

Policy Name: CCTV Policy

DPC approved: 16th January 2025

CCTV Policy

1. Introduction

- 1.1 This policy sets out how Dalton Parish Council (DPC) approach to the use of CCTV in the workplace and the affects on employees and volunteers.
- 1.2 DPC has a duty under the data protection regulations to ensure that the images captured by the CCTV system at both Parish Hall and Sunnyside Community Centre comply with the Information Commissioner's Office (ICO) CCTV Code of Practice. This document details how the images captured by the CCTV system will be managed.
- 1.3 Cameras are sited to ensure they cover DPC's premises and vulnerable public-facing areas as far as is possible including the main halls, car park and outside around the building.
- 1.4 DPC seeks to operate its CCTV system in a manner that is consistent with respect for the individual's privacy.
- 1.5 All images recorded by the CCTV system remain the property and copyright of DPC.

2. Purpose of CCTV

- 2.1 CCTV cameras are installed for the following reasons:
 - i. The prevention, reduction, detection and investigation of crime and other incidents;
 - ii. To ensure, as far as is reasonably possible, the safety of staff, volunteers and visitors to the premises.
- 2.2 DPC will not use CCTV for monitoring the work of employees or finding out whether or not they are complying with the organisation's policies and procedures other than in line with 6.1 below.
- 2.3 CCTV will be installed only if it is a necessary and proportionate way of dealing with a problem. DPC will ensure that all cameras are set up in a way that ensures that there is minimal intrusion of staff privacy, and that any intrusion is fully justified.
- 2.4 Signs are placed at prominent points on the premises in order to inform staff, volunteers, visitors and members of the public that CCTV is in operation.

3. Nominated Data Controller

3.1 The system and its use will be managed by the Clerks or their nominated substitute. Any requests for images must be made to the Clerks in writing and they will decide whether the request is appropriate and respond to the request accordingly.

4. Authorised Users

4.1 The only staff authorised to use the system are the data controller or their nominated substitute.

5. Limits on the use of CCTV

- 5.1 CCTV will not be operated in toilets, private offices or changing rooms, unless this is necessary for the investigation of a serious crime or there are circumstances in which there is a serious risk to health and safety or to the operation of the employer's business. CCTV will be used in this way only where it is a proportionate means of achieving the aim in the circumstances.
- 5.2 Covert CCTV will only ever be set up for the investigation or detection of crime or serious misconduct. The use of covert CCTV will be justified only in circumstances where the investigator has a reasonable suspicion that the crime or serious misconduct is taking place and where CCTV use is likely to be a proportionate means of securing evidence.
- 5.3 Covert recording will only take place if informing the individual/s concerned would seriously prejudice the reason for making the recording and where there are reasonable grounds to suspect that illegal or unauthorised activity is taking place. Any such monitoring will be fully documented and will only take place for a limited and reasonable period.

6. Evidence from CCTV footage

6.1 CCTV evidence may be used against an employee in disciplinary proceedings only where such evidence tends to show, in the reasonable belief of the employer, that he or she has been guilty of serious misconduct. The employee will be given a chance to see and respond to the images in these circumstances.

7. Storage of CCTV footage

- 7.1 Images from CCTV footage will be securely stored on the server and only authorised personnel will have access to them. The images will be retained only long enough for an incident to come to light and any investigation to be conducted.
- 7.2 The cameras installed provide images that are of suitable quality for the specified purposes for which they are installed and all cameras are checked periodically to ensure that the images remain fit for purpose and that accurate dates and times are being recorded.

8. Access to CCTV footage

- 8.1 Employees and volunteers whose images are recorded (known as the Data Subject) have a right to view images of them and to be provided with a copy of the images. In order to locate the image/s on the system, sufficient detail must be provided by the individual (including date and time of the image if known) in order to allow the relevant image/s to be located and the Data Subject to be identified.
- 8.2 Individuals will be allowed access to such images within one calendar month of the written request.
- 8.3 Where DPC is unable to comply with a request for CCTV footage without disclosing the personal data of another individual who is identified or identifiable from that information,

it is not obliged to comply with the request unless satisfied that the other individual has provided their express consent to the disclosure or, if it is reasonable given the circumstances, to comply without the consent of the individual

9. Access to and disclosure of images to third parties

- 9.1 A request for images made by a third party must be made in writing to the Clerks.
- 9.2 Images will only be disclosed to third parties in particular circumstances, such as when a disclosure is required by law in relation to the prevention or detection of a crime.

10. Operation and Monitoring of the system

- 10.1 The system itself will run continuously with images captured being stored on a rolling 28 day basis. There is no need for regular monitoring and the system does not need to be actively managed, however, monthly checks by the data controller or nominated substitute will be made to ensure the system is functioning correctly.
- 10.2 Where an image is required to be held for a longer period of time, the Clerks or their nominated substitute will be responsible for authorising such a request.
- 10.3 The procedures and policies stated above will be ratified by the full council and reviewed on a yearly basis.

Date of review: Jan 2026