



## CCTV

Jackie Howe, Chief Executive, National Golf Club Advisory Association, discusses the use of CCTV cameras.

Recently there seems to be an upsurge in thefts from golf clubs, particularly of silverware in the form of trophies.

Whether or not CCTV cameras either helps deter such a theft, or enable the thieves to be caught is a moot point.

However, it is as well to know your rights and obligations if you were to install CCTV. This article is a précis of the Information Commissioners Office CCTV Code of Practice. The original can be seen on line at [ico.org.uk](http://ico.org.uk).

The code of practice is published under Topic Guides. Whilst we will also give an indication of whether or not you need to register with the ICO, there is a flow chart on that site which can be easily followed notifying whether or not you have to register and giving you the opportunity to do so. At first sight it would seem that most members clubs would not have to register, but it is a matter for each club to make appropriate enquiries.



The processing of information from the CCTV is governed by the Data Protection Act 1998. That Act not only creates obligations for organisation but it gives individuals rights, such as the right to gain access to their details. A brief overview is as follows:

- 1 Personal data shall be processed fairly and lawfully and, in particular, shall not be processed unless –
  - a) at least one of the conditions in Schedule 2 is met – in this case the processing is necessary for the purpose of legitimate interest of the data controller and
  - b) in the case of sensitive personal data, at least one of the conditions in Schedule 3 is also met – in this case it would be where the processing is necessary for the purpose of or in connection with any legal proceedings (including prospective legal proceedings), as necessary for the purpose of obtaining legal advice, or is otherwise necessary for the purposes of establishing, exercising or defending the equal rights.
- 2 Personal data shall be obtained only for one or more specified and lawful purposes, and shall not be further processed in any manner incompatible with that purpose or those purposes.
- 3 Personal data shall be adequate, relevant and not excessive in relation to the purpose or purposes for which they are processed.

- 4 Personal data shall be accurate and, where necessary, kept up to date.
- 5 Personal data processed for any purpose or purposes shall not be kept for longer than is necessary for that purpose or those purposes.
- 6 Personal data shall be processed in accordance with the rights of data subjects under this Act.
- 7 Appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data.
- 8 Personal data shall not be transferred to a country or territory outside the European Economic Area unless that country or territory ensures an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data.

The Code covers the use of CCTV and other systems which capture images of identifiable individuals or information relating to individuals for amongst other things potentially taking some action in relation to an individual, eg handing the images over to the Police to investigate a crime.

### Should we have CCTV?

In the Code it is recommended that careful consideration should be given as to whether to use it. Account should be taken of the benefits which could be gained and whether better solutions exist and, finally, what effect it may have on individuals. An example given is where there are cars in a car park that are frequently damaged or broken into. It should be considered whether improved lighting would reduce the problem more effectively than CCTV.

The consideration does not have to be extensive or time consuming but relates to the size of the proposed scheme. The examples given of an impact assessment include:

- ☹ Who will be using the CCTV images?
- ☹ Who will take legal responsibility under the DPA (the Data Controller)?
- ☹ What is the purpose for using CCTV?
- ☹ What are the problems it is meant to address?
- ☹ What are the benefits to be gained from its use?
- ☹ Can CCTV technology realistically deliver these benefits? Are there any less privacy intrusive solutions, such as improved lighting which could achieve the same objects?
- ☹ Do you need images of identifiable individuals or could the scheme use other images not capable of identifying the individual?
- ☹ Will a particular system work being considered to deliver the desired results now and in the future?

Appendix 2 of the Guidance gives a ‘tick’ list for users of limited CCTV systems monitoring small retail and business premises.

	Date Checked	By	Date of next Review
Notification has been submitted to the Information Commissioner and the next renewal date recorded.			
Named individual responsible for the operation of the system.			
A system has been chosen which produces clear images which 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).			
Images from this CCTV system are securely stored, where only a limited number of authorised persons may have access to them.			
The recorded images will only be retained long enough for any incident to come to light (eg for a theft to be noticed) and be investigated.			
Except for law enforcement bodies, images will not be provided to third parties.			
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.			
Regular checks are carried out to ensure that the system is working properly and produces high quality images.			

**Administration of CCTV**

For a small organisation this can be relatively straight forward. There will have to be a Data Controller who is responsible for compliance with the DPA.

You will also need clear procedures to determine how you use the system in practice. This will involve the Data Controller ensuring that the terms of the Data Protection Act are complied with.

**Selecting and Siting the Cameras**

Consideration will have to be given as to the purpose for the installation of CCTV. Consideration should be given as to whether it is necessary to get a clear identification of the face of any person and if so to ensure that the images provided by the cameras are adequate to do this.

**Storing Images**

Any 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, the material



can be used as evidence in Court. This is obviously something you need to agree with your CCTV provider.

## Disclosure

If the purpose of the CCTV was, for example, to monitor thefts from vehicles, it will be appropriate to disclose images to law enforcement agencies where a crime needs to be investigated. It would not, however, be appropriate to disclose images of identified individuals for any other reason.

A judgment has to be made about disclosure by the Data Controller. That person can refuse a request for information unless there is an overriding legal obligation such as a Court Order or Information Access Rights. Once an image has been disclosed to another body, such as the Police, then they become Data Controller of that image and they are responsible for complying with the DPA in relation to any further disclosures.

## How Long Do I Need to Keep Images

There is no specific period. Only sufficient for the purpose for which you have installed a CCTV.

## Letting People Know

If a CCTV camera or system is in operation there should be an appropriate warning sign both outside and where the CCTV is situated. The sign does not need to say who is operating the system if this is obvious.

## Access Requests

Individuals whose images are recorded have a right to view the images of themselves unless they agree otherwise to be provided with a copy of the images. This must be provided within 40 days of receiving a request. You can charge up to £10.00 in dealing with that request.

## Other Responsibilities

Staff operating the CCTV system need to be aware of two further rights that individuals have under the DPA. They need to recognise a request from an individual to prevent processing likely to cause substantial and unwarranted damage or distress (Section 10 DPA) and one to prevent automated decision taken in relation to the individual (Section 12 DPA). In practice neither of these are likely to occur.

### ***Golf Club Management: July 2014***

*[This document is prepared for guidance and is accurate at the date of publication only. We will not accept any liability (in negligence or otherwise) arising from any member or third party acting, or refraining from acting, on the information contained in this document.]*

***For further help and advice please contact:  
National Golf Clubs Advisory Association,  
The Old Threshing Barn, Homme Castle Barns,  
Shelsley Walsh, Worcestershire WR6 6RR***

***Tel: 01886 812943 E-mail: [info@ngcaa.co.uk](mailto:info@ngcaa.co.uk)***

