Surveillance camera systems
Guidance for controllers

information commissioner
Barrantagh Fysseree

Surveillance camera systems have become a common feature of our daily lives, and whilst they continue to enjoy general public support, intrusion into the lives of ordinary individuals going about their routine business is inevitable. Research has shown that the public expect systems to be used responsibly with effective safeguards in place and maintaining public trust and confidence in the use of such systems is essential if the benefits are to be realised.

Surveillance camera systems include closed circuit television or automatic number plate recognition systems, any other systems for recording or viewing visual images for surveillance purposes, any systems for storing, receiving, transmitting, processing or checking images or information obtained by such systems, or any other systems associated with, or otherwise connected with these systems. The generic terms 'CCTV' and 'images' are used in this guidance for ease of reference.

The aim of this guidance is to assist controllers to understand and comply with the responsibilities and obligations set out in the data protection legislation.

Contents

How does data protection legislation apply to CCTV?

The Isle of Man data protection legislation includes the:

- *Data Protection Act 2018;*
- *Data Protection (Application of GDPR) Order 2018("Applied GDPR");*
- *Data Protection (Application of LED) Order 2018("Applied LED"); and*
- *GDPR and LED Implementing Regulations 2018 ("Regulations").*

These are collectively referred to as the ***"DP law"*** *in this guidance.*

Most CCTV is installed to view and/or record the activities of individuals. Information about living individuals is 'personal data' and DP law applies to the use, or processing, of 'personal data'.

CCTV images identify living individuals and are, therefore, personal data. This means that the use of CCTV will be covered by the DP law, regardless of the size of the system or organisation.

The basic legal requirement is to comply with the DP law itself. Article 5 of the Applied GDPR sets out the data protection principles that lie at the heart of DP law. These principles are set out on page 18 and further guidance is available on our website.

The DP law not only creates obligations for organisations when processing personal data, it also gives individuals rights, such as the right of access to their personal data and to seek compensation for any damage suffered, for example, if the right of access is not complied with.

The guidance is set out to follow the lifecycle and practical operation of CCTV and there are questions that must be positively addressed to help ensure that compliance with the principles is being achieved.

Following the recommendations in this guidance will:

- help ensure that those capturing images of individuals comply with the DP law;
- mean that the images that are captured are usable; and
- reassure those whose images are being captured.

Deciding whether to use CCTV or continue using CCTV

Using CCTV can be privacy intrusive, as it is capable of putting many law-abiding people under surveillance and recording their movements as they go about their routine activities. There must be a lawful reason for considering the use of CCTV, such as crime prevention and detection, health and safety of workers or the public, property security, for example.

The use of CCTV must be necessary and proportionate. You should carefully consider, therefore, whether to use CCTV; the fact that it is possible, affordable or has public support should not be the primary motivating factor. You should take into account what benefits can be gained, whether better solutions exist, and what effect it may have on individuals.

For example, vehicles in a car park are frequently damaged and broken into at night. Consider whether improved lighting would reduce the problem more effectively than CCTV.

You should consider these matters objectively as part of an assessment of the scheme's impact on people's privacy. The extent of assessment necessary will depend on the size of the proposed scheme and the level of impact it is likely to have on people's privacy.

However, when considering monitoring publicly accessible areas, a data protection impact assessment (DPIA) must be carried out. Advice about DPIAs is available at: https://www.inforights.im/organisations/data-protection-law-2018/accountability-and-governance/data-protection-impact-assessments/

You should use the results of the DPIA to determine whether CCTV is justified in all the circumstances and, if so, how it should be operated in practice.

Points to consider

The points to consider in any DPIA therefore include:

- What are the problems, or risks, the CCTV is meant to address?
- What are the benefits to be gained from its use?
- Can CCTV technology realistically deliver these benefits?
- Can less privacy-intrusive solutions, such as improved lighting, achieve the same objectives?
- Do you need images of identifiable individuals, or could the scheme use other images not capable of identifying the individual?
- Will the particular equipment/system of work being considered deliver the desired benefits now and remain suitable in the future?

- What organisation will be using the CCTV images?
- Who will take legal responsibility under the DP law? (See 'Ensuring effective administration')
- What is the organisation's purpose for using CCTV?
- What future demands may arise for wider use of images and how will you address these?
- What are the views of those who will be under surveillance?
- What could you do to minimise intrusion for those that may be monitored, particularly if specific concerns have been expressed?

Additional considerations for public and local authorities

Where the controller is a public authority or body and where the processing results from a legal obligation, i.e. the processing is necessary for compliance with a legal obligation to which the controller is subject, a DPIA may not be necessary, provided the privacy impacts were considered as part of the legislative process.

Where the system will be operated by or on behalf of a public authority, the authority will also need to consider wider human rights issues and in particular the implications of the European Convention on Human Rights, Article 8 (the right to respect for private and family life). This will include:

- Is the proposed system established on a proper legal basis and operated in accordance with the law?
- Is it necessary to address a pressing need, such as public safety, crime prevention or national security?
- Is it justified in the circumstances?
- Is it proportionate to the problem that it is designed to deal with?

If these criteria cannot be met, then it would not be appropriate to use CCTV.

Local authorities should also be aware of the additional obligations placed upon them by section 2 of the Criminal Justice Act 1996 when considering purchasing and using CCTV.

Ensuring effective administration

The controller is legally responsible for compliance with the DP law and has responsibility for the control of the images, for example, deciding what is to be recorded, how the images should be used and to whom they may be disclosed.

Where more than one controller (organisation, business etc) is involved, each should know its responsibilities and obligations. If both make decisions about the purposes and operation of the scheme, then both are responsible under the DP law. This may be the case, for example, where the police have access to local authority-owned CCTV.

Points to consider

- Understand who the "controller" is and if there is more than one controller have responsibilities been agreed and does each know its responsibilities?
- Is the controller registered with the Commissioner?
- If someone outside your organisation provides you with any processing services, for example, editing the images, is a written contract in place with clearly defined responsibilities?
- Are there clear procedures to determine how you use the system in practice?
- Have you identified clearly defined and specific purposes for the use of images, and have these been communicated to those who operate the system?
- Are there clearly documented procedures for how the images should be handled in practice? This could include guidance on disclosures and how to keep a record of these. Have these procedures been given to appropriate people?
- Has responsibility for ensuring that procedures (including security measures and compliance with rights) are followed been allocated to an appropriate individual (or a data protection officer)?
- Are proactive checks carried out on a regular basis to ensure that procedures are being complied with? This can be done either by you as the system operator or a third party.

You should regularly review whether the use of CCTV continues to be justified.

Selecting and locating the cameras

Any CCTV images must be adequate and limited to what is necessary for the purpose for which you are collecting them. It is essential that you choose camera equipment and locations that achieve the purposes for which you are using CCTV.

Both permanent and movable cameras should be sited, and image capture restricted, to ensure that they do not view areas that are not of interest and are not intended to be the subject of surveillance, such as individuals' private property. The system must have the necessary technical specification to ensure that images are of the appropriate quality for the envisaged purpose.

Example: Check that a fixed camera positioned in winter will not be obscured by the growth of spring and summer foliage.

Example: A supermarket installs CCTV to detect acts of theft or vandalism to customers' cars. The cameras should not record callers to a neighbouring property, such as a doctor's surgery. Such processing is both excessive and irrelevant and will breach the DP law.

Points to consider

- Have you carefully chosen the camera location to minimise viewing spaces that are not of relevance to the purposes for which you are using CCTV?
- Where CCTV has been installed to deal with a specific problem, have you considered setting the system up so it only records at the time when the problem usually occurs? Alternatively, have you considered other privacy-friendly ways of processing images? For example, some systems only record events that are likely to cause concern, such as movement into a defined area. This can also save on storage capacity.
- Will the cameras be sited to ensure that they can produce images of the right quality, taking into account their technical capabilities and the environment in which they are placed?
- Is the camera suitable for the location, bearing in mind the light levels and the size of the area to be viewed by each camera?
- Are the cameras sited so that they are secure and protected from vandalism?
- In areas where people have a heightened expectation of privacy, such as changing rooms or toilet areas, cameras should only be used in the most exceptional circumstances where it is necessary to deal with very serious concerns. In these cases, you should make extra effort to ensure that those under surveillance are aware.
- Will the system produce images of sufficient size, resolution and frames per second?

To judge the quality of images that will be necessary, you will need to take into account the purpose for which CCTV is used and the level of quality that will be necessary to achieve the purpose. The Home Office Scientific Development Branch recommends identifying the needs of a CCTV system by using four categories:

- **Monitoring**: to watch the flow of traffic or the movement of people where you do not need to pick out individual figures.
- **Detecting**: to detect the presence of a person in the image, without needing to see their face.
- **Recognising**: to recognise somebody you know, or determine that somebody is not known to you.
- **Identifying**: to record high quality facial images which can be used in court to prove someone's identity beyond reasonable doubt.

Using the equipment

It is important that a CCTV system produces images that are of a suitable quality for the purpose for which the system was installed. If identification is necessary, then poor quality images which do not help to identify individuals may undermine the purpose for installing the system.

CCTV must not be used to record conversations between members of the public as this is highly intrusive and unlikely to be justified.

Points to consider

- Do the recorded pictures and prints as well as the live screens produce good clear pictures? This is important to ensure that there has not been an unacceptable loss of detail during the recording process.

- Have you considered the compression settings for recording material? In a digital system, a high level of compression will result in poorer picture quality on playback.

- Have you set up the recording medium in such a way that images cannot be inadvertently corrupted?

- Is there a regular check that the date and time stamp recorded on the images is accurate?

- Has a regular maintenance regime been set up to ensure that the system continues to produce high quality images?

- If a wireless transmission system is used, are sufficient safeguards in place to protect it from being intercepted?

Looking after the recorded material and using the images

Storing and viewing the images

Recorded material should be stored in a way that maintains the integrity of the image. This is to ensure that the rights of individuals recorded by the CCTV system are protected and that the material can be used as evidence in court.

To do this you need to carefully choose the medium on which the images are stored, and then ensure that access is restricted. You should keep a record of how the images are handled if they are likely to be used as evidence in court. Finally, once there is no reason to retain the recorded images, they should be deleted. Exactly when you decide to do this will depend on the purpose for using CCTV, but it should be the minimum period necessary.

Most CCTV systems rely on digital recording technology and this present its own problems. With video tapes it was very easy to remove a tape and give it to the law enforcement agencies such as the police for use as part of an investigation. It is important that your images can be used by appropriate law enforcement agencies if this is envisaged. If they cannot, this may undermine the purpose for undertaking CCTV surveillance.

You must ensure that you can make a copy of recording if requested by a data subject or if required by the police.

- Can this be done without interrupting the operation of the system?
- Will they find your recorded images straightforward to use?
- What will you do when recorded material needs to be taken away for further examination?
- Have you the capability to obscure third party images?

Viewing of live images on monitors should usually be restricted to the operator unless the monitor displays a scene which is also in plain sight from the monitor location.

Example: *Customers in a bank can see themselves on a monitor screen. This is acceptable as they cannot see anything on the screen that they could not see by looking around them. The only customers who can see the monitor are those who are also shown on it.*

Example: *Monitors in a hotel reception area show guests in the corridors and lifts, i.e. out of sight of the reception area. They should be turned so that they are only visible to staff, and members of the public should not be allowed access to the area where staff can view them.*

Recorded images should also be viewed in a restricted area, such as a designated secure office. The monitoring or viewing of images from areas where an individual would have an expectation of privacy should be restricted to authorised persons.

Points to consider

- Are your CCTV monitors correctly sited taking into account the images that are displayed?

- Is your CCTV monitor viewing area appropriate and secure?

- Where necessary is access to CCTV monitors limited to authorised people?

Disclosure of images

Disclosure of images from the CCTV system must also be controlled and consistent with the purpose for which the system was established. However, individuals have the right to request copies of their images (i.e. their personal data).

For example, if the system is established to help prevent and detect crime it will be appropriate to disclose images to law enforcement agencies where a crime needs to be investigated, but it would not be appropriate to disclose images of identifiable individuals to the media for entertainment purposes or place them on the internet.

Images should not be released to the media or uploaded to social media.

NOTE: Even if a system was not established to prevent and detect crime, it would still be acceptable to disclose images to law enforcement agencies if failure to do so would be likely to prejudice the prevention and detection of crime.

Any requests made by third parties for images should be approached with care, as a wide disclosure of these may be unfair to the individuals concerned. In some limited circumstances, it may be appropriate to release images to a third party, where their needs outweigh those of the individuals whose images are recorded.

Example: *A member of the public requests CCTV footage of a car park, which shows their car being damaged. They say they need it so that they or their insurance company can take legal action. You should suggest that they ask the insurance company to make the request.*

Points to consider

- Are arrangements in place to restrict disclosure of images in a way consistent with the purpose for establishing the system?

- Do those that may handle requests for disclosure have clear guidance on the circumstances in which it is appropriate to make a disclosure and when it is not?

- Do you record the date of the disclosure along with details of who the images have been provided to (the name of the person and the organisation they represent) and why they are required?

Judgements about disclosure should be made by the organisation operating the CCTV system. They have discretion to refuse any request for information unless there is an overriding legal

obligation, such as the right of access to personal data, or a court order.

Once you have disclosed an image to another body, such as the police, they become the controller for their copy of that image. It is their responsibility to comply with the DP law in relation to any further disclosures.

The method of disclosing images should be secure to ensure they are only seen by the intended recipient.

Retention of images

The DP law does not prescribe any retention periods. Retention should reflect the organisation's own purposes for recording images or any industry standards or requirements .

However, you should not keep images for longer than strictly necessary to meet your own purposes for recording them. Occasionally, you may need to retain images for a longer period, for example, where the police are investigating a crime, to give them opportunity to view the images as part of an active investigation.

Example: *A system installed to prevent fraud being carried out at an ATM may need to retain images for several weeks, since a suspicious transaction may not come to light until the victim gets a bank statement.*

Example: *Images from a town centre system may need to be retained for enough time to allow crimes to come to light, for example, a month. The exact period should be the shortest possible, based on your own experience.*

Example: *A small system in a pub may only need to retain images for a shorter period of time because incidents will come to light very quickly.*

Points to consider

- Have you determined the shortest period that you need to retain the images, based upon your own purpose for recording the images?
- Is your image retention policy documented and understood by those who operate the system?
- Are measures in place to ensure the permanent deletion of images through secure methods at the end of this period?
- Do you undertake systematic checks to ensure that the retention period is being complied with in practice?

Responsibilities

Letting people know

Individuals must be informed when they are in an area where CCTV surveillance is being undertaken.
The most effective way of doing this is by using prominently placed signs at the entrance to the CCTV zone and reinforcing this with further signs inside the area.

Clear and prominent signs are particularly important where the cameras themselves 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 where it would otherwise be less obvious to people that they are on CCTV.

Signs should:

- be clearly visible and readable;
- contain details of the organisation operating the system,
- the purpose(s) for using CCTV, and
- who to contact about the scheme (where these things are not obvious to those being monitored); and
- be an appropriate size depending on context, for example, whether they are viewed by pedestrians or car drivers.

Signs do not need to say who is operating the system if this is obvious. If CCTV is installed within a shop, for example, it will be obvious that the shop is responsible.

All staff should know what to do or who to contact if a member of the public makes a request for their images from the CCTV system. Systems in public spaces and shopping centres should have signs giving the name and contact details of the company, organisation or authority responsible.

Points to consider

- Do you have signs in place informing people that CCTV is in operation?

- Do your signs convey the appropriate information?

Individuals' rights - subject access requests & erasure requests

In deciding to use CCTV systems, the controller must understand that individuals have rights in respect of their personal data, including the right of access and the right to erasure, and comply with such requests. There are some exceptions to those rights set out in Schedule 9 to the GDPR and LED Implementing Regulations 2018.

Requests can be made in writing or orally. Compliance with a request is not dependent on the individual completing a specified form.

Costs associated with dealing with the exercise of those rights, including the need to obscure any third party images, must be borne by the controller.

Subject access requests

Individuals whose images are recorded have a right to view the images of themselves and, if they ask, be supplied with a copy of the images. Copies of images must be provided without undue delay and in any event within one month of receiving the request.

It should be noted that subject access requests cannot be refused due to the expense incurred by a controller for editing and copying the recordings.

Those who request access must provide you with sufficient details to allow you to identify them as the subject of the images and also to locate the images on your system.

Erasure requests

Individuals whose images are recorded have a right to have those images erased, where that right is engaged. That right must be complied with without undue delay and in any event within one month of receiving the request.

Points to consider

- How will the staff involved in operating the CCTV system recognise a subject access or erasure request?

- Do you have internal procedures in place for handling such requests? This could include keeping a log of the requests received, and how they were dealt with, in case you are challenged.

A clearly documented process will also help guide individuals through such requests. This should make it clear what an individual needs to supply when they make a request.

You will need to decide, for example:

- What details will you need to find the images?
- Will an individual need to supply a photograph of themselves or a description of what they were wearing at the time they believe they were captured on the system to aid identification, if they are not already known to you?
- Will details of the date, time and location be required?

How will you provide an individual with copies of the images?

When images of third parties are also shown alongside the images of the person who has made the subject access request, you must consider whether you need to obscure the images of third parties. If providing those images would involve an unfair intrusion into the privacy of the third party, or cause unwarranted harm or distress, then their images should be obscured. In many

cases, third party personal data can be disclosed as there will not be such intrusion, particularly if the third party is known to the data subject.

Example: *A public space CCTV camera records people walking down the street and going about their ordinary business. Where nothing untoward has occurred, this can be released without editing out third party images.*

Example: *Images show the individual who has made the request with a group of friends, waving at a camera in the town centre. There is little expectation of privacy and the person making the request already knows their friends were there. It is likely to be fair to release the image to the requester without editing out the faces of their friends.*

Example: *Images show a waiting room in a doctor's surgery. Individuals have a high expectation of privacy and confidentiality. Images of third parties should be redacted (blurred or removed) before release.*

Where you decide that third parties should not be identifiable, then you will need to make arrangements to disguise or blur the images in question. It may be necessary to contract this work out to another organisation. Where this occurs, you will need to have a written contract with the processor that specifies exactly how the information is to be used and provides you with explicit security guarantees.

Information about the rights of individuals can be found on the Commissioner's website at: https://www.inforights.im/organisations/data-protection-law-2018/rights/

Monitoring your workforce

When you install CCTV in a workplace, such as a shop, it is likely to capture pictures of workers, even if they are not the main subject of surveillance. If the purpose of the CCTV is solely to prevent and detect crime, then you should not use it for monitoring the amount of work done or compliance with company procedures.

In some cases, it may be appropriate to install CCTV specifically for workforce monitoring, for example hazardous working environments where CCTV is permanently monitored. You should go through the decision making process and consider whether CCTV is justified. In particular, consider whether better training or greater supervision would be a more appropriate solution.

Example: *You suspect that your workers are stealing goods from the store room. It may be appropriate to install CCTV in this room, as it will not involve continuous or intrusive monitoring and is proportionate to the problem.*

Example: *You suspect that your workers are making mobile phone calls during working hours, against company policy, and you consider installing CCTV cameras on their desks, or activating webcams in laptops, to monitor them throughout the day. This would be intrusive and disproportionate. Continuous monitoring should only be used in very exceptional circumstances, for example, where hazardous substances are used and failure to follow procedures would pose a serious risk to life.*

Points to consider

- Are images of workers used only if you see something you cannot be expected to ignore, such as criminal activity, gross misconduct, or behaviour which puts others at risk?
    - If these images are used in disciplinary proceedings, is the footage retained so that the worker can see it and respond? A still image is unlikely to be enough.
- Is CCTV limited to areas that workers would not expect to be private? CCTV should not be used in toilet areas or private offices.
- Are workers made aware that the CCTV is for staff monitoring and how it will be used?
- How are visitors informed that CCTV is in operation?
- If CCTV is used to enforce internal policies, are workers fully aware of these policies and have they had sufficient training?
- Do you have procedures to deal appropriately with subject access requests from workers?

Workers should normally be made aware that they are being monitored, but in exceptional circumstances, covert monitoring may be used as part of a specific investigation. Covert

monitoring is where video or audio recording equipment is used, and those being monitored are unaware that this is taking place.

Before approving covert monitoring, you should ask yourself:

- Is this an exceptional circumstance, and is there is reason to suspect criminal activity or equivalent malpractice?
- Will the cameras only be used for a specific investigation, and will they be removed once the investigation is complete?
- Would it prejudice the investigation to tell workers that cameras are being used?
- Have you taken into account the intrusion on innocent workers?
- Has the decision been taken by senior management?

Cameras and listening devices should not be installed in private areas such as toilets and private offices, except in the most exceptional circumstances where serious crime is suspected. This should only happen where there is an intention to involve the police, not where it is a purely internal disciplinary matter.

In some cases, covert cameras installed for one investigation may turn up evidence of other criminal behaviour or disciplinary matters. You should only make use of this where the offence is serious, or for example, where gross misconduct or misconduct putting others at risk is involved. It would be unfair to use images obtained covertly for minor disciplinary matters.

Other guidance relating to staff can be found in our guidance note "Employment data – getting it right"

Staying in control

Once you have considered the guidance in this document and set up the CCTV system, you need to ensure that its operation continues to comply with the DP law.

If requested you should:

- tell people how they can make a subject access request, who it should be sent to and what information needs to be supplied with their request;
- tell people how to complain about either the operation of the system or failure to comply with the requirements of the DP law.

Staff using the CCTV system or images should be trained to ensure the use complies with the DP law.

In particular, do they know:

- what the organisation's policies are for recording and retaining images?
- how to handle the images securely?
- what to do if they receive a request for images, for example, from the police?
- how to recognise a subject access or erasure request and what to do if they receive one?

All images must be protected by sufficient security. This should include technical, organisational and physical security.

For example:

- Is the ability to make copies of images restricted to appropriate staff?
- Where copies of images are disclosed, how are they safely delivered to the intended recipient?
- Are control rooms and rooms where images are stored secure?
- Are staff trained in security procedures, and are there sanctions against staff who misuse CCTV images?
- Are staff aware that they could be committing a criminal offence if they misuse CCTV images?

Any documented procedures which you produce should be reviewed regularly, either by a designated individual within the organisation or by a third party. This is to ensure the ongoing

integrity of the system and that standards established during the setup of the system are maintained.

Similarly, there should 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.

Points to consider

- Is information available to help deal with queries about the operation of the system and how individuals may make access or erasure requests?

- Is a system of regular compliance reviews in place, including compliance with the provisions of the DP law, 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?

Data Protection Principles

Article 5 - Data Protection (Application of GDPR) Order 2018

1. Personal data shall be:

(a)processed lawfully, fairly and in a transparent manner in relation to the data subject (**'lawfulness, fairness and transparency'**);

(b)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, in accordance with Article 89(1), not be considered to be incompatible with the initial purposes (**'purpose limitation'**);

(c)adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed (**'data minimisation'**);

(d)accurate and, where necessary, kept up to date; every reasonable step must 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 (**'accuracy'**);

(e)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 in accordance with Article 89(1) subject to implementation of the appropriate technical and organisational measures required by this Regulation in order to safeguard the rights and freedoms of the data subject (**'storage limitation'**);

(f)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 (**'integrity and confidentiality'**).

2. The controller shall be responsible for, and be able to demonstrate compliance with, paragraph 1 (**'accountability'**).

This is not a full explanation of the principles. For more information, see our website.

Checklist for small retail and business premises

- ❑ Registration as a controller with the Information Commissioner completed. (mandatory)
- ❑ There are visible signs showing that CCTV is in operation, including contact details for the business (principle of lawfulness, fairness and transparency). (mandatory)
- ❑ The organisation knows how to respond to individuals exercising their right of access or erasure. (mandatory)
- ❑ Cameras have been positioned so that they provide clear images and avoid capturing images of persons who are not visiting the premises. (principle of data minimisation)
- ❑ Regular checks are carried out to ensure that the system is working properly and produces high quality images.
- ❑ 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. (principle of storage limitation)
- ❑ Images from the CCTV system are securely stored, and only a limited number of authorised persons may have access to them. (principle of integrity and confidentiality)
- ❑ Images can be taken from the system if required by the police to investigate crimes but will not be provided to other third parties. (principle of purpose limitation)
- ❑ A nominated individual is responsible for the administration of the system.

Published: August 2019