Redbridge Alternative Provision

CCTV Policy

Written by

R Jonker

Written on

February 2025

Due for review on

January 2027

Statement of intent

At Redbridge Alternative Provision (RAP) 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 data protection legislation, including the Data Protection Act 2018 and the General Data Protection Regulation (GDPR).
- 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:

- Taking action to prevent a crime.
- Using images of individuals to detect crime.

1. Legal framework

This policy has due regard to legislation and statutory guidance, 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 (GDPR).
- The 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 2004.
- The Equality Act 2010.

This policy has been created with regard to the following statutory and non- statutory guidance:

- Home Office (2013) 'The Surveillance Camera Code of Practice'.
- Information Commissioner's Office (ICO) (2017) 'Overview of the General Data Protection Regulation (GDPR)'.
- ICO (2017) 'Preparing for the General Data Protection Regulation (GDPR) 12 steps to take now'.
- ICO (2017) 'In the picture: A data protection code of practice for surveillance cameras and personal information'.

2. Definitions

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

- Surveillance –For the purpose of this policy only video footage will be applicable. Surveillance refers to the equipment and associated systems and governance. No surveillance of individuals will be conducted.
- 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. RAP will not under any circumstances employ covert surveillance practices.

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

3. Roles and responsibilities

The role of the Headteacher, Senior Information Risk Owner (SIRO) 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 PRU Management Committee.
- Abiding by confidentiality requirements in relation to the duties undertaken while in the role.
  Monitoring the performance of the school's privacy impact assessment (PIA), and under the GDPR the data protection impact assessment (DPIA), and providing advice where requested.
- Presenting reports regarding data processing at the school to senior leaders and the PRU Management Committee.
- RAP is the data controller. The PRU Management Committee therefore has overall responsibility for ensuring that records are maintained, including security and access arrangements in accordance with regulations.
- The role of the Federation Business Manager (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.

4. Purpose and justification

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

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

Surveillance will be used as a method to investigate incidents and allegations.

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 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

- The surveillance system will be registered with the ICO in line with data protection legislation.
- The surveillance system is a closed digital system which does not record audio.
- Warning signs have been placed throughout the premises where the surveillance system is active, as mandated by the ICO's Code of Practice.
- 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.
- The surveillance system will not be trained on individuals unless an immediate response to an incident is required.
- The surveillance system will not be trained on private vehicles or property outside the perimeter of the school.

8. Security

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

The school's authorised CCTV system operators are:

- Rubert Jonker, Headteacher
- Matthew Knell, Deputy Headteacher

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

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

The Headteacher will decide when to record footage, e.g. a continuous loop will be recorded at each location

Any unnecessary footage captured will be securely deleted from the school system.
Any cameras that present faults will be repaired immediately as to avoid any risk of a data breach.

9. Privacy by design

An Impact Assessment will be undertaken prior to the installation of any additional surveillance and CCTV system equipment.

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

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 alternative provision.

10. Code of practice

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

The school notifies all pupils, staff and visitors of the purpose for collecting surveillance data via signs in the school grounds where cameras are based.

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

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.

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.

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

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

11. Access

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

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

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

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

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.

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

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.

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

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

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

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.

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.

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.

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.

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

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.

12. Monitoring and review

This policy will be monitored and reviewed on a biennial basis, or in light of any changes to relevant legislation by the DPO and the Headteacher.

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

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

Appendix 1: Personal data breach procedure

This procedure is based on guidance on personal data breaches produced by the ICO.

- On finding or causing a breach, or potential breach, the staff member or data processor must immediately notify the DPO.
- The DPO will investigate the report, and determine whether a breach has occurred. To decide, the DPO will consider whether personal data has been accidentally or unlawfully:
    - Lost.
    - Stolen.
    - Destroyed.
    - Altered.
    - Disclosed or made available where it should not have been.
    - Made available to unauthorised people.
- The DPO will alert the Headteacher and the Chair of Committee Members.
- The DPO will make all reasonable efforts to contain and minimise the impact of the breach, assisted by relevant staff members or data processors where necessary. (Actions relevant to specific data types are set out at the end of this procedure).
- The DPO will assess the potential consequences, based on how serious they are, and how likely they are to happen.
- The DPO will work out whether the breach must be reported to the ICO. This must be judged on a case-by-case basis. To decide, the DPO will consider whether the breach is likely to negatively affect people's rights and freedoms, and cause them any physical, material or non-material damage (e.g. emotional distress), including through:
    - Loss of control over their data.
    - Discrimination.
    - Identify theft or fraud.
    - Financial loss.
    - Unauthorised reversal of pseudonymisation (for example, key-coding).
    - Damage to reputation.
    - Loss of confidentiality.
    - Any other significant economic or social disadvantage to the individual(s) concerned
    - If it's likely that there will be a risk to people's rights and freedoms, the DPO must notify the ICO.
- The DPO will document the decision (either way), in case it is challenged at a later date by the ICO or an individual affected by the breach. Documented decisions are stored on the server in each institution.
- Where the ICO must be notified, the DPO will do this via the 'report a breach' page of the ICO website within 72 hours. As required, the DPO will set out:
    - A description of the nature of the personal data breach including, where possible:
        - The categories and approximate number of individuals concerned.
        - The categories and approximate number of personal data records concerned.
    - The name and contact details of the DPO.
    - A description of the likely consequences of the personal data breach.

    - A description of the measures that have been, or will be taken, to deal with the breach and mitigate any possible adverse effects on the individual(s) concerned.
- If all the above details are not yet known, the DPO will report as much as they can within 72 hours. The report will explain that there is a delay, the reasons why, and when the DPO expects to have further information. The DPO will submit the remaining information as soon as possible.
- The DPO will also assess the risk to individuals, again based on the severity and likelihood of potential or actual impact. If the risk is high, the DPO will promptly inform, in writing, all individuals whose personal data has been breached. This notification will set out:
    - The name and contact details of the DPO.
    - A description of the likely consequences of the personal data breach.
    - A description of the measures that have been, or will be, taken to deal with the data breach and mitigate any possible adverse effects on the individual(s) concerned.
- The DPO will notify any relevant third-parties who can help mitigate the loss to individuals – for example, the Police, insurers, banks or credit card companies.
- The DPO will document each breach, irrespective of whether it is reported to the ICO. For each breach, this record will include the:
    - Facts and cause.
    - Effects.
    - Action taken to contain it and ensure it does not happen again (such as establishing more robust processes or providing further training for individuals).

  Records of all breaches will be stored on the institutions server in a secure folder names GDPR Breach Reports. The DPO and Headteacher will meet to review what happened and how it can be stopped from happening again. This meeting will happen as soon as reasonably possible.

Actions to minimise the impact of data breaches

We will take the actions set out below to mitigate the impact of different types of data breach, focusing especially on breaches involving particularly risky or sensitive information. We will review the effectiveness of these actions and amend them as necessary after any data breach.

Set out the relevant actions you will take for different types of risky or sensitive personal data processed by your school. For example:

Sensitive information being disclosed via email (including safeguarding records)

- If special category data (sensitive information) is accidentally made available via email to unauthorised individuals, the sender must attempt to recall the email as soon as they become aware of the error.
- Members of staff who receive personal data sent in error must alert the sender and the DPO as soon as they become aware of the error.
- If the sender is unavailable or cannot recall the email for any reason, the DPO will ask the ICT or Network Manager to recall it.
- In any cases where the recall is unsuccessful, the DPO will contact the relevant unauthorised individuals who received the email, explain that the information was sent in error, and request that those individuals delete the information and do not share, publish, save or replicate it in any way.
- The DPO will ensure we receive a written response from all the individuals who received the data, confirming that they have complied with this request.
- The DPO will carry out an internet search to check that the information has not been made public; if it has, we will contact the Publisher/Website Owner or Administrator to request that the information is removed from their website and deleted.

Other types of breach that you might want to consider could include:

- Details of pupil premium interventions for named children being published on the school website.
- Non-anonymised pupil exam results or staff pay information being shared with Committee Members.
- A school laptop containing non-encrypted sensitive personal data being stolen or hacked. The school's cashless payment provider being hacked and Parents'/Carers' financial details stolen.

Appendix 2: Records Management Policy and Retention Schedule

Records Management Policy

RAP collects and uses personal information about staff, pupils, Parents/Carers and other individuals who come into contact with the school. This information is gathered in order to enable it to provide education and other associated functions. In addition, there may be a legal requirement to collect and use information to ensure that the school complies with its statutory obligations.

The school recognises that by efficiently managing its records, it will be able to comply with its legal and regulatory obligations and to contribute to the effective overall management of the institution. Records provide evidence for protecting the legal rights and interests of the school, and provide evidence for demonstrating performance and accountability. This document provides the policy framework through which this effective management can be achieved and audited. The school has adopted the Information Management ToolKit for Schools created by the IRMS (information and Records Management Society) and adheres to its principles and guidance, including the retention schedule for school records. A full copy of the Information Management ToolKit is available on the school website.

1. Scope of the policy

1.1 This policy applies to all records created, received or maintained by staff of the school in the course of carrying out its functions.

1.2 Records are defined as all those documents which facilitate the business carried out by the school and which are thereafter retained (for a set period) to provide evidence of its transactions or activities. These records may be created, received or maintained in hard copy or electronically.

1.3 A small percentage of the school's records may be selected for permanent preservation as part of the institution's archives and for historical research.

2. Responsibilities

2.1 The school has a corporate responsibility to maintain its records and record keeping systems in accordance with the regulatory environment. The person with overall responsibility for this policy is the Headteacher.

2.2 The person responsible for records management in the school will give guidance for good records management practice and will promote compliance with this policy so that information will be retrieved easily, appropriately and in a timely way. They will also monitor compliance with this policy by surveying at least annually to check if records are stored securely and can be accessed appropriately.

2.3 Individual staff and employees must ensure that records for which they are responsible are accurate, and are maintained and disposed of in accordance with the school's records management guidelines.