the following school policies

- Photography and Videos at School Policy
- E-Safety Policy
- Freedom of Information Policy
- GDPR Data Protection Policy

2. DEFINITIONS

2.1 For the purpose of this policy a set of definitions will be outlined, in accordance with the surveillance code of conduct:

- Surveillance – monitoring the movements and behaviour of individuals; this can include video, audio or live footage. For the purpose of this policy only video and audio footage will be applicable.
- Overt surveillance – any use of surveillance for which authority does not fall under the Regulation of Investigatory Powers Act 2000.

- Covert surveillance – any use of surveillance which is intentionally not shared with the subjects it is recording. Subjects will not be informed of such surveillance.

2.2 All Saints' CE Primary School does not condone the use of covert surveillance when monitoring the school's staff, pupils and/or volunteers. Covert surveillance will only be operable in extreme circumstances.

2.3 Any overt surveillance footage will be clearly signposted around the school.

2.4 For the purposes of this policy, the following terms have the following meanings

CCTV means fixed and domed cameras designed to capture and record images of individuals and property.

Data is information which is stored electronically or in certain paper-based filing systems and may include Personal Data. In respect of CCTV, this generally means video images. It may also include static pictures such as printed screen shots.

Data Controllers means the person or organisation that determines when, why and how to process Personal Data. We are the Data Controller of all Personal Data used in multi-academy trust for our own commercial and educational purposes.

Data Processors means the person or organisation that is not a Data User that Processes Personal Data on our behalf and in accordance with our instructions (for example, a supplier which handles Personal Data on our behalf).

Data Users are those of our employees whose work involves Processing Personal Data. This will include those whose duties are to operate CCTV cameras and other surveillance systems to record, monitor, store, retrieve and delete images. Data users must protect the data they handle in accordance with this Policy and our Privacy Standard and Privacy Policy.

Data Subjects means a living, identified or identifiable individual about whom we hold Personal Data as a result of the operation of our CCTV (or other surveillance systems).

Personal Data means any information identifying a Data Subject or information relating to a Data Subject that we can identify (directly or indirectly) from that data alone or in combination with other identifiers we possess or can reasonably access. This will include video images of Data Subjects.

Processing means any activity that involves the use of Personal Data. It includes obtaining, recording or holding the data, or carrying out any operation or set of operations on the data including organising, amending, retrieving, using, disclosing, erasing or destroying it. Processing also includes transmitting or transferring Personal Data to third parties.

Surveillance systems means any devices or systems designed to monitor or record images of individuals or information relating to individuals. The term includes CCTV systems as well as any technology that may be introduced in the future such as automatic number plate

recognition (ANPR), body worn cameras, unmanned aerial systems and any other systems that capture information of identifiable individuals or information relating to identifiable individuals.

3. ROLES AND RESPONSIBILITIES

3.1 The role of the data protection officer (DPO) in respect of CCTV includes:

- Ensuring that all data controllers at the school handle and process surveillance and CCTV footage in accordance with data protection legislation.
- Ensuring that surveillance and CCTV footage is obtained in line with legal requirements.
- Ensuring that surveillance and CCTV footage is destroyed in line with legal requirements when it falls outside of its retention period.
- Informing data subjects of how their data captured in surveillance and CCTV footage will be used by the school, their rights for the data to be destroyed and the measures implemented by the school to protect individuals' personal information.

All Saints' CE Primary School as the corporate body, is the data controller.

The Governing Board of All Saints' CE Primary School therefore has overall responsibility for ensuring that records are maintained, including security and access arrangements in accordance with regulations.

3.2 The SBM deals with the day-to-day matters relating to data protection and thus, for the benefit of this policy will act as the data controller.

3.3 The role of the data controller includes:

- Processing surveillance and CCTV footage legally and fairly.
- Collecting surveillance and CCTV footage for legitimate reasons and ensuring that it is used accordingly.
- Collecting surveillance and CCTV footage that is relevant, adequate and not excessive in relation to the reason for its collection.
- Ensuring that any surveillance and CCTV footage identifying an individual is not kept for longer than is necessary.
- Protecting footage containing personal data against accidental, unlawful destruction, alteration and disclosure – especially when processing over networks.

3.4 The role of the Head teacher includes:

- Meeting with the DPO to decide where CCTV is needed to justify its means.
- Conferring with the DPO with regard to the lawful processing of the surveillance and CCTV footage.

- Reviewing the Surveillance and CCTV Policy to ensure it is compliant with current legislation.
- Monitoring legislation to ensure the school is using surveillance fairly and lawfully.
- Communicating any changes to legislation with all members of staff.

4. PURPOSE AND JUSTIFICATION

4.1 The school will only use surveillance cameras for the safety and security of the school and its staff, pupils and visitors.

4.2 Surveillance will be used as a deterrent for violent behaviour and damage to the school.

4.3 The school will only conduct surveillance as a deterrent and under no circumstances will the surveillance and the CCTV cameras be present in any changing facility.

4.4 If the surveillance and CCTV systems fulfil their purpose and are no longer required the school will deactivate them.

5. THE DATA PROTECTION PRINCIPLES

Data collected from surveillance and CCTV will be:

- Processed lawfully, fairly and in a transparent manner in relation to individuals.
- Collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public 27 interest, scientific or historical research purposes or statistical purposes shall not be considered to be incompatible with the initial purposes.
- Adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed.
- Accurate and, where necessary, kept up-to-date; every reasonable step will be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay.
- Kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods, insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes, subject to implementation of the appropriate technical and organisational measures required by the GDPR in order to safeguard the rights and freedoms of individuals.
- Processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against

accidental loss, destruction or damage, using appropriate technical or organisational measures.

6. OBJECTIVES

The surveillance system will be used to:

- Maintain a safe environment.
- Ensure the welfare of pupils, staff and visitors.
- Deter criminal acts against persons and property.
- Assist the police in identifying persons who have committed an offence.

7. PROTOCOLS

7.1 The surveillance system will be registered with the ICO in line with data protection legislation.

7.2 The surveillance system is a closed digital system.

7.3 Warning signs have been placed throughout the premises where the surveillance system is active, as mandated by the ICO's Code of Practice.

7.4 The surveillance system has been designed for maximum effectiveness and efficiency; however, the school cannot guarantee that every incident will be detected or covered and 'blind spots' may exist.

7.5 The surveillance system will not be trained on individuals unless an immediate response to an incident is required.

7.6 The surveillance system will not be trained on private vehicles or property outside the perimeter of the school.

8. SECURITY

8.1 Access to the surveillance system, software and data will be strictly limited to authorised operators and will be password protected.

8.2 The school's authorised CCTV system operators are:

- Headteacher
- Deputy Headteacher.
- School Business Manager
- IT Manager

8.3 The main control facility is kept secure and locked when not in use.

8.4 If, in exceptional circumstances, covert surveillance is planned, or has taken place, copies of the Home Office's authorisation forms will be completed and retained.

8.5 Surveillance and CCTV systems will be tested for security flaws termly to ensure that they are being properly maintained at all times.

8.6 Surveillance and CCTV systems will not be intrusive.

8.7 Any unnecessary footage captured will be securely deleted from the school system.

8.8 Any cameras that present faults will be repaired immediately as to avoid any risk of a data breach.

8.9 Visual display monitors are located in the designated area.

9. PRIVACY BY DESIGN

9.1 A DPIA will be carried out prior to the installation of any additional surveillance and CCTV system.

9.2 If the DPIA reveals any potential security risks or other data protection issues, the school will ensure they have provisions in place to overcome these issues.

9.3 Where the school identifies a high risk to an individual's interests, and it cannot be overcome, the school will consult the ICO before they use the additional CCTV, and the school will act on the ICO's advice.

9.4 The school will ensure that the installation of the surveillance and CCTV systems will always justify its means.

9.5 If the use of a surveillance and CCTV system is too privacy intrusive, the school will seek alternative provision.

10. CODE OF PRACTICE

10.1 The school understands that recording images of identifiable individuals constitutes as processing personal information, so it is done in line with data protection principles.

10.2 The school notifies all pupils, staff and visitors of the purpose for collecting surveillance data via notice boards, letters and emails.

10.3 CCTV cameras are only placed where they do not intrude on anyone's privacy and are necessary to 29 fulfil their purpose.

10.4 All surveillance footage will be kept for 28 days for security purposes; the head teacher and the data controller are responsible for keeping the records secure and allowing access.

10.5 The school has a surveillance system for the purpose of the prevention and detection of crime and the promotion of the health, safety and welfare of staff, pupils and visitors.

10.6 The surveillance and CCTV system is owned by the school and images from the system are strictly controlled and monitored by authorised personnel only.

10.7 The school will ensure that the surveillance and CCTV system is used to create a safer environment for staff, pupils and visitors to the school, and to ensure that its operation is consistent with the obligations outlined in data protection legislation. The policy is available from the school's website.

10.8 The surveillance and CCTV system will:

- Be designed to take into account its effect on individuals and their privacy and personal data.
- Be transparent and include a contact point, the DPO, through which people can access information and submit complaints.
- Have clear responsibility and accountability procedures for images and information collected, held and used.
- Have defined policies and procedures in place which are communicated throughout the school.
- Only keep images and information for as long as required.
- Restrict access to retained images and information with clear rules on who can gain access.
- Consider all operational, technical and competency standards, relevant to the surveillance and CCTV system and its purpose, and work to meet and maintain those standards in accordance with the law.
- Be subject to stringent security measures to safeguard against unauthorised access.
- Be regularly reviewed and audited to ensure that policies and standards are maintained.
- Only be used for the purposes for which it is intended, including supporting public safety, the protection of pupils, staff and volunteers, and law enforcement.

10.9 Be accurate and well maintained to ensure information is up-to-date

11. ACCESS

11.1 Under the GDPR, individuals have the right to obtain confirmation that their personal information is being processed.

11.2 All disks containing images belong to, and remain the property of, the school.

11.3 Individuals have the right to submit an SAR to gain access to their personal data in order to verify the lawfulness of the processing.

11.4 The school will verify the identity of the person making the request before any information is supplied.

11.5 A copy of the information will be supplied to the individual free of charge; however, the school may impose a 'reasonable fee' to comply with requests for further copies of the same information.

11.6 Where a SAR has been made electronically, the information will be provided in a commonly used electronic format.

11.7 Requests by persons outside the school for viewing or copying disks, or obtaining digital recordings, will be assessed by the head teacher, who will consult the DPO, on

a case-by-case basis with close regard to data protection and freedom of information legislation.

11.8 Where a request is manifestly unfounded, excessive or repetitive, a reasonable fee will be charged.

11.9 All fees will be based on the administrative cost of providing the information.

11.10 All requests will be responded to without delay and at the latest, within one month of receipt

11.11 In the event of numerous or complex requests, the period of compliance will be extended by a further two months. The individual will be informed of this extension, and will receive an explanation of why the extension is necessary, within one month of the receipt of the request.

11.12 Where a request is manifestly unfounded or excessive, the school holds the right to refuse to respond to the request. The individual will be informed of this decision and the reasoning behind it, as well as their right to complain to the ICO and to a judicial remedy, within one month of the refusal.

11.13 In the event that a large quantity of information is being processed about an individual, the school will ask the individual to specify the information the request is in relation to.

11.14 It is important that access to, and disclosure of, the images recorded by surveillance and CCTV footage is restricted and carefully controlled, not only to ensure that the rights of individuals are preserved, but also to ensure that the chain of evidence remains intact, should the images be required for evidential purposes.

11.15 Releasing the recorded images to third parties will be permitted only in the following limited and prescribed circumstances, and to the extent required or permitted by law:

- The police – where the images recorded would assist in a specific criminal inquiry
- Prosecution agencies – such as the Crown Prosecution Service (CPS)
- Relevant legal representatives – such as lawyers and barristers
- Persons who have been recorded and whose images have been retained where disclosure is required by virtue of data protection legislation and the Freedom of Information Act 2000

11.16 Requests for access or disclosure will be recorded and the head teacher will make the final decision as to whether recorded images may be released to persons other than the police.

12. MONITORING AND REVIEW

12.1 This policy will be monitored and reviewed every two years by the DPO, Head teacher and the Chair of Governors to ensure that it meets legal requirements, relevant guidance published by the ICO and industry standards. A breach of this

Policy may, in appropriate circumstances, be treated as a disciplinary matter. Following investigation, a breach of this Policy may be regarded as misconduct leading to disciplinary action, up to and including dismissal.

12.2 The Head teacher and DPO will be responsible for monitoring any changes to legislation that may affect this policy, and make the appropriate changes accordingly.

12.3 The Head teacher will communicate changes to this policy to all members of staff.

12.4 The scheduled review date for this policy is December 2020 and reviewed thereafter every three years. The school will update/amend other policies linked to this policy

- Data Protection Policy - annually reviewed
- Data Retention Policy – every 3 years
- Data Privacy Notices Pupil- annually reviewed
- Data Privacy Notices Staff - annually reviewed
- Data Privacy Notices Governors- annually reviewed
- Data Privacy Notices Visitors- annually reviewed
- Data Privacy Notices Job Applicants- annually reviewed