Netherhall School
An Ambitious, Caring Community

CCTV PROCEDURES

Adopted by Netherhall School Governing Body On: 1 September 2023

Signed:  **(Neil Watt, Chair of Governors)**

Date by which the procedure was last reviewed: September 2023

Anticipated review date: September 2024

Equality Act 2010
Our school is committed to equality both as an employer and a service provider. We welcome our general duty under the Equality Act 2010 to eliminate discrimination, advance equality of opportunity and foster good relations. In addition we recognise our specific duties to publish information every year about our school population; explain how we have due regard for equality; publish equality objectives which show how we plan to tackle particular inequalities and reduce or remove them.

We recognise our duty to ensure no-one experiences harassment, less favourable treatment or discrimination because of their age, any disability they may have, their ethnicity, colour or national origin, their gender identity or reassignment, their marital or civil partnership status, being pregnant or having recently had a baby, their religion or belief, their sexual identity and orientation.

We also welcome our duty under the Education and Inspections Act 2006 to promote community cohesion and British values.

REVIEW SHEET

The information in the table below details earlier versions of this document with a brief description of each review and how to distinguish amendments made since the previous version date (if any).

Version Number	Version Description	Date of Revision
2	Significant rewrite in line with the ICO 'In the Picture: A Data Protection Code of Practice for Surveillance Cameras and Personal Data' (May 2015)	September 2015
3	Minor amendment	February 2016
4	GDPR May 2018	May 2018
5	Removed sentence in Section 12 which referred to itself	April 2019
6	Various amendments due to complete rewire works and new CCTV system.	September 2021

Contents

CCTV PROCEDURES

References and Useful Links

The Information Commissioners Office 'In the Picture: A Data Protection Code of Practice for Surveillance Cameras and Personal Data, May 2015
The Information Commissioners Office (ICO) Website
Information Commissioner's Office 'Conducting Privacy Impact Assessments' Code of Practice
Information Commissioner's Office 'Subject Access Code of Practice'.
Regulation of Investigatory Powers Act (RIPA) 2000
Data Protection Act 1998

1. INTRODUCTION

The purpose of these Procedures is to regulate the use of CCTV and its associated technology in the monitoring of both the internal and external environs of the premises under the remit of Netherhall School, hereinafter referred to as 'the school'.

The CCTV system is owned and operated by the school, the deployment of which is determined by the school senior leadership team.

These procedures follow the Information Commissioners Office 'In the Picture: A Data Protection Code of Practice for Surveillance Cameras and Personal Data' (May 2015); the General Data Protection Regulation (2018) guidelines and the School General Data Protection Policy, both of which are held separately.

These Procedures will be subject to regular review to include consultation as appropriate with interested parties.

New CCTV systems will be introduced in consultation with staff, the school senior leadership team, students and parents/carers. Where systems are already in operation, their operation will be reviewed regularly in consultation with staff, the school senior leadership team, students and parents/carers.

1.1 Exemptions

The use of surveillance systems for limited household purposes is exempt from the GDPR e.g. a video of a child in a nativity play recorded for the parent/carer's own family use is not covered by the GDPR.

The covert surveillance activities of public authorities (refer to Section 7) are not covered here because they are governed by the Regulation of Investigatory Powers Act (RIPA) 2000. This type of recording is covert and directed at an individual or individuals.

The use of conventional cameras (not CCTV) by the news media or for artistic purposes, such as for film making, are not covered by these procedures as an exemption within the GDPR applies to activities relating to journalistic, artistic and literary purposes.

2. OBJECTIVES OF THE CCTV SCHEME

The system comprises a number of fixed and dome cameras located around the site both internally and externally for the purpose of enhancing security of the building and its associated equipment as well as creating a mindfulness among the occupants, at any one time, that a surveillance security system is in operation within and/or in the external environs of the premises during both the daytime and hours of darkness. CCTV surveillance at the school is intended for the purposes of:

- Protecting the school buildings and assets, both during and after school hours.
- Increasing the personal safety of staff, students and visitors.
- Reducing the fear of crime.
- Reducing the risk of bullying.
- Reducing the incidence of crime and anti-social behaviour (including theft and vandalism).
- Supporting the Police in a bid to deter and detect crime.
- Assisting in identifying, apprehending and prosecuting offenders.
- Protecting members of the public; and

- ensuring that the school rules are respected so that the school can be properly managed.

3. GENERAL PRINCIPLES

The school as the corporate body has a statutory responsibility for the protection of its property, equipment and other plant as well providing a sense of security to its employees, students and invitees to its premises. The school owes a duty of care under the provisions of the Health and Safety at Work etc. Act, 1974 and associated legislation and utilises CCTV systems and their associated monitoring and recording equipment as an added mode of security and surveillance for the purpose of enhancing the quality of life of the school community by integrating the best practices governing the public and private surveillance of its premises. The use of CCTV, and the associated images and any sound recordings is covered by the General Data Protection Regulation 2018. These Procedures outline the school's use of CCTV and how it complies with the regulation. The school will treat the system and all information, documents and recordings obtained and used as data which are protected by the Act.

The school complies with the Information Commissioner's Office (ICO) CCTV Code of Practice to ensure it is used responsibly and safeguards both trust and confidence in its continued use. The ICO 'In the Picture: A Data Protection Code of Practice for Surveillance Cameras and Personal Data, May 2015 can be found at https://ico.org.uk/media/1542/cctv-code-of-practice.pdf

The Head teacher is responsible for all day-to-day General Data Protection matters, and he will be responsible for ensuring that all members of staff and relevant individuals abide by these procedures, and for developing and encouraging good information handling within the school. The school is registered as a Data Controller on the Data Protection Register held by the Information Commissioner. Notification to the ICO is renewed annually.

All authorised operators and employees with access to images are aware of the procedures that need to be followed when accessing the recorded images and sound. All operators are trained by the school data controller in their responsibilities under these CCTV Procedures. Staff using the surveillance system or information have been trained to ensure they comply with these procedures. In particular, they have been made aware of:

- What the school's arrangements are for recording and retaining information.
- How to handle the information securely.
- What to do if they receive a request for information, for example, from the police.
- How to recognise a subject access request and what to do if they receive one.

Monitoring for security purposes will be conducted in a professional, ethical and legal manner and any diversion of the use of CCTV security technologies and personnel for other purposes is prohibited e.g. monitoring of political or religious activities, or employee and/or student evaluations that would undermine the acceptability of the resources for use regarding critical safety and security objectives.

CCTV monitoring of public areas for security purposes will be conducted in a manner consistent with all existing policies adopted by the school including the General Data Protection Policy, Single Equality Scheme and Whole School Behaviour Policy (incorporating Anti-Bullying and Harassment strategies) etc.

Our procedures for video monitoring prohibit monitoring based on the characteristic and classification contained in Equality and other related legislation, for example race, gender, sexual orientation, national origin, disability etc. The system is in place to monitor suspicious behaviour and not individual characteristics.

Video monitoring of public areas for security purposes is limited to uses that do not violate the reasonable expectation of privacy as defined by Law.

Consideration will be given to both staff and students regarding possible invasions of privacy and confidentiality due to the location of a particular CCTV camera or associated equipment. The Head teacher will ensure that all areas being monitored are not in breach of an enhanced expectation of the privacy of individuals within the school and be mindful that no such infringement is likely to take place. The camera control will be monitored to ensure it is not in breach of the intrusion on intimate behaviour by persons in public changing and toilet areas.

Cameras will be used to monitor activities within the school and its car parks and other public areas to identify criminal activity actually occurring, anticipated, or perceived, and for the purpose of securing the safety and wellbeing of the school, together with its visitors.

Staff have been instructed that static cameras are not to focus on private homes, gardens and other areas of private property. Unless an immediate response to events is required, staff must not direct cameras at an individual, their property or a specific group of individuals, without an authorisation being obtained for Directed Surveillance to take place, as set out in the Regulation of Investigatory Power Act 2000 (RIPA).

The head teacher will approve any temporary cameras to be used during special events that have particular security requirements and ensure their withdrawal following such events. (Temporary cameras do not include mobile video equipment or hidden surveillance cameras used for criminal investigations).

When a zoom facility on a camera is being used, a second person will be present with the camera operator to guarantee that there is no unwarranted invasion of privacy.

Materials or knowledge secured as a result of CCTV will not be used for any commercial purpose. Data will only be released to the media for use in the investigation of a specific crime and with the written authority of the police. Data will never be released to the media for purposes of entertainment.

The planning and design have endeavoured to ensure that the surveillance scheme will give maximum effectiveness and efficiency, but it is not possible to guarantee that the system will cover or detect every single incident taking place in the areas of coverage.

Information obtained through the CCTV system may only be released when authorised by the Head teacher following consultation with the Chair of the Governing Body. Any requests for CCTV recordings/images from the Police will be fully recorded. If a law enforcement authority is seeking a recording for a specific investigation, any such request made should be made in writing.

4. JUSTIFICATION OF USE FOR CCTV

4.1 Visual recording

The General Data Protection Regulation requires that data is "adequate, relevant and not excessive" for the purpose for which it is collected. This means that the school needs to be able to justify the obtaining and use of personal data by means of a CCTV system by conducting a Privacy Impact Assessment (PIA) – refer to the Information Commissioner's Office 'Conducting Privacy Impact Assessments' Code of Practice https://ico.org.uk/media/for-organisations/documents/1595/pia-code-of-practice.pdf . We have considered the privacy issues involved with using surveillance systems and have concluded that their use is necessary and proportionate and address a pressing need that we have identified. We have considered less privacy intrusive methods of achieving this need where possible.

The use of CCTV to control the perimeter of the school buildings and entrances/exits for security purposes has been deemed to be justified by the Senior Leadership Team. The system is intended to capture images of intruders or of individuals damaging property or removing goods without authorisation for example.

In other areas of the school where CCTV has been installed, e.g. hallways, stairwells, locker areas, etc. the Head teacher has demonstrated that there is a proven risk to security and/or health & safety and that the installation of CCTV is proportionate in addressing such issues that have arisen prior to the installation of the system.

CCTV systems will not be used to monitor normal teacher/student classroom activity in school.

4.2 CCTV controls

The school has been installed with a completely new CCTV system and operates 24 hours per day at multiple locations around the site. The CCTV is now operated online with the Head Teacher, Business Manager, Safeguarding lead and Facilities Manager have access to the system if required, as the cameras only show images that should not be seen by the public. The

Head teacher will regularly check and confirm the efficiency of the system and in particular that the equipment is properly recording and that cameras are functional.

- Unless an immediate response to events is required, the chosen members of staff above must not direct cameras at an individual or a specific group of individuals.
- Any visit may be immediately curtailed if prevailing operational requirements make this necessary.
- If out of hours emergency maintenance arises, the chosen members of staff must be satisfied of the identity and purpose of contractors before allowing entry.
- Other administrative functions will include maintaining video data and hard disc space, filing and maintaining occurrence and system maintenance logs.
- Emergency procedures will be used in appropriate cases to call the Emergency Services.

5. SITING OF CAMERAS

The location of cameras is a key consideration. Use of CCTV to monitor areas where individuals would have a reasonable expectation of privacy would be difficult to justify. During the electrical rewire of the school, the local authority and the school has endeavoured to select locations for the installation of CCTV cameras which are least intrusive to protect the privacy of individuals. Cameras placed so as to record external areas are positioned in such a way as to prevent or minimise recording of passers-by or of another person's private property.

CCTV video monitoring and recording of public areas in the school may include the following:

- **Protection of school buildings and property:** The building's perimeter, entrances and exits, lobbies and corridors, reception.
- **Monitoring of Access Control Systems:** Monitor and record restricted access areas at entrances to buildings and other areas.
- **Verification of Security Alarms:** Intrusion alarms, exit door controls, external alarms.
- **Video Patrol of Public Areas:** Parking areas, main entrance/exit gates, Traffic Control.
- **Criminal Investigations (carried out by the Police):** Robbery, burglary and theft surveillance.

The following points were considered when the CCTV cameras were installed:

- Camera locations were chosen carefully to minimise viewing spaces that are not of relevance to the purposes for which we are using CCTV.
- Where CCTV has been installed to deal with a specific problem, we have considered setting the system up so it only records during the time when the problem usually occurs.
- The cameras have been sited to ensure that they can produce images of the right quality, considering their technical capabilities and the environment in which they are placed.
- Cameras are suitable for the location, bearing in mind the light levels and the size of the area to be viewed by each camera.
- We have checked that a fixed camera positioned in winter will not be obscured by the growth of plants and trees in the spring and summer.
- Cameras are sited so that they are secure and protected from vandalism.
- The system will produce images of sufficient size, resolution and frames per second.

6. COVERT SURVEILLANCE

The school will not engage in covert surveillance.

Certain law enforcement agencies may request to carry out covert surveillance on school premises. Such covert surveillance may require a Court Order. Accordingly, any such request made by law enforcement agencies will be requested in writing. The covert surveillance activities of public authorities are not covered here because they are governed by the Regulation of Investigatory Powers Act (RIPA) 2000. This type of recording is covert and directed at an individual or individuals.

7. NOTIFICATION - SIGNAGE

The Headteacher will provide a copy of these CCTV Procedures on request to staff, students, parents/carers and visitors to the school. These Procedures describe the purpose and location of

CCTV monitoring, a contact number for those wishing to discuss CCTV monitoring and guidelines for its use.

We must let people know when they are in an area where a surveillance system is in operation. The most effective way of doing this is by using prominently placed signs at the entrance to the surveillance system's zone and reinforcing this with further signs inside the area. Clear and prominent signs are particularly important where the surveillance systems are very discreet, or in locations where people might not expect to be under surveillance. As a general rule, signs should be more prominent and frequent in areas where people are less likely to expect that they will be monitored by a surveillance system.

Signs should:

- Be clearly visible and readable.
- Contain details of the organisation operating the system, the purpose for using the surveillance system and who to contact about the scheme (where these things are not obvious to those being monitored).
- Include basic contact details such as a simple website address, telephone number or email contact; and be an appropriate size.

8. STOARGE AND RETENTION OF RECORDED IMAGES

8.1 Storage

Tapes/DVDs will be stored in a secure environment with a log of access to tapes kept. Access will be restricted to authorised personnel as above. Similar measures will be employed when using disk storage, with automatic logs of access to the images created.

Supervising the access and maintenance of the CCTV System is the responsibility of the Head teacher. The Head teacher may delegate the administration of the CCTV System to another staff member. In certain circumstances, the recordings may also be viewed by other individuals in order to achieve the objectives set out above e.g. the Police, the Deputy Head teacher, the relevant Year Head, other members of the teaching staff, representatives of the DfE, representatives of the HSE and/or the parent of a recorded student. When CCTV recordings are being viewed, access will be limited to authorised individuals on a need-to-know basis.

We will keep a record or audit trail showing how the information must be handled if it is likely to be used as evidence in court. Once there is no reason to retain the recorded information, it will be deleted. Exactly when we decide to do this will depend on the purpose for using the surveillance systems. A record or audit trail of this process will also be captured.

CCTV images are digitally recorded. It is important that our information can be used by appropriate law enforcement agencies if it's required.

8.2 Retention

The General Data Protection Regulation states that data "shall not be kept for longer than is necessary for" the purposes for which it was obtained. As a data controller, the school needs to be able to justify this retention period. For a normal CCTV security system, it would be difficult to justify retention beyond a month (28 days), except where the images identify an issue – such as a break-in or theft and those particular images/recordings are retained specifically in the context of an investigation/ prosecution of that issue.

Accordingly, the images captured by the CCTV system will be retained for a maximum of 28 days except where the image identifies an issue and is retained specifically in the context of an investigation/prosecution of that issue.

- £10 for subject access requests; a sum not exceeding the cost of materials in other cases.

8.3 Access

Digitally captured images and the monitoring equipment will be securely stored in a restricted area. Unauthorised access to that area will not be permitted at any time. The area will be locked when not occupied by authorised personnel.

Access to the CCTV system and stored images will be restricted to authorised personnel only i.e. the Headteacher, Facilities Manager and Business Manager.

9. DISCLOSURE OF IMAGES

There will be no disclosure of recorded data to third parties other than to authorised personnel such as the Police and service providers to the school where these would reasonably need access to the data (e.g. investigators). In relevant circumstances, CCTV footage may be disclosed:

- To the Police where the school is required by law to make a report regarding the commission of a suspected crime; or
- Following a request by the Police when a crime or suspected crime has taken place and/or when it is suspected that illegal/anti-social behaviour is taking place on the school property, or
- To the HSE and/or any other statutory body charged with child safeguarding; or
- To assist the Headteacher/Manager in establishing facts in cases of unacceptable student behaviour, in which case, the parents/carers will be informed. The data may be used within the school's discipline and grievance procedures as required, and will be subject to the usual confidentiality requirements of those procedures; or
- To data subjects (or their legal representatives), pursuant to an access request where the time, date and location of the recordings is furnished to the school; or
- To individuals (or their legal representatives) subject to a court order; or
- To the school's insurance company where the insurance company requires same in order to pursue a claim for damage done to the insured property.

Only authorised and trained staff are allowed to make external disclosures of CCTV footage (Head teacher, Facilities Manager and Business Manager)

Data will never be placed in the internet and will not be released to the media. Information may be released to the media for identification purposes, but this must NOT be done by anyone other than a law enforcement agency.

Once we have disclosed information to another body, such as the police, they become the Data Controller for the copy they hold. It is their responsibility to comply with the GDPR in relation to any further disclosures.

9.1 Requests by the police

Information obtained through video monitoring will only be released when authorised by the Head teacher/Manager following consultation with the Chair of the Governing Body. If the Police request CCTV images for a specific investigation, any such request made by the Police should be made in writing.

9.2 Subject Access Request

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.

To make a subject access request, please complete the subject access request form (Appendix 3) and return this 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.

Our DPO is Jennifer Rowlands and is contactable via e-mail: Jennifer.rowlands@solway.cumbria.sch.uk or telephone: 07794 753 510

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.

Requests for Data Subject Access should be made on an application form available from the Business Manager (refer to the school's GDPR Policy for further details).

A person should provide all the necessary information to assist the school in locating the CCTV recorded data, such as the date, time and location of the recording. If the image is of such poor quality as not to clearly identify an individual, that image may not be considered to be personal data and may not be handed over by the school. The school reserves the right to refuse access to CCTV footage where this would prejudice the legal rights of other individuals or jeopardise an on-going investigation.

In giving a person a copy of their data, the school may provide a still/series of still pictures, a tape or a disk with relevant images. However, other images of other individuals will be obscured before the data is released.

For further information on subject access requests, refer to the ICO's 'Subject Access Code of Practice' https://ico.org.uk/media/for-organisations/documents/1065/subject-access-code-of-practice.pdf.

9.3 Freedom of Information

The school may receive requests under the Freedom of Information Act (FOIA). We have a member of staff who is responsible for responding to freedom of information requests and understands the school's responsibilities. We must respond within 20 working days from receipt of the request.

Section 40 of the FOIA contain a two-part exemption relating to information about individuals. If we receive a request for surveillance system information, we will consider:

- Is the information personal data of the requester? If so, then that information is exempt from the FOIA. Instead this request should be treated as a data protection subject access request.

- Is the information personal data of other people? If it is, then the information can only be disclosed if this would not breach the data protection principles.

In practical terms, if individuals are capable of being identified from the relevant surveillance system, then it is personal information about the individual concerned. It is generally unlikely that this information can be disclosed in response to a freedom of information request as the requester could potentially use the information for any purpose and the individual concerned is unlikely to expect this. This may be unfair processing in contravention of the DPA.

10. BREACHES OF THE PROCEDURES (including security breaches)

- Any breach of these procedures by school staff will be initially investigated by the Data Protection Officer, in order for her to take the appropriate disciplinary action.
- Any serious breach of the procedures will be immediately investigated, and an independent investigation carried out to make recommendations on how to remedy the breach.
- Information obtained in violation of these procedures may not be used in a disciplinary proceeding against an employee of the school, or a student.

11. MONITORING AND REVIEW

Routine performance monitoring, including random operating checks, may be carried out by the Facilities Manager

These procedures will be regularly reviewed, either by a designated individual within the school or by a third party. This is to ensure the standards established during the setup of the system are maintained.

Similarly, there will be a periodic review, at least annually, of the system's effectiveness to ensure that it is still doing what it was intended to do. If it does not achieve its purpose, it should be stopped or modified. The review will consider the following:

- Is it addressing the needs and delivering the benefits that justified its use?
- Is information available to help deal with queries about the operation of the system and how individuals may make access requests?
- Does the information include our commitment to the recommendations in the ICO Code of Practice and include details of the ICO if individuals have data protection compliance concerns?
- Is a system of regular compliance reviews in place, including compliance with the provisions of the ICO Code of Practice, continued operational effectiveness and whether the system continues to meet its purposes and remains justified?
- Are the results of the review recorded, and are its conclusions acted upon?

The periodic review will also ensure all information is sufficiently protected to ensure that it does not fall into the wrong hands. This will include technical, organisational and physical security. For example:

- Sufficient safeguards are in place to protect wireless transmission systems from interception.
- The ability to make copies of information is restricted to appropriate staff.
- There are sufficient controls and safeguards in place if the system is connected to, or made available across, a computer, e.g. an intranet.
- Where information is disclosed, it is safely delivered to the intended recipient e.g. by Royal Mail Special Delivery if posted or identification verified, and receipt signed for if collected in person.
- Staff are trained in security procedures and there are sanctions against staff who misuse surveillance system information.
- Staff have been made aware that they could be committing a criminal offence if they misuse surveillance system information.
- The process for deleting data is effective and being adhered to.
- If there have been any software updates (particularly security updates) published by the equipment's manufacturer, then they have been applied to the system.

12. COMPLAINTS

- Any complaints about the school's CCTV system should be addressed to the Headteacher.

ANNUAL REVIEW OF CCTV SYSTEMS			
The school has considered the need for using CCTV and have decided it is required for the prevention and detection of crime and for protecting the safety of staff and students. It will not be used for other purposes. We conduct an annual review of our use of CCTV as follows.			
School/Setting:		**Date:**	
Assessor:		**Signed:**	

	Satisfactory		**Problems Identified** *(if any)*	**Corrective Action Taken** *(if relevant)*	**Completed By**	**Date Complete**
	Yes	**No**				
Notification has been submitted to the Information Commissioner and the next renewal date recorded.						
There is a named individual who is responsible for the operation of the system.						
The problem we are trying to address has been clearly defined and installing cameras is the best solution.						
The CCTV system is addressing the needs and delivering the benefits that justified its use.						
A system has been chosen which produces clear images which the law enforcement bodies (usually the police) can use to investigate crime and these can easily be taken from the system when required.						
Cameras have been sited so that they provide clear images.						
Cameras have been positioned to avoid capturing the images of persons not visiting the premises.						
There are visible signs showing that CCTV is in operation. Where it is not obvious who is responsible for the system contact details are displayed on the sign(s).						
Information is available to help deal with queries about the operation of the system and how individuals may make access requests.						

	Satisfactory		Problems Identified *(if any)*	Corrective Action Taken *(if relevant)*	Completed By	Date Complete
	Yes	No				
Sufficient safeguards are in place to protect wireless transmission systems from interception.						
There are sufficient controls and safeguards in place if the system is connected to, or made available across, a computer, e.g. an intranet.						
Images from this CCTV system are securely stored, where only a limited number of authorised persons may have access to them.						
The ability to make copies of information is restricted to appropriate staff.						
The recorded images will only be retained long enough for any incident to come to light (e.g. for a theft to be noticed) and the incident to be investigated.						
The process for deleting data is effective and being adhered to.						
Except for law enforcement bodies, images will not be provided to third parties.						
The potential impact on individuals' privacy has been identified and taken into account in the use of the system.						
The organisation knows how to respond to individuals making requests for copies of their own images. If unsure the controller knows to seek advice from the Information Commissioner as soon as such a request is made.						
Where information is disclosed, it is safely delivered to the intended recipient e.g. by Royal Mail Special Delivery if posted or identification verified, and receipt signed for if collected in person.						
Staff are trained in security procedures and there are sanctions against staff who misuse surveillance system information.						

	Satisfactory		Problems Identified *(if any)*	Corrective Action Taken *(if relevant)*	Completed By	Date Complete
	Yes	**No**				
Staff have been made aware that they could be committing a criminal offence if they misuse surveillance system information.						
Regular checks are carried out to ensure that the system is working properly and produces high quality images.						
If there have been any software updates (particularly security updates) published by the equipment's manufacturer, then they have been applied to the system.						
Please keep this checklist in a safe place until the date of the next Annual Review.						

THE GUIDING PRINCIPLES OF THE SURVEILLANCE CAMERA CODE OF PRACTICE

System operators should adopt the following 12 guiding principles:

1. Use of a surveillance camera system must always be for a specified purpose which is in pursuit of a legitimate aim and necessary to meet an identified pressing need.
2. The use of a surveillance camera system must consider its effect on individuals and their privacy, with regular reviews to ensure its use remains justified.
3. There must be as much transparency in the use of a surveillance camera system as possible, including a published contact point for access to information and complaints.
4. There must be clear responsibility and accountability for all surveillance camera system activities including images and information collected, held and used.
5. Clear rules, policies and procedures must be in place before a surveillance camera system is used, and these must be communicated to all who need to comply with them.
6. No more images and information should be stored than that which is strictly required for the stated purpose of a surveillance camera system, and such images and information should be deleted once their purposes have been discharged.
7. Access to retained images and information should be restricted and there must be clearly defined rules on who can gain access and for what purpose such access is granted; the disclosure of images and information should only take place when it is necessary for such a purpose or for law enforcement purposes.
8. Surveillance camera system operators should consider any approved operational, technical and competency standards relevant to a system and its purpose and work to meet and maintain those standards.
9. Surveillance camera system images and information should be subject to appropriate security measures to safeguard against unauthorised access and use.
10. There should be effective review and audit mechanisms to ensure legal requirements, policies and standards are complied with in practice, and regular reports should be published.
11. When the use of a surveillance camera system is in pursuit of a legitimate aim, and there is a pressing need for its use, it should then be used in the most effective way to support public safety and law enforcement with the aim of processing images and information of evidential value.
12. Any information used to support a surveillance camera system which compares against a reference database for matching purposes should be accurate and kept up to date.

Source: *The Information Commissioners Office 'In the Picture: A Data Protection Code of Practice for Surveillance Cameras and Personal Data, May 2015 (Appendix 3)*