# Use & Access to CCTV Recordings – Policy

## Table of Contents

## Introduction

The Midcounties Co-operative ("the Society") places the health, safety and welfare of its colleagues, members, customers, contractors and visitors amongst its priorities and aims to ensure it maintains safe and secure conditions throughout its premises.

To assist with these responsibilities, the Society uses closed circuit television ("CCTV") cameras from which both recorded and live images may be viewed remotely.

The Society may also, during the course of business, view and review CCTV images captured in branches and stores for the purpose of improving customer service, and for matters of operational compliance.

## Policy objective

This policy sets out the guidelines colleagues must follow to ensure the Society complies with applicable legislation in the UK relating to the processing of personal data, eg. **The Protection of Freedoms Act**; the ICO's **CCTV Code of Practice**, The **General Data Protection Regulation** (the 'GDPR') and the **Data Protection Act 2018** (the 'DPA').

The **Information Commissioner's Office** ("**ICO**") is the UK's Supervisory Authority for data protection matters and is responsible for enforcing the applicable legislation in respect of the processing of any personal data, which includes the processing of CCTV images.

This policy should be read in conjunction with the Society's **CCTV Policy & Guidance for Managers**, the **Data Protection Policy** and other related policies and guidance for colleagues put in place by the Society and concerning the processing of people's personal data.

## Legal obligations

There are key principles which UK businesses must keep in mind when operating CCTV cameras in their premises:

- **Maintain mutual trust and confidence**: as employers, businesses should not act in a way, without reasonable and proper cause, which is likely to destroy or damage the relationship of mutual trust and confidence between themselves and their employees. If they do so, there is a risk that employees may resign, and/or initiate a legal claim against the Society, which could lead to litigation.

- **Comply with data protection law**: employers, and businesses generally, should act in accordance with applicable data protection law which protects people's rights in respect of their personal data, such as images of them

captured by CCTV cameras. Breaches of data protection law may lead to both financial and reputational damage for the Society.

Data protection law provides that when CCTV cameras are in use for monitoring purposes, then we must tell people they may be recorded. This is usually done by displaying signs at our business premises, clearly visible and readable, explaining the reasons why CCTV cameras are in operation, and what rights people have in relation to their personal data. Colleagues may find this information also in the Colleague Handbook.

The Society's **CCTV Policy & Guidance for Managers** explains our legal obligations and provides guidance to colleagues to ensure our CCTV systems are operated in line with the law, and that Managers are aware of their responsibilities when handling people's personal data. The Policy & Guidance also explains what to do when requests for copies of CCTV footage are received either from the public or law enforcement bodies.

- **Be mindful of employees' rights under the Human Rights Act("HRA"):** while employers in the public sector should be particularly aware of the right to privacy which their employees have under the HRA as it applies directly to them, it is still equally important for employers in the private sector, such as the Society, to consider this right and to ensure that, when CCTV cameras are used for monitoring purposes, their use is not disproportionate or intrusive. In the event of litigation tribunals and courts are expected to take this aspect into account when making decisions about employees' claims.

## Why we may need to review CCTV images

The Society may need to review CCTV footage captured in any of its business premises for the following purposes:

- Crime prevention, detection and security, and assist law enforcement agencies for the apprehension and prosecution of offenders (including use of images as evidence in criminal proceedings)
- Provide reassurance to colleagues and the public against crime
- In the interest of the public's and colleagues' health and safety
- Compliance auditing
- Improve customer service
- Protection of the Society's property and assets
- Provide supporting evidence for the Society's insurance claims
- Gain evidence when investigating complaints and during disciplinaries (in the event of a formal complaint investigation)
- Provide added reassurance to colleagues of single-staffed branches.

## Justifying the use of CCTV cameras for remote monitoring

Before deciding whether to introduce CCTV cameras for remote monitoring in an area of the business, the following is taken into consideration:

- The reasons for implementing this measure, and the benefits that it will bring.
- Any negative effects that being monitored may have on colleagues. This is done by completing a risk impact assessment.
- Ensuring that the monitoring is justified. The most senior colleague of the relevant business area (COO or GGM) must agree that the CCTV monitoring is justified and **authorise the list of colleagues who will be permitted to access/view CCTV images** captured in the business premises.

## Authorising access to CCTV footage

Access to CCTV images must only be given to authorised colleagues by the relevant COO/GGM. **Usernames and passwords** issued to authorised colleagues to gain access to CCTV images must be treated as confidential and not shared with anyone.

For audit trail purposes, **it is the responsibility of the relevant business area to maintain an adequate record of the list of authorised colleagues**, as it may need to be supplied to the ICO in the event of an investigation into an alleged, or actual, personal data breach.

Authorised colleagues must receive appropriate training in the operation of CCTV images, the legal requirements associated with it, and any relevant procedures and policies.

Authorised colleagues and their Line Managers must sign the "Declaration of Confidentiality Form" which can be found in the Society's **CCTV Policy & Guidance for Managers** and forward signed copies to the Society's Data Protection Manager ("DPM")[1], to comply with audit trail requirements, at: data-protection@midcounties.coop.

Authorised colleagues can only view and use CCTV images for the purpose that has been stated by their business area, and this must be compatible with their job role and responsibilities.

Authorised colleagues must be at all times compliant with the Society's **CCTV Policy & Guidance for Managers**. Any colleague found to be in breach of the Policy & Guidance can expect disciplinary action to be taken against them, which may result in dismissal.

[1] The GDPR provides that, in certain cases, organisations must formally appoint a Data Protection Officer (DPO). For the Society, this legal obligation applies to our Energy, Phone Co-op and Healthcare businesses. The role of the DPO is carried out by the Society's Data Protection Manager (DPM).

Colleagues who no longer have the responsibility to view CCTV images or who leave their employment with the Society must have their usernames and passwords disabled as soon as their job responsibilities change, or they leave the Society.

**It is the responsibility of line managers to ensure these changes of permission are actioned timely**.

## Viewing CCTV images

CCTV footage must be viewed in a private area of the business.

An audit trail must be maintained to show who has accessed CCTV footage, and when – **it is the responsibility of line managers to maintain such records for each of the authorised colleagues**. Line managers may be asked to produce copies of such records from time to time, for audit purposes and in case there is an investigation into an alleged, or actual, personal data breach.

Storage devices used for transferring or sharing CCTV footage must have adequate security features to ensure the safe transit of personal data.

The retention and disposal of CCTV footage must be carried out in accordance with the Society's **CCTV Policy & Guidance for Managers**.

## Who to contact?

For queries relating to the processing of personal data, or any other Society's policy or guidance in relation to data protection compliance, please contact the Society's DPM by email: data-protection@midcounties.coop.

Other policies and procedures relating to the processing of people's personal data can be found on Colleagues Connect: https://colleaguesconnect.midcounties.coop/working-here/data-protection/.