CCTV Policy

Statement of intent:
At Burley Oaks Primary School, we respect and value all children and are committed to providing a caring, friendly and safe environment for all our pupils so they can learn, in a relaxed and secure atmosphere. We believe every pupil should be able to participate in all school activities in an enjoyable and safe environment and be protected from harm. This is the responsibility of every adult employed by, or invited to deliver services at Burley Oaks Primary School. We recognise our responsibility to safeguard all who access school and promote the welfare of all our pupils by protecting them from physical, sexual and emotional abuse, neglect and bullying.

The main priority is to prevent an emergency from occurring in the setting; however, this is sometimes, unfortunately, out of the hands of the school. In an emergency, staff members at Burley Oaks Primary School will endeavour to take all reasonable actions in order to ensure the safety of pupils.
The procedures outlined in this policy aim to minimise disruption to the learning environment whilst ensuring the safety of all pupils, staff members and visitors.

This policy was agreed in May 2025 and will be reviewed in May 2028.

Chair of Governors **Date 1 May 2025**

Headteacher **Date 1 May 2025**

Contents:

Statement of intent

1. Legal framework
2. Definitions
3. Roles and responsibilities
4. Purpose and justification
5. The data protection principles
6. Objectives
7. Protocols
8. Security
9. Privacy by design
10. Code of practice
11. Access
12. Monitoring and review

Statement of intent

At Burley Oaks, 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 school and its members.

The purpose of this policy is to manage and regulate the use of the surveillance and CCTV systems at the school and ensure that:

- We comply with the GDPR, effective 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

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.

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
- Data Protection Act 2018
- 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 non-statutory guidance:

- Home Office (2021) 'The Surveillance Camera Code of Practice'
- ICO (2021) 'Guide to the UK General Data Protection Regulation (UK GDPR)'
- ICO (2017) 'In the picture: A data protection code of practice for surveillance cameras and personal information'
- ICO (2022) 'Video Surveillance'

1.3. This policy operates in conjunction with the following school policies:

- E-safeguarding Policy
- Freedom of Information Policy
- School Security 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 and live streams. For the purpose of this policy only video and audio footage will be applicable.
- **Overt surveillance** – Surveillance which is clearly visible and signposted around the school and 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. Burley Oaks does not condone the use of covert surveillance when monitoring the school's staff, pupils and/or volunteers.

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

2.4. **Biometric data** – data which is related to the physiological characteristics of a person, which confirm the unique identification of that person, such as fingerprint recognition, facial recognition (FRT), or iris recognition.

Definition of Acronyms

CCTV – Closed Circuit Television
DPIA – Data Protection Impact Assessment
DPO – Data Protection Officer
FRT – Facial Recognition Technology
GDPR – General Data Protection
ICO – Information Commissioner's Office
SAR – Subject Access Request

3. Roles and responsibilities

3.1. The role of the data protection officer (DPO) includes:

- Dealing with freedom of information requests and subject access requests (SAR) in line with legislation, including the Freedom of Information Act 2000.
- 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 consent is clear, positive and unambiguous. Pre-ticked boxes and answers inferred from silence are non-compliant with the GDPR.
- Ensuring that surveillance and CCTV footage is destroyed in line with legal requirements when it falls outside of its retention period.
- Keeping comprehensive and accurate records of all data processing activities, including surveillance and CCTV footage, detailing the purpose of the activity and making these records public upon request.
- 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.
- Preparing reports and management information on the school's level of risk related to data protection and processing performance.
- Reporting to the highest management level of the school, e.g. the governing board.
- Abiding by confidentiality requirements in relation to the duties undertaken while in the role.
- Monitoring the performance of the school's data protection impact assessment (DPIA) and providing advice where requested.
- Presenting reports regarding data processing at the school to senior leaders and the governing board.

3.2. Burley Oaks, as the corporate body, is the data controller. The governing board of Burley Oaks therefore has overall responsibility for ensuring that records are maintained, including security and access arrangements in accordance with regulations.

3.3. 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.

3.4. 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.

3.5. The role of the headteacher 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 school classrooms or 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. Data protection

5.1. Data collected from surveillance and CCTV will be:

- Processed lawfully, as determined by a DPIA, or from advice from the DPO. In less common circumstances, lawful processing will be determined by a legitimate interests assessment (LIA).
- Processed fairly, in a manner that people would reasonably expect, and taking into account advancements in technology that may not be anticipated by some people.
- Processed in a transparent manner, meaning that people are informed when their data is being captured.
- Collected for specified and legitimate purposes – data will not be processed further in a manner that is incompatible with the following purposes:
- Further processing for archiving data in the public interest
- Scientific or historical research
- Statistical purposes n
- 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 is inaccurate, having regard to the purposes for which they are processed, is 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 is processed.
- 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.
- Held for no longer than one month
- Justifiable, proportionate, and able to address specific needs

5.2. The use of surveillance cameras, CCTV, and biometric systems, will be critically analysed using a DPIA, in consultation with the DPO.

5.3. A DPIA will be carried out prior to the installation of any surveillance, CCTV, or biometric system. A DPIA will:

- Describe the nature, scope, context, and purposes of the processing.
- Assess necessity, proportionality, and compliance measures.
- Identify and assess risks to individuals.
- Identify any additional measures to mitigate those risks.

5.4. Sensitive data obtained via biometric technology will be processed via special conditions (listed in Article 9 of the UK GDPR).

5.5 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.

5.6. 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 CCTV, and the school will act on the ICO's advice.

5.7. The school will ensure that the installation of the surveillance and CCTV systems will always justify its means. If the use of a surveillance and CCTV system is too privacy intrusive, the school will seek amendments.

5.8. Surveillance and CCTV systems will not be intrusive. Pupils, staff and visitors will be made aware of the following:

- Whenever they are being monitored by a surveillance camera system
- Who is undertaking the activity
- The purpose for which the associated information is being used

5.9. The use of any video conferencing technology will be fair and transparent. Any pupils and staff who are part of any video conference calls will be informed of its purpose, and recording and publication of any video to an indefinite audience will be consented to and will not be used outside of the intended purpose.

6. Protocols

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

6.2. The surveillance system is a closed digital system.

6.3. Warning signs have been placed throughout the premises where the surveillance system is active, as mandated by the ICO's Code of Practice. Warning signs will be more prominent in areas where surveillance is less expected to be in operation, and when using systems that can capture a large amount of personal data at one time.

6.4. 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.

6.5. The surveillance system will not be used to focus on a particular group or individual unless an immediate response to an incident is required.

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

7. Security

7.1. Access to the surveillance system, software and data will be strictly limited to authorised operators, and will be password protected, and where appropriate, will be encrypted.

7.2. In exceptional cases where large amounts of information need to be collected and retained, the school will consider using cloud storage. This will be secure and only accessible to authorised individuals.

7.3. The school's authorised CCTV system operators are:

- Emma Learmonth, Headteacher
- Jenni Warbrick, data controller
- Karen Armitage, data processor
- Libby Harris, data processor

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

7.5. 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.

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

7.7. The DPO and headteacher will decide when to record footage, e.g. a continuous loop outside the school grounds to deter intruders.

7.8. Staff will be trained in security procedures, and sanctions will be put in place for those who misuse security system information. Staff will be made aware that they could be committing a criminal offence if they do this.

7.9. The ability to produce copies of information will be limited to the appropriate staff.

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

7.11. Each system will have a separate audio and visual system that can be run independently of one another. The school will not record audio unless it has:

- Identified a particular need or issue and can evidence that this need must be addressed by audio recording;
- Considered other less privacy intrusive methods of achieving this need;
- Reviewed the other less privacy intrusive methods and concluded that these will not appropriately address the identified issue and the only way to do so is via the use of audio recording.

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

7.13. A visual display monitor is located in the main office.

8. Code of practice

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

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

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

8.4. All surveillance footage will be kept for one month for security purposes; the headteacher and the data controller are responsible for keeping the records secure and allowing access.

8.5. 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.

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

8.7. 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.

8.8. 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 which enables people to request information and submit complaints via the DPO.
- 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.
- Be accurate and well maintained to ensure information is up-to-date.

9. Access

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

9.2. All disks and hard drives containing images belong to, and remain the property of, the school.

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

9.4. Individuals have the right to have personal data erased if:

- The data is no longer necessary for the original purpose it was collected for.
- They are relying on legitimate interests as a basis for processing, the individual objects to the processing of their data, and there is no overriding legitimate interest to continue the processing.
- The data has been processed unlawfully.
- There is a specific legal obligation.

9.5. There are certain exceptions where the right to erasure cannot be exercised, these include, but are not limited to:

- Where the processing is needed for the performance of a task in the public interest or an official authority.
- Certain research activities.
- Compliance with a specific legal obligation.

9.6. As an alternative to the right of erasure, individuals can limit the way their data is used if they have issues with the content of the data held by the school or they object to way it was processed.

9.7. Data can be restricted by either:

- Moving the data to another processing system.
- Making the data unavailable to users.
- Temporarily removing published data from a website.

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

9.9. 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. The individual will either be provided with a permanent copy of the information or allowed to view the information.

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

9.11. Requests by persons outside the school for viewing or copying disks, or obtaining digital recordings, will be assessed by the headteacher, who will consult the DPO, on a case-by-case basis with close regard to data protection and freedom of information legislation.

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

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

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

9.14 In the event of numerous or complex requests, the period of compliance will be extended by no more than an additional 20 working days. 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.

9.15. 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.

9.16. 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.

9.17 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.

9.18 Where data requests contain the personal data of a separate individual, the rights and freedoms of others will be protected by asking for their consent, or removing specific footage where appropriate.

9.20. 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

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

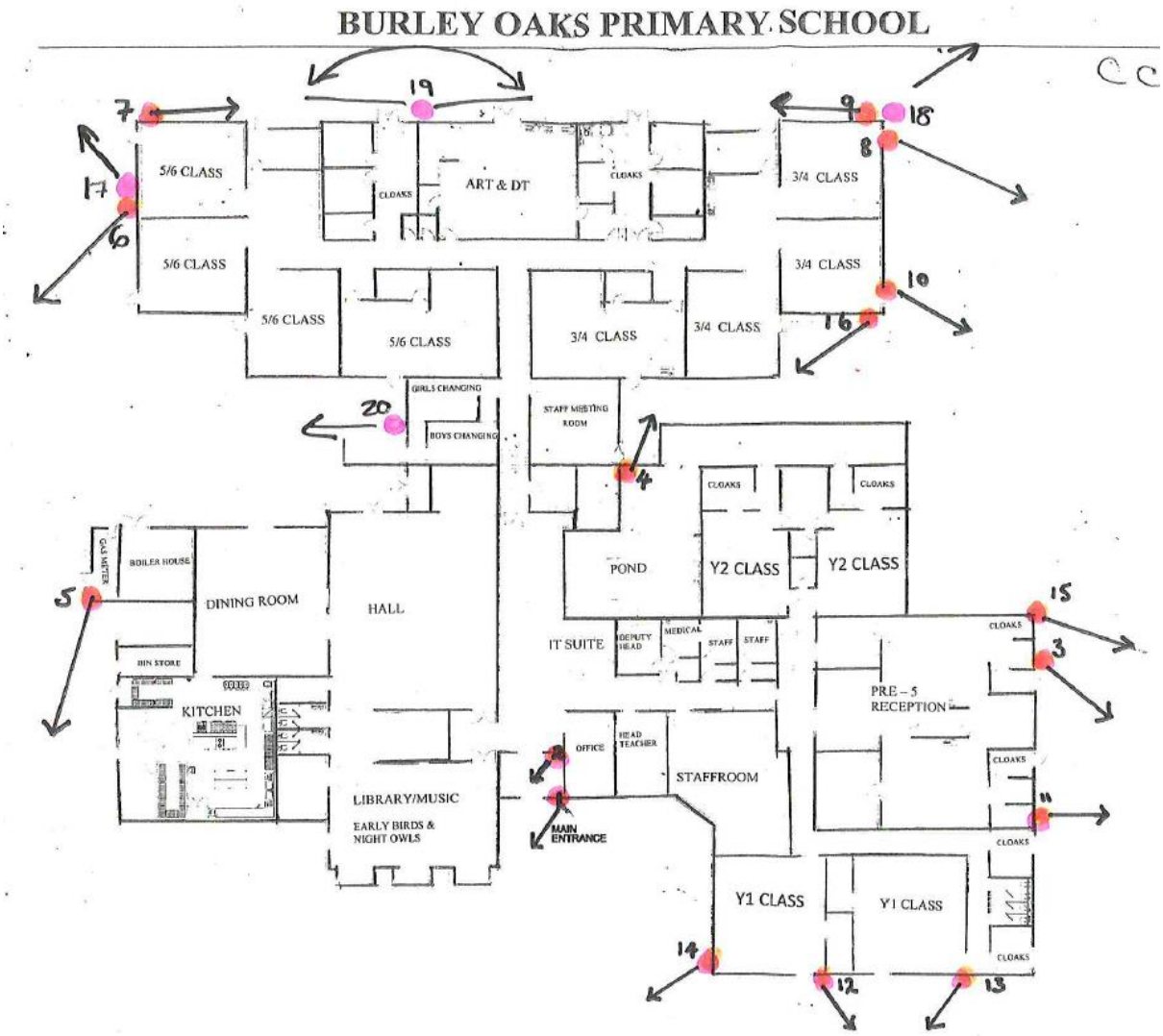
10. Monitoring and review

10.1 This policy will be monitored and reviewed on a three yearly basis by the Business Manager.

10.2 The headteacher will be responsible for monitoring any changes to legislation that may affect this policy, and make the appropriate changes accordingly.

10.3 The headteacher will communicate changes to this policy to all members of staff.

10.4 The scheduled review date for this policy is **May 2028**.

Appendix 1

CCTV Citing