

Data Protection Impact Assessment (CCTV)



Northwest Kilmarnock Bowling Club (the Club) operates a CCTV system. As such the Club must consider the privacy implications of such a system. There are a number of other issues The Club will also need to consider. The completion of the Data Protection Impact Assessment highlights some of the key implications.

A Data Protection Impact Assessment is also recommended by the Surveillance Camera Code of Practice which sets out the guiding principles that should be applied when CCTV systems are in place to ensure that privacy risks are minimized whilst ensuring the aims of the CCTV system are met.

The Data Protection Impact Assessment looks at the wider context of privacy taking into account Data Protection Law and the Human Rights Act. It considers the need for the CCTV system and the impact it may have on individual privacy.

The Data Protection Impact Assessment helps determine whether the proposed system can be justified as proportionate to the needs of the Club. In undertaking this Data Protection Impact Assessment, the Club has considered its obligations under Data Protection Law.

The Club recognizes that changes do occur, and, on this basis, good practice recommends that the Club review its Data Protection Impact Assessment. The Club recognizes that it is good practice to undertake a Data Protection Impact Assessment before a system is put in place and follows the surveillance commissioner's passport to compliance. The Club also has a CCTV Policy. A Data Protection Impact Assessment will typically consist of the following key steps:

1. Identify the need for a DPIA.
2. Describe the information flow.
3. Identify data protection and related risks.
4. Identify data protection solutions to reduce and eliminate the risks.
5. Sign off the outcomes of the DPIA.

Step 1: Identify the need for a DPIA

Explain broadly what 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 identified the need for a DPIA.

What is the aim of the project? – CCTV consistently delivers benefits in terms of improved health and safety and security within Clubs and similar premises. It complements other security measures which are in place within the Club.

CCTV aims to achieve the following:

- Improve the health and safety and security of members, staff, and visitors
- Protect the Club buildings and internal infrastructure
- Reduce vandalism
- Provide assistance in the detection and prevention of crime
- Assist in the effective management of the Club

The Club has updated its Privacy Notice for its CCTV system. The Privacy Notice highlights what personal information is used and the lawful basis for using this personal information. It also highlights who the Club will share the personal information with and how long the information will be kept. The Privacy Notice documents what rights an individual has regarding their personal information.

Step 2: Describe the processing

Describe the nature of the processing: how will you collect, use, store and delete data? What is the source of the data? Will you be sharing data with anyone? You might find it useful to refer to a flow diagram or other way of describing data flows. What types of processing identified as likely high risk are involved?

How will you collect, use, store and delete data? – The CCTV system will provide the Club with pictures from 4 fixed based cameras located on the Club building and the images will be transmitted/captured on a digital video recorder (DVR). The CCTV system is operational 24 hours a day, 7 days a week.

The images are transmitted to a digital video recorder which is housed in the Bar area. Access is restricted via a locked door. Access to the Club is via a secure door entry system. The images are stored on the hard drive of the digital video recorder.

The transmitted images can be viewed live in the Bar area on a video screen by authorised persons, the video screen cannot be seen by customers at the Bar. Images can also be viewed securely on Smart Devices to persons authorised by the Committee. This is documented in the Home's CCTV Policy. This helps to maintain site security, access control, member and staff safety.

What is the source of the data? – The CCTV system provides still/video pictures, which are transmitted from cameras positioned in various locations throughout the Club. All of the CCTV cameras are fixed on a particular scene. The location of the CCTV cameras are as follows:

- 1 Internal fixed camera located in the Bar
- 1 Internal fixed camera located in the corridor outside the Bar
- 1 Internal fixed camera located in the committee room
- 1 External fixed camera facing the main entrance
- 1 External fixed camera facing the exit to the green from the Lounge
- 1 External fixed camera facing the entrance gate
- 1 External fixed camera facing the car park above the defibrillator cabinet
- 1 External fixed camera facing the bin store area

Will you be sharing data with anyone? – The information is used to ensure the health and safety and security of members, staff, and visitors. They can be used to detect

unauthorized visitors, and protection of damage to Club assets. The information may be shared with the Committee and the Police for investigation and enforcement purposes.

Disclosure of data is covered by the Club's internal processes which are fully compliant with relevant legislation and Codes of Practice (please see the Club's CCTV Policy).

What types of processing identified as likely high risk are involved? – Recording of images. Storage of images securely. Appropriate data retention applied to the images.

The digital video recorder is in the Bar area which is locked when unoccupied. Access to the images is password protected.

Data Management controls include passwords to the CCTV system. (see comment above)

Individuals can request copies of CCTV data which contains their personal information by submitting a subject access request.

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 are affected? What geographical area does it cover?

What is the nature of the data? – The CCTV data captured are still and video recordings.

Special Category data? – By default the CCTV may be picking up special category data including race/ethnic origin and the health of an individual

How much data is collected and used and how often? – The CCTV system is operational 24 hours a day, 7 days a week.

How long will you keep the data for? – Images will be retained for 30 days unless requested as part of an incident and then stored on archive for the period of the investigation process or for 12 months whichever is the lesser. The data will be deleted after 30 days.

Scope of data obtained? – The CCTV images are obtained within the confines of the Club grounds.

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)?

What is the nature of your relationship with the individuals? – The Club provides leisure facilities to its members and guests and may receive a number of visitors on a daily basis including contractors.

How much control will they have? – The Club does inform members, staff, and visitors that CCTV is in use by installing signs detailing their presence. One is located to the front of the Club and internal signs are also provided. These signs contain details of who the data controller is i.e., the Club and the contact email address.

The CCTV system is capable of identifying individuals from the system and the images can be used in both criminal and civil court cases.

If a Subject Access Request is made data may be downloaded or copied for release to the data subject or a third party (in the case of a Data Protection request). Each request for data must be requested via a signed data release form.

Do they include children or other vulnerable groups? – Cameras are in areas where members and staff have access. Cameras are not located in areas where privacy is expected. There are no cameras in toilet areas, changing rooms, and there are no cameras aimed at private areas such as residents' houses, etc. CCTV signage should be clearly visible from the street.

Are there prior concerns over this type of processing or security flaws? – The Club has a CCTV Policy. The system is operated in line with relevant legislation and the Surveillance Camera Code of Practice (consideration respecting data retention).

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

The CCTV system is proportionate and justified. It also achieves for the Club the following benefits:

1. demonstrates a duty of care to its members, staff, and visitors
2. protects the fabric of the Club both externally and internally
3. provides assistance in the detection and prevention of crime
4. to assist in managing the Club

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?

The CCTV system was installed in 2022 The system has 8 cameras.

The decision to install and expand the CCTV system was agreed by the Club Committee.

This has been communicated to members and the public via the Club's CCTV Privacy Notice. This will be published on the Club's website.

Step 4: Assess necessity and proportionality

Describe compliance and proportionality measures, in particular: what is your lawful basis for processing? Does the processing actually 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?

What is the lawful basis for processing? – The lawful basis for processing is contained in the Club’s Privacy Notices. The lawful basis includes the following:

- The Common Law Duty of Care
- Health and Safety at Work Act

Does the processing achieve your purpose? – Cameras are in areas where members and staff have access. Cameras are not located in areas where privacy is expected.

Is there another way to achieve the same outcome? – To support Club security, improved lighting and other improvements have been put in place.

How will you prevent function creep? – The lawful basis for processing will be contained in the Club’s Privacy Notice (CCTV). Where there have been material changes to the way CCTV is used, the Club will undertake a review of its CCTV system to ensure compliance and mitigate against ‘function creep.’

How will you ensure data quality and data minimisation? – Consider the source of the data. The Club will consider developing a separate data retention policy which identifies data retention periods for CCTV. However, the Club will note data retention periods as specified in CCTV Policy Notice. The Club will continue to be compliant with its CCTV Policy.

What information will you give the individuals? – The Club will inform members, staff and visitors that CCTV is in use by installing signs detailing the scheme and its purpose, along with contact details. The Club does have a Privacy Notice for its CCTV.

How will you help them support their rights? – The Club has a Subject Access Request procedure in place to ensure compliance with Data Protection Law. CCTV signage states contact details. The Club will continue to be compliant with its Data Protection Policy.

Step 5: Identify and assess risks

| Describe source of risk and nature of potential impact on individuals. Include associated compliance and corporate risks as necessary. | Likelihood of harm | Severity of harm | Overall risk |
|---|------------------------------|--------------------------------|---------------------|
| <p>Positioning of CCTV cameras at entrance points to the Club and the issue of privacy</p> <p>Housing of CCTV cameras outside and ingress of water</p> <p>Ongoing maintenance of CCTV equipment preventing breakdowns, etc.</p> <p>CCTV policies and procedures not in place leading to inconsistencies, etc.</p> <p>Appropriate CCTV signage in place which conforms to industry standards</p> <p>Training not undertaken by those using CCTV</p> <p>Privacy Notice</p> <p>Noncompliance when upgrading the Club's CCTV system</p> | Remote, possible or probable | Minimal, significant or severe | Low, medium or high |
| | Remote | Minimal | Low |
| | Possible | Minimal | Low |
| | Possible | Medium | Medium |
| | Remote | Minimal | Low |
| | Remote | Minimal | Low |
| | Possible | Medium | Medium |
| | Remote | Minimal | Low |
| | Possible | Medium | 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 | Effect on risk | Residual risk | Measure approved |
| | | Eliminated reduced accepted | Low medium high | Yes/no |
| CCTV & ingress of water | Use of waterproof enclosures | Reduced | Low | Yes |
| CCTV Maintenance | Maintenance contract in place with Security Services | Reduced | Low | No |
| CCTV Policies & Procedures | Policies and Procedures insitu | Reduced | Low | Yes |
| Training | Undertaken in GDPR and Information Security | Reduced | Low | No |
| Privacy Notices | Update the Privacy Notices to include reference to CCTV | Reduced | Low | Yes |

Step 7: Sign off and record outcomes

| Item | Name/date | Notes |
|--------------------------------------|----------------------|---|
| Measures approved by: | Management Committee | System Manager to report to Committee |
| Residual risks approved by: | Management Committee | If accepting any residual high risk, consult the ICO |
| DPO advice provided: | Not Required | Due to nature of CCTV system advice is not deemed necessary. |
| Summary of DPO advice: | | |
| DPO advice accepted or overruled by: | N/A | If overruled, you must explain your reasons |
| Comments: | | |
| Consultation responses reviewed by: | N/A | If your decision departs from individuals' views, you must explain your reasons |
| Comments: | | |
| This DPIA will kept under review by: | Data Protection Lead | The DPL should also review ongoing compliance with DPIA |