

## DIGITAL OFFICE CENTRES

### CCTV POLICY

**Date: 1 March 2022**

## Summary

Introduction .....	3
1. General Policy and Guidelines .....	3
2. Retention .....	3
3. Security and Authorised Use .....	4
4. Redaction/Pixelation .....	4
5. Access to and disclosure of images to third parties .....	5
6. Questions.....	5

## Introduction

This Policy sets out the basic conditions of use for Closed Circuit Television (CCTV) systems by Digital Office Centres.

All persons involved in the planning, supervision or operation of such a CCTV scheme will familiarise themselves with this document from the outset.

This Policy document seeks compliance with Irish Law (Data Protection Acts, 1988, 2003 and 2018) and European Law (Regulation (EU) 2016/679 of the European Parliament and of the Council (GDPR).

In order for this Policy to remain relevant to the day to day activities of CCTV operation, it needs to be updated as practice and understanding of the laws in this area develop. Accordingly, this Policy will be kept under review to ensure that it remains relevant in the context of changes in technology, and compliant with any developments in this area.

## 1. General Policy and Guidelines

- 1.1 CCTV is used by Digital Office Centres as part of the operational system for safety, security and crime prevention.
- 1.2 The primary purposes of having CCTV are for security, crime prevention and health and safety reasons. Recorded images will only be used in particular circumstances. These include a security breach or suspected breach of law; for employee personal protection; a health and safety incident; or where recourse to CCTV images is necessary in the course of any investigation carried out by Digital Office Centres. In the case of an investigation, the CCTV footage may be required to prove or disprove any concerns regarding a customer, employee(s), any third party or the workplace itself.
- 1.3 For the avoidance of doubt, CCTV can be used as evidence in disciplinary investigation
- 1.4 Digital Office Centres operates cameras that are at various locations on the premises. Signage is displayed to highlight the presence of CCTV cameras. These operate on a [24-hour basis, seven days a week.] basis.

## 2. Retention

- 2.1 Recorded images and associated information will be retained for a maximum of 30 days from the date of recording. After a period of up to a maximum of [30 days, the system will automatically overwrite images. However, Digital Office Centres reserves the right to retain images for a longer period where there are objective reasons for doing so.

2.2 Where CCTV is retained for a longer period in the context of an investigation, then it will only be retained for as long as is required for the duration of the investigation/proceedings/disciplinary proceedings, including any court proceedings or appeals process, and will be permanently deleted once these proceedings/appeals are concluded in full.

### **3. Security and Authorised Use**

3.1 CCTV footage will be retained securely. The CCTV storage medium will be kept securely and only accessed by designated individuals. Unauthorised accessing of CCTV is strictly prohibited.

3.2 Those employees with responsibility for processing CCTV images must only do so in line with established procedures and must ensure the security of the data at all times.

3.3 CCTV footage will only be retained and /or used for the specific purpose(s) for which it was captured.

3.4 Any employee/manager who uses the CCTV system /CCTV images in an unauthorised manner may be subject to disciplinary action up to and including dismissal. Unauthorised use is any processing incompatible with the data's original purpose including, but not limited to:

3.4.1 Disclosure of images containing Personal Data to an unauthorised third party, including other employees.

3.4.2 Unauthorised processing of Personal Data in the form of copying the images on to a disk, website or print format.

3.4.3 Unauthorised circulation of images containing Personal Data by email, phone or posting of images containing personal data on the internet.

### **4. Redaction/Pixelation**

4.1 Circumstances might arise where an employee or other individual requests a copy of CCTV footage in which their image is captured. Such a request should be received in writing specifying as accurately as possible the time periods/time frame of the CCTV footage being requested. Where other individuals are identifiable on the footage, then in all cases their image will be redacted/pixelated before a copy of the footage is passed over to the individual requesting a copy of the footage, unless the permission of the other individual is obtained.

## 5. Access to and disclosure of images to third parties

5.1 Access to and disclosure of images recorded by the CCTV system is carefully monitored. Access to images by third parties will only be allowed in limited and prescribed circumstances permitted by legislation. Such circumstances may include the disclosure of Personal Data in order to

5.1.1 Prevent injury or damage to property.

5.1.2 Meet legal requirements.

5.1.3 Obtain legal advice, or for the purpose of legal proceedings.

5.1.4 Meet a request from, or with the consent of, the data subject, or a person acting on his or her behalf.

5.2 Garda/police requests for copies of CCTV footage or requests from legally authorised Regulatory agencies should only be acceded to where a formal written request is provided to Digital Office Centres by a Garda/police stating that they are investigating a criminal matter or a regulatory matter where they are permitted to access such data. In some instances, where the Gardaí or a regulator indicate that the viewing of CCTV footage is deemed urgent, then Digital Office Centres may facilitate a viewing without the formal written request but on the understanding that the formal written request will be sent by the Gardaí or relevant regulator as soon as is reasonably practicable.

5.3 Digital Office Centres also reserves the right to disclose Personal Data to specific third parties where there are objective business reasons for doing so. Such third parties may include:

5.3.1 Insurance providers.

5.3.2 Legal advisers.

5.3.3 Pension and medical insurance providers.

5.3.4 Security providers.

## 6. Questions

6.1 Any queries in relation to this policy may be directed to the site manager of Digital Office Centres

*Please note the terms of this policy may be changed from time to time to reflect the requirements of ourselves, our suppliers and partners as well as legal and regulatory changes and you should make sure you keep it under regular review.*