# CCTV POLICY & GUIDANCE FOR MANAGERS

## 1. Policy Statement

1.1. The Society is mindful of the rights and obligations established by the **General Data Protection Regulation 2016** ("the GDPR"), the **Data Protection Act 2018** ("the Act") and any other applicable legislation in relation to the management and processing of personal data.

1.2. This Policy & Guidance should be read in conjunction with the Society's **Data Protection Policy** and other related policies put in place by the Society and concerning the processing of personal data.

1.3. Colleagues who, in the course of their job responsibilities, need to gain access to CCTV recordings captured at any of the Society's business premises, must also be familiar with the **Use & Access to CCTV Recordings – Policy**.

## 2. Introduction

2.1. The Society, as any other organisation within the private sector, is required to follow the ICO[1]'s **CCTV Code of Practice** ("the Code"), issued in 2000 and last updated in June 2017, to meet its legal obligations under the Act, when using cameras to process personal data, eg. still images and video footage of customers shopping in our Food stores, parents and children at our nurseries, customers visiting our Funeral or Travel branches etc.

2.2. This Policy & Guidance provides principles and guidance to Managers and colleagues operating CCTV systems, to ensure the Society remains compliant with data protection legislation and CCTV operating practices.

2.3. Note that the Code also covers the use of other camera-related surveillance equipment such as **Automatic Number Plate Recognition** (ANPR) – the Society currently only operates ANPR at one of its sites, however it is appropriate for Managers to be aware of this, as the number of sites operating ANPR may increase in future.

2.4. This Policy & Guidance covers acceptable practices for areas where the public have access to, and **it is the responsibility of all Managers to**

[1] Information Commissioner's Office, the UK's data protection Supervisory Authority.

**ensure that the Society complies with legally enforceable standards** that apply to the collection and processing of images relating to individuals.

## 3. How the ICO's Code of Practice applies to the Society

3.1. The recommendations contained in the Code will:

3.1.1. Help ensure that when capturing individuals' personal data, the Society complies with the Act and other relevant statutory obligations.

3.1.2. Contribute to the efficient deployment and operation of a camera system in our branches and ensure the personal data captured on sites is usable and meets its objectives.

3.1.3. Reduce reputational risks by staying within the law and avoiding regulatory action and penalties against the Society.

## 4. Breaches of Policy

4.1. All colleagues must be mindful that any misuse of personal data obtained from a digital image, or the inappropriate use of any of the Society's CCTV systems or other recording equipment, may result in disciplinary action being taken.

4.2. This Policy & Guidance relates to an Act of Law, therefore failure to comply with it may result in legal proceedings being initiated.

## 5. Responsibilities: general

5.1. **The Society is responsible, as the Data Controller**, for the way people's personal data is processed, and for dealing with the ICO as and when required. For clarity, "processing" means capturing, storing, copying, sharing or deleting CCTV footage.

5.2. **All Managers are responsible** for ensuring they – and any other colleague(s) within their teams designated to operate the CCTV system at any of our business premises – have read and understood this Policy & Guidance.

5.3. Any colleague operating a CCTV system must be aware of the need for confidentiality and that recorded personal data must be secure.

5.4. Managers should undertake regular review of the procedures to ensure that the provisions of this Policy & Guidance are being complied with.

5.5. Any queries about data protection compliance should be addressed to the relevant **Data Protection Champions** ("DPCs") in the first instance or, alternatively, to the Society's **Data Protection Manager ("DPM")**[2].

## 6. MANAGERS' RESPONSIBILITIES: monitoring CCTV operations

6.1. **Managers are responsible for the control of CCTV information we collect**, for example, to decide what is to be recorded and how the personal data should be stored in store/branch, and in due course disposed of.

6.2. **Managers are also responsible for assessing the legitimacy of any request made by customers, or third parties,** to obtain copies of CCTV footage from any of the Society's business groups, based on the guidelines given in this Policy & Guidance.

If in doubt, Managers should always check with their business group's DPC in the first instance. Alternatively, colleagues may contact the Society's DPM.

6.3. Any branch that has outsourced the processing of personal data captured by our CCTV cameras must have a **written service/data sharing contract** in place with the third party provider, which clearly defines responsibilities to ensure that personal data is only processed in accordance with the Society's instructions, and should also include guarantees about security, such as storage and employing properly trained staff.

6.4. Managers should contact the Society's **Specialist Services Group** (Andrew Stride, Head of Legal Services) if they think they may need a contract, or if they require further assistance on existing contracts with third parties.

6.5. **Managers must**:

6.5.1. Maintain a Register of CCTV requests – a template register is enclosed in **Appendix 1** to this Policy & Guidance.

**IMPORTANT** → Managers must ensure the register is kept up to date and records are made accurately and without omitting any of the required information, as the Society's DPM may be asked to produce them as

[2] Under current legislation, the Society had an obligation to formally appoint a Data Protection Officer (DPO) for its Healthcare, Phone Co-op and Energy businesses. This role is held by the Society's DPM.

audit evidence to the ICO in the event of a dispute/complaint being raised by a customer.

6.5.2. Ensure they, and any other relevant colleagues on site, sign a CCTV Declaration of Confidentiality – a template declaration can be found in **Appendix 2** to this Policy & Guidance.

6.5.3. Ensure all signed declaration are scanned and saved electronically, and a copy forwarded to data-protection@midcounties.coop.

6.5.4. Ensure they, and all relevant colleagues on site, are fully trained and understand how to use the recording equipment on site. Training should be based on the operating instructions booklet left on site by the CCTV system's installer.

## 7. MANAGERS' RESPONSIBILITIES: storage, retention and disposal of CCTV records

### 7.1. Storage

7.1.1. **Managers must** ensure that, if any CCTV footage recorded on site is kept in store, the integrity of the personal data is maintained, eg. locked in a cabinet only accessible to designated staff. This is to ensure that the privacy rights of the individuals recorded on the footage are protected.

7.1.2. Not all our recording systems on site are fitted with a USB port to allow for downloading, and storing, of images on USB memory sticks. Where this is not available, managers should use DVDs instead.

**Managers must** have particular care when personal data captured by our CCTV cameras is transferred on any mobile memory device (eg. USB memory sticks) to ensure the device is only given to the intended and legitimate recipient – this is likely to be the person captured in the footage, or someone acting on their behalf (subject to certain conditions), or a law enforcement body.

**IMPORTANT →** The release of CCTV footage to any individual and/or company/organisation - other than law enforcement representatives and bodies - must be authorised by the Society's DPM.

7.1.3. **Managers must** ensure that access to CCTV footage is restricted to the relevant colleagues only. The Society's **Use & Access to CCTV Recordings – Policy** explains this in more detail.

### 7.2. Retention and disposal

7.2.1. The Society has adopted a **maximum period of 30 days** for the retention of CCTV footage captured in any of its stores and branches. This is in line with current best practice in several industries, and the approach taken by other societies as well as by most organisations similar in size and type of business to the Society.

7.2.2. After 30 days, and if not already automatically deleted by the system, **Managers must** dispose of the footage securely.

7.2.3. Generally, CCTV systems should automatically record over existing images, which effectively deletes the old images. However, if Managers are in doubt, or there is a need to dispose of records in any other way, they should contact their business group's DPC in the first instance to seek further guidance. Alternatively, colleagues may contact the Society's DPM.

## 8. MANAGERS' RESPONSIBILITIES: requests for disclosure made by law enforcement bodies

8.1. **Public and government bodies, as well as law enforcement bodies, such as the Police, or crime and fraud investigation units**, often need access to CCTV recordings captured in business premises, to support an on-going **criminal investigation** or a **personal injury case** suffered by members of the public or staff. Requests to access the Society's CCTV recordings may therefore be made to a store or branch – these requests are sometimes referred to as official disclosure requests, and are dealt with in a similar way to Subject Access Requests made by members of the public.

8.2. Generally, police officers would walk into a branch and make the request verbally to colleagues. When receiving these requests in any of our stores or branches, whether they relate to CCTV footage captured within the trading premises or in its car parking area, **Managers must**:

8.2.1. Ensure the CCTV footage is not disposed of or deleted, and immediately transfer a copy of the relevant footage onto a USB memory stick or a DVD, depending on the recording system's available facilities.

8.2.2. Complete the Register of CCTV Requests (see Appendix 1).

8.2.3. Release the CCTV footage to the requesting law enforcement representative (eg. Police officer).

8.3. **If the CCTV footage is no longer available** at the time it is requested, for example because it has already been disposed of/overwritten because the

request refers to footage older than 30 days, **Managers must** explain to the law enforcement representative that the footage is no longer available, and why.

## 9. MANAGERS' RESPONSIBILITIES: requests for disclosure made by members of the public or other private organisations

9.1. The Society has seen a significant increase in the number of requests for disclosure of CCTV footage made by motor insurances, accident claims companies and other similar private organisations acting on behalf of their clients.

In most cases, the request relates to damages to cars occurred in our stores' car parks while customers are shopping in our stores and branches.

9.2. Under data protection law, **the Society does not have an obligation to release any CCTV footage that does not constitute personal data**.

What does this mean?

It means that CCTV footage merely showing unidentifiable cars driving into each other, or being scratched or bumped into while being parked does not constitute personal data, **as long as neither people nor cars' registration numbers are recognisable in the footage**, and as such there is no obligation to release it.

**IMPORTANT** → it is a **breach of data protection law** to disclose someone's personal data to unauthorised third parties - for example friends, co-workers or family members. Personal data is precisely that - personal, and it should not be disclosed inappropriately (regardless of how genuine, or insistent, the third party may seem).

9.3. **When receiving these requests** in any of our stores and branches, **Managers must**:

9.3.1. Complete the Register of CCTV Requests (see Appendix 1) for good record-keeping, and in case the incident becomes part of a criminal investigation in future;

9.3.2. Advise the person, or organisation, making the request to contact the Society's DPM, as further evidence may be needed before the CCTV footage can be released;

**IMPORTANT** → Managers and colleagues in stores and branches **must not** immediately confirm to the person or organisation making the

request that the CCTV footage will be provided, as sometimes exceptions apply in law when the Society may not be able/willing to release the CCTV footage.

9.3.3. Locate and secure from deletion the CCTV footage, in case it becomes evidence in a criminal investigation, and it needs to be released to law enforcement bodies. The footage should be transferred onto a USB memory stick (or other suitable memory storage device e.g. DVD) and stored securely.

**If the footage you have saved is not needed within the following 30 days**, it should be deleted and/or disposed of securely in line with this Policy & Guidance.

## 10. Location of CCTV Cameras

10.1. Both permanent and movable cameras should be positioned in a way that they don't capture images in irrelevant areas not intended for surveillance, for example neighbouring private properties, or colleagues' changing areas.

10.2. Managers who are not sure whether the CCTV camera(s) in their branch are properly positioned should contact the Society's Specialist Services Group for further assistance.

## 11. Letting People Know

11.1. The Society has a legal obligation to let people know when they are being filmed by our CCTV cameras or other surveillance systems.

11.2. Under current legislation, the Society must:

11.2.1. **Prominently place a notice to customers** in any of its trading premises (eg. a sticker on the door), advising that CCTV is in operation in the business premises. Notice must be given at the entrance of a branch because people have the right to choose whether they wish to be filmed or not before they walk in.

11.2.2. **Inform customers of their privacy rights**. This means that people have the right to know why they are being filmed, how their personal data (CCTV footage of them) will be processed, stored, shared and disposed of by the Society; the details of the systems' operators (ie. the company contracted by the Society to provide the CCTV equipment) and who to contact if they want more information.

The Society has produced a **CCTV Privacy Notice** for all applicable branches to use. This should be placed either on the door, visible from outside the store, or inside the store/branch in a prominent place – which means visible by customers.

A downloadable copy of the Notice can be found on Colleagues Connect: https://colleaguesconnect.midcounties.coop/working-here/data-protection/.

## 12. Further Information & Contact Details

12.1. Colleagues requiring additional guidance about this Policy & Guidance may refer to their **business group's DPCs** in the first instance. A contact list of all the Society's DPCs is available on Colleague Connect: https://colleaguesconnect.midcounties.coop/working-here/data-protection/.

12.2. Alternatively, colleagues may contact the **Society's DPM** at data-protection@midcounties.coop; Co-operative House, Warwick Technology Park, Warwick CV34 6DA.

12.3. Colleagues requiring technical assistance about operating a CCTV system on site should refer to the Society's **Specialist Services Group** at specialistservicesmanagement@midcounties.coop.

12.4. Colleagues requiring guidance on contracts with third party service providers should contact Andrew Stride, **Head of Legal Services**, at andrew.stride@midcounties.coop; tel: 01926 516 064; Co-operative House, Warwick Technology Park, Warwick CV34 6DA.

12.5. The Government's "**Guiding Principles of the Surveillance Camera Code of Practice**" are enclosed in **Appendix 3** for information.

## 13. Policy Review

13.1. This Policy & Guidance will be reviewed by the Society's DPM on a regular basis and, in any case, at least annually.

# APPENDIX 1

## REGISTER OF CCTV REQUESTS

**Branch name/Store** _____

| **Time & Date of request** | **Camera No.** (if applicable) | **Name of person/organisation making the request** | **Signature of person/organisation making the request** | **Has the CCTV footage been copied on USB device and released?** (yes/no) **If YES, indicate date of release If NO, indicate reason** |
|---|---|---|---|---|
| **Time:** | | | | ☐ **YES** ☐ **NO** |
| | | | | **Date of release:** |
| **Date:** | | | | **Reason:** |
| **Time:** | | | | ☐ **YES** ☐ **NO** |
| | | | | **Date of release:** |
| **Date:** | | | | **Reason:** |
| **Time:** | | | | ☐ **YES** ☐ **NO** |
| | | | | **Date of release:** |
| **Date:** | | | | **Reason:** |
| **Time:** | | | | ☐ **YES** ☐ **NO** |
| | | | | **Date of release:** |
| **Date:** | | | | **Reason:** |

# APPENDIX 2

## CCTV DECLARATION OF CONFIDENTIALITY

All matters relating to the CCTV system, its installation, location of cameras, types of equipment used and the recorded images remain confidential.

As an authorised Operator of the system I understand that I may only discuss this with the appropriate authorities and the relevant Society's management.

### Colleague's Declaration

I confirm that I have read the Society's CCTV Policy & Guidance to Managers, and that I have received the relevant training.

I also confirm that I fully understand the procedures and that I am able to competently carry out the required task(s). Finally, I understand that I may face disciplinary action if I do not adhere to the training I have received and the relevant Society's policies and procedures.

Colleague's signature_____ Date_____

Name in full: _____

### Manager's Declaration

I confirm the above colleague has been properly trained and has demonstrated full competence to operate the CCTV system on site, is fully aware of her/his legal responsibilities with regards the handling of personal data and has read and understood the relevant policies and procedures.

Manager's signature_____ Date_____

Name in full: _____

# APPENDIX 3

## THE GUIDING PRINCIPLES OF THE SURVEILLANCE CAMERA CODE OF PRACTICE

System operators should adopt the following 12 guiding principles:

1. Use of a surveillance camera system must always be for a specified purpose which is in pursuit of a legitimate aim and necessary to meet an identified pressing need.

2. The use of a surveillance camera system must take into account its effect on individuals and their privacy, with regular reviews to ensure its use remains justified.

3. There must be as much transparency in the use of a surveillance camera system as possible, including a published contact point for access to information and complaints.

4. There must be clear responsibility and accountability for all surveillance camera system activities including images and information collected, held and used.

5. Clear rules, policies and procedures must be in place before a surveillance camera system is used, and these must be communicated to all who need to comply with them.

6. No more images and information should be stored than that which is strictly required for the stated purpose of a surveillance camera system, and such images and information should be deleted once their purposes have been discharged.

7. Access to retained images and information should be restricted and there must be clearly defined rules on who can gain access and for what purpose such access is granted; the disclosure of images and information should only take place when it is necessary for such a purpose or for law enforcement purposes.

8. Surveillance camera system operators should consider any approved operational, technical and competency standards relevant to a system and its purpose and work to meet and maintain those standards.

9. Surveillance camera system images and information should be subject to appropriate security measures to safeguard against unauthorised access and use.

10. There should be effective review and audit mechanisms to ensure legal requirements, policies and standards are complied with in practice, and regular reports should be published.

11. When the use of a surveillance camera system is in pursuit of a legitimate aim, and there is a pressing need for its use, it should then be used in the most effective way to support public safety and law enforcement with the aim of processing images and information of evidential value.

12. Any information used to support a surveillance camera system which compares against a reference database for matching purposes should be accurate and kept up to date.