Close Circuit Television at 119 Main Street, Ayr

Policy on its use

The association has installed Close Circuit Television (CCTV) in the following places:

- At the entrance, front and rear of our office.
- In the public and working areas of the office – this includes the reception and waiting area, public meeting rooms and interview rooms.

As expected by the Information Commissioner. We carried out a data protection impact assessment (DPIA) before commissioning the CCTV system. We have implemented a risk management strategy to ensure that it complies with the Data Protection Act. The DPIA is available on our website and on request from our office.

The purpose of the CCTV is to:

- Protect users of the building including employees from criminal or anti-social behaviour.
- To minimise the risk of theft.
- To protect the premises when they are unoccupied.

To keep intrusion to minimum the following policy is applied:

- The recordings are of images only – there is no sound recording.
- All images are securely held and will only be observed by authorised employees.
- Unless required by the police or other legitimate individuals, images will be deleted after 30 days.

Further information:

Our reception staff will be delighted to answer any questions about the CCTV recording. Information is also available in advance of a visit to the office at www.ayrshirehousing.org.uk

You can find out about our approach to data protection in Our Privacy Notice. The notice gives you details of your right to request copies of images and any other information we might hold of you. You can get a copy of the Privacy Notice at our reception or on our website.

If you still have concerns, please ask to speak to our Data Protection Officer at 01292 880120 who will be pleased to answer your questions.

Created: 1 July 2021
Reviewed: 21 June 2022

DATA PROTECTION IMPACT ASSESSMENT (DPIA)

This template should be filled out at the start of any major project involving the use of personal data, or if you are making a significant change to an existing process. The final outcomes should be integrated into a project plan.

SUBMITTING DATA PROTECTION OFFICER DETAILS	
Name of Controller	Ayrshire Housing
Title of DPO	Head of Finance
Name of DPO	Alan Park

STEP 1: HOW DO WE DECIDE WHETHER TO DO A DPIA

Explain broadly what the project aims to achieve and what type of processing it involves. You may find it helpful to refer or link to other documents, such as a project proposal. Summarise why you have identified the need for a DPIA.

As part of our office extension there is an intention to upgrade our CCTV system. This will include the introduction of external cameras to the front and rear of the building as well as cameras within the office in areas where staff are located and over-looking interview rooms where tenant/applicant interviews are being carried out. The CCTV system will not include sound.

The location of some of the cameras could result in systematic monitoring of employees' activities, including the monitoring of employees' workstations and internet activity.

This is a substantial change for the association and a DPIA is being undertaken to assess the extent to which monitoring is required, where it is required and at what times. We need to determine if the system is justifiable and that everyone who will be affected are consulted to assess the impact on their privacy and determine any safeguards which can and should be put in place.

We need to be mindful of the regulatory environment when using CCTV systems and consider our obligations under GDPR, Data Protection Act 2018, Freedom of Information (Scotland) Act 2002, Human Rights Act 1998 (HRA) and CCTV Strategy for Scotland.

Using CCTV cameras can be privacy intrusive; they can place large numbers of law-abiding people under surveillance and recording their movements as they go about their day-to-day activities. We need to consider the problem(s) we are seeking to address; whether CCTV would be a justified and an effective solution or whether a better solution exists and what affect it may have on individuals. We need to establish if we have a lawful basis for processing which is justified, necessary and proportionate.

We must establish who has responsibility for controlling the information we collect, i.e., deciding what is being recorded, how the information should be used and to whom it may be disclosed.

As the data controller we **would be** responsible for compliance with DPA and GDPR.

STEP 2: DESCRIBE THE PROCESSING

Describe the nature of your processing: how will you collect, use, store and delete the data? Will you be sharing data with anyone? Are they any types of processing involved which are likely to be considered as high risk?

How will we collect the data?

The data will be collected by cameras situated on our office at both the front and rear of the building with some cameras being located internally covering areas where staff are located or where tenants/applicants and other visitors are seated or being interviewed. The system will collect images only, not sound. The external cameras will point towards the ground to exclude filming any of the business premises on the opposite side of the road.

How will we use this data/equipment?

- The cameras will act as a deterrent against theft or other criminal activity.
- To provide employees and visitors with a safe environment to work and do business. By allowing us to monitor what is happening in the office we can help to protect staff and visitors against violence and protect them from false accusations.
- To monitor the office during periods when it is empty.
- In the event of a crime occurring, we can provide the Police with evidence.

How will we store the data?

The data will be stored on a CCTV 6 terabyte drive located in our server room. The data will not form part of our daily back-up programme.

Will the data be shared with anyone?

The data would be shared to the PCs of reception staff and others with dedicated responsibilities to monitor its use. It will also be loaded onto the mobile devices of staff on call if the intruder alarm is activated. We would anticipate that sharing of data would be controlled and consistent with the purpose for which the system was installed. For example, we would as a matter of course disclose information to the Police, but any other requests would be approached with care.

All staff are aware of the association's Privacy Policy and of the consequences of breaching it.

We would share information with members of the public should they make a legitimate subject access request. Clear guidance is in place through our Privacy Policy to determine who is authorised to make these disclosures and when it is appropriate to do so. A record of all disclosures will be kept.

We would ensure that viewing of live images is restricted to authorised persons unless the monitor displays a scene which is also in plain sight. Where possible, we would only view recorded images in a restricted area such as the server room or from under the counter of the reception desk.

Staff who are authorised to disclose data will be trained to use the system so that they are able to easily extract information in the prescribed format. We will ensure that,

where required, 3rd party individuals' features are obscured to minimise the privacy intrusion.

We will ensure that any disclosures are made in a secure manner.

How would we delete the data?
DPA does not prescribe any specific minimum or maximum retention periods, but we would keep data for the shortest period necessary to serve our purpose. This will not be determined by the storage capacity of the drive.

The supplier proposes that the drive be over-written every 30 days. We will implement this proposal.

High Risk Processing
Under Article 35 of the GDPR we are required to carry out a DPIA for every processing operation which may result in "risks for the rights and freedoms of natural persons". Article 35(3) provides some examples of when a processing operation is likely to result in a high risk - condition [c] notes "a systematic monitoring of a publicly accessible area on a large scale".

In addition, CCTV monitoring does not always ensure that the data subject is aware of who is collecting their data and how it is being used. It may also be impossible for individuals to avoid being subject to such processing in publicly available spaces. The proposed location within the office of some of the cameras could also result in the monitoring of some employees' activities, including the monitoring of employees' workstations and internet activity. Under Article 35 of GDPR any excessive use of CCTV monitoring to profile employees is "high risk".

Describe the scope of the processing: what is the nature of the data, and does it include special category or criminal offence data? How much data will you be collecting and using? How often? How long will you keep it? How many individuals will be affected? What geographical areas does it cover?

What is the nature of the data, and does it include special category or criminal offence data?
CCTV, closed-circuit television also known as video surveillance. The data would not include special category or criminal offence data.

How much data will you be collecting and using?
Data will be continuously collected for 30 days. At the end of this period, it will be over-written. It is not possible to quantify how much data will be collected over that period. The data should **only** be used to respond to subject access requests and requests from the Police.

How often will it be collected?
24-hours per day.

How long will you keep it?
30 days.

How many individuals will be affected?
All employees of Ayrshire Housing and any visitors to the office. This will include service users such as tenants and applicants, contractors, Board members and other members of the public.

What geographical area does this cover?
119 Main Street, Ayr, KA8 8BX

Describe the context of the processing: what is the nature of your relationship with the individuals? How much control will they have? Would they expect you to use their data in this way? Do they include children or other vulnerable groups? Are there prior concerns over this type of processing or security flaws? Is it novel in any way? What is the current state of technology in this area? Are there any current issues of public concern that you should factor in? Are you signed up to any approved code of conduct or certification scheme (once any have been approved)?

Nature of Relationship, Control and Expectations

Staff Members [employed directly by Ayrshire Housing]
Under GDPR, employers are entitled to monitor employee activity if they have a lawful basis for doing so and the purpose of their monitoring is clearly communicated to employees in advance. Employees currently agree to this processing under the Workers Privacy Notice which everyone has signed. The notice states that employee monitoring may be required to carry out exercises in accordance with our "procedures on security and appropriate usage". These are described in the Conditions of Service, Code of Conduct and Staff Handbook

We cannot rely on consent as there is an imbalance of power in the employer/employee relationship. Employees can object to the use of CCTV cameras in a particular area which would then place the burden on Ayrshire Housing to demonstrate that we have "compelling legitimate grounds" for processing that override the employees' rights.

Members of the Public
CCTV monitoring does not always allow for the data subject to be aware of who is collecting their data and how it is being used. It may also be impossible for individuals to avoid being subject to such processing in publicly available spaces. Signage will be displayed prominently at the entrance so that individuals are aware of the CCTV installation and can ask for further information. Details of the installation will be included in the section on our office on our website

Due to the nature of the processing this could include children and other vulnerable groups. It is possible that children will be captured on CCTV, but the likelihood is that any children attending our office will be accompanied by an adult who will have the opportunity to review the CCTV information and the Privacy Notice to ensure that they are comfortable with our processing. It is also possible that vulnerable people could use our office, we will ensure that we provide all possible assistance to ensure that they understand the implications of our processing and the impact it might have on them.

Signage will be displayed at the public entrance and in the areas where CCTV cameras will be installed. This signage will be prominent.

Ayrshire Housing will consult with its IT specialists to ensure that appropriate safeguards are in place to mitigate any risks posed by data breach.

Technology in our area and current issues of public concern
We are not aware of any current areas of public concern regarding technology in our area, for example CCTV in public areas.

Approved Code of Conduct or Certification Scheme
We are not currently signed up to any certification scheme.

Describe the purposes of the processing: what do you want to achieve? What is the intended effect on individuals? What are the benefits of processing – for you and more broadly?

Our purposes for processing are as stated above:

- The cameras will act as a deterrent against theft or criminal activity.
- To provide employees and visitors with a safe environment to work and do business. By allowing us to monitor what is happening in the office we can help to protect staff and visitors against violence and protect them from false accusations.
- To monitor the office during periods when it is empty.
- In the event of a crime occurring, we can provide the Police with evidence.

Data will **only** be used to review specific incidents that have occurred and will not be routinely used or checked.

The impact on individuals should be low, unless they have committed a crime at which point their data will be reported to the Police.

Step 3: Consultation Process

Consider how to consult with relevant stakeholders: describe when and how you will seek individuals' views – or justify why it's not appropriate to do so. Who else do you need to involve within your organisation? Do you need to ask your processors to assist? Do you plan to consult information security experts, or any other experts?

We will inform staff of the purpose of the installation. Notwithstanding the primary purpose to ensure a safe working environment, staff will be reminded that the installation does not extend the range of monitoring already permitted.

It is not possible to consult with service users and the public in advance of the installation. We will however make information available so that they are given a degree of choice regarding their options in engaging with the association.

Step 4: Assess necessity and proportionality

Describe compliance and proportionality measures, in particular: what is your lawful basis for processing? Does the processing achieve your purpose? Is there another way to achieve the same outcome? How will you prevent function creep? How will you ensure data quality and data minimisation? What information will you give individuals? How will

you help to support their rights? What measures do you take to ensure processors comply? How do you safeguard any international transfers?

Lawful Basis for Processing

Legitimate Interest

- Prevention and detection of crime.
- Safeguarding staff and visitors.
- Ensuring compliance with health and safety procedures.

Does the processing achieve your purpose?

Yes, we can provide the police with enhanced information regarding any incidents that occur. CCTV will provide greater protection to individuals and improved health and safety. We are obligated to report crime and help the community at large to prevent crime or damage, this will allow us to achieve this purpose.

Is there another way to achieve the same outcome?

Not without using more intrusive methods such as a security guard posted outside the office.

How will you prevent function creep?

Function creep happens when we use technology and systems in ways beyond the original purpose, particularly when the new purpose results in invasion of privacy.

We will have a clear approach in place about our use of CCTV and we will not deviate from this. If we make any substantive modifications to the system, we will undertake a new DPIA.

How will you ensure data quality and data minimisation?

The data will be kept and used only to fulfil its original purpose. By working with our supplier, we will ensure that footage will continue to be of sufficient quality to aid easy identification of individuals. We will require the supplier to regularly update the software, especially in relation to security updates. We will ask that the drive is regularly checked to prevent degradation from constant over-writing. We will check the information provided by our supplier with our own IT Specialists.

We will ensure that recordings and logs are stored securely, and that access is limited to authorised persons only when required and the data is encrypted.

What information will you give individuals?

Clear signage will be posted wherever a camera is located informing individuals that CCTV is in operation. Further information will be readily available.

Employees have signed privacy notices providing them with information about monitoring.

We will ensure that individuals know how to make a subject access request, who it should be sent to and what information needs to be supplied with the request. We will inform individuals how to complain about the operation of our CCTV system or failure to comply with data protection legislation.

How will you support their rights?
Individuals have the right to request a copy of any CCTV footage in which they are clearly identifiable. If the request is valid and permissible, we will supply the individual with that footage within 30 days of the validation.

What measures do you take to ensure processors comply?
Staff will be trained in security procedures and will be advised about the potential consequences of misuse of the system.

Created: 1 July 2021
Reviewed: 21 June 2022

Step 5: Identify and Assess Risk

Describe source of risk and nature of potential impact on individuals. Include associated compliance and corporate risks as necessary.	**Likelihood of Harm** [remote, possible or probable]	**Severity of Harm** [minimal, significant or severe]	**Overall Risk** [low, medium or high]
Policies not in place about CCTV and no nominated individual with responsibility.	Possible	Minimal	Medium
Staff not properly trained in how to handle information securely.	Possible	Minimal	Medium
Staff not properly trained in how to recognise a subject access request v FOISA	Probable	Significant	Medium
Staff who are authorised to access the cameras not familiar with the system, and with the processes for reviewing footage and extracting it if required.	Possible	Minimal	Medium
Staff not trained on how to handle a request for information from the Police.	Probable	Significant	Medium
Data breach, safeguards not in place to protect the data and ensure it is stored securely.	Probable	Significant	Medium
Data breach, information is disclosed but not delivered safely to the intended recipient.	Possible	Minimal	Medium
Access to data not restricted.	Possible	Significant	Medium
Staff misuse data.	Possible	Significant	Low
Data deletion not effective or being adhered to. Retention Policy not in place or adequate. Information not being permanently deleted.	Possible	Minimum	Medium
Image quality poor and not fit for purpose.	Remote	Minimal	Low
Are there security safeguards in place to prohibit interception and unauthorised access?	Remote	Minimal	Low
Have we notified individuals using privacy notices (where applicable)	Remote	Minimal	Low
Is the correct signage in place?	Remote	Minimal	Low
Are the cameras correctly placed? Will they work after dark? Are cable elements adequately protected from the elements? In workplace, consider the expectation of privacy (i.e., in social areas).	Remote	Minimal	Low
Do we have a maintenance contract to ensure our equipment is properly maintained and up to date (security software)?	Remote	Minimal	Low
Regular review of whether CCTV is still the best solution not undertaken.	Remote	Minimal	Low
Staff invasion of privacy challenge due to positioning of cameras.	Possible	Minimal	Medium

Step 6: Identify measures to reduce risk

Identify additional measures you could take to reduce or eliminate risks identified as medium or high risk in step 5.				
Risk	**Options to reduce or eliminate risk** In addition to the existing policies in place regarding privacy, data management and staff conduct, the identified risks will be addressed by applying the measures described above at steps 2 to 4.	**Effect on Risk** [Eliminated, reduced, accepted] Reduced to an acceptable level.	**Residual Risk** [Low, medium, high] Low	**Measure Approved** [Yes/No] Yes

Step 7: Sign off and record outcomes

Item	Name/Position/Date	Notes
Measure approved by:	Alan Park, DPO, 26 April 2021	Implementation of measures checked after first month of operation.
Residual Risks approved by:	Deemed low and approved by Jim Whiston, Director, 26 April 2021.	If accepting any residual high risks, consult ICO before going ahead.
DPO Advice provided:	Agreed that processing can proceed.	DPO should advise on compliance. Step 6 measures and whether processing can proceed.
Summary of DPO Advice: Full implementation of the measures identified above required.		
DPO Advice accepted or overruled by:	Accepted by Jim Whiston Director, 26 April 2021	If overruled, you must explain the reason why.
Comments: none.		
Consultation responses reviewed by:	Not applicable, see step 3.	If your decision departs from individuals views, you must explain your reasons.
Comments: none.		
This DPIA will be kept under review by:	Alan Park, DPO	The DPO should also review ongoing compliance with DPIA.