CCTV POLICY AND GUIDANCE FOR MANAGERS

1. About this Policy

1.1. The Society uses CCTV cameras to view and record individuals on and around our premises in order to maintain a safe environment for colleagues, customers, members and visitors. However, we recognise that the images of individuals recorded by CCTV cameras are personal data which must be processed in accordance with data protection legislation. As a data controller, we have registered our use of CCTV with the Information Commissioner's Office (ICO) and seek to comply with its best practice suggestions.

1.2. This policy does not form part of any contract of employment or other contract to provide services, and we may amend it at any time.

1.3. A breach of this policy may, in appropriate circumstances, be treated as a disciplinary matter. Following investigation, a breach of this policy may be regarded as misconduct leading to disciplinary action, up to and including dismissal.

1.4. This policy applies to all employees, officers, consultants, self-employed contractors, casual workers, agency workers, volunteers and interns. It also applies to anyone visiting our premises or using our vehicles.

1.5. This Policy and 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.

1.6. 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, should also refer to the **Use and Access to CCTV Recordings – Policy**.

2. Responsibilities: general

2.1. **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.

2.2. **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 and Guidance.

2.3. CCTV footage must **not** be copied or recorded unless authorised in accordance with this Policy and Guidance.

2.4. Any colleague operating a CCTV system must be aware of the need for confidentiality and that recorded personal data must be secure. Allowing access to CCTV contrary to this Policy may result in disciplinary action being taken.

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

2.6. 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")**[1].

3. MANAGERS' RESPONSIBILITIES: monitoring CCTV operations

3.1. **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.

3.2. **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 and 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 by email: data-protection@midcounties.coop.

3.3. 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.

[1] Under current legislation, the Society had an obligation to formally appoint a Data Protection Officer (DPO) for its Utilities business. This role is held by the Society's DPM.

3.4. Managers should contact the Society's legal team by email: legal@midcounties.coop if they think they may need a contract, or if they require further assistance on existing contracts with third parties.

3.5. **Managers must**:

3.5.1. Maintain a Register of CCTV requests – a template register is enclosed in **Appendix 1** to this Policy and 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 audit evidence to the ICO in the event of a dispute/complaint being raised by a customer.

3.5.2. 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 and Guidance.

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

3.5.4. 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.

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

4.1. Storage

4.1.1. **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.

4.1.2. 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.

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

4.2. Retention and disposal

4.2.1. 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.

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

4.2.3. 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.

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

5.1. **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.

5.2. Generally, police officers would walk into a branch and make the request verbally to colleagues and follow up the request in writing. 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**:

5.2.1. Verify the identity of the police officer by requesting a copy of their police warrant card, as proof of their identity and authority.

5.2.2. 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.

5.2.3. Advise the police officer that the request must be made to the Society's DPM by email: data-protection@midcounties.coop. Upon receipt of the request by email, it will be processed and the CCTV footage can be released.

5.3. **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.

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

6.1. 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.

6.2. 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).

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

6.3.1. 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;

6.3.2. Managers and/or colleagues should **not** allow members of the public or other private organisations to view, copy or record CCTV footage in store without prior authorisation from the Data Protection team;

6.3.3. 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.

6.3.4. 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 and Guidance.

7. Location of CCTV Cameras

7.1. 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.

7.2. Managers who are not sure whether the CCTV camera(s) in their branch are properly positioned should contact Property Services for further assistance.

8. Letting People Know

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

8.2. Under current legislation, the Society must:

8.2.1. **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.

8.2.2. **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/.

9. Further Information and Contact Details

9.1. Colleagues requiring additional guidance about this Policy and 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/.

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

10. Policy Review

10.1. This Policy and Guidance will be reviewed by the Society's DPM at least every two years.

APPENDIX 1

REGISTER OF CCTV REQUESTS **Branch name/Store** _____

Time and 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 and 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: _____