# Middle Temple CCTV Policy

**January 2020**

# Introduction and Accountability

Following the Government's commitment to further regulate Closed Circuit Television ('CCTV'), the Protection of Freedoms Act 2012 ('PFA2012') provided for the development of a Code of Practice relating to CCTV, and other surveillance camera systems, and the appointment of a Surveillance Camera Commissioner.

The 'Surveillance Camera Code of Practice' ('the SCC Code'), pursuant to the PFA2012, was published in August 2013 and has been influential in the development of this policy ('the MT CCTV policy'). The MT CCTV policy will help to ensure that the Inn makes transparent decisions about the legitimacy and proportionality of any camera-based surveillance requirements.

The MT CCTV policy covers the Inn's CCTV systems and is intended to reflect the guidance issued by the Information Commissioner's Office, 'In the picture: a data protection code of practice for surveillance cameras and personal information' (see https://ico.org.uk/media/for-organisations/documents/1542/cctv-code-of-practice.pdf).

## Closed Circuit Television Systems ('the CCTV system')

The Inn is the owner of public closed-circuit television ('CCTV') systems that are currently installed on its premises. The Security Manager at the Inn retains overall responsibility for the CCTV system, in consultation with the Director of Estates and the Under Treasurer.

All images produced by the CCTV system remain the property of the Inn and are also subject to data protection regulations (see the Inn's Data Protection Policy).

All of the Inn's permanent cameras are **overt** cameras, with the images recorded centrally, and are only viewable by appropriately trained Security staff and those whose roles include data protection responsibility. The cameras cover roadways, car parks, buildings (internally and externally), court yards, and vulnerable public-facing offices. Monitors are installed in the Security Office that allow Security Officers to view the images that are being recorded by each CCTV camera. In exceptional circumstances, there may also be a requirement for temporary **covert** cameras and these are referred to in the section on 'Covert filming or monitoring', below.

The primary Security Control room is situated on the ground floor of the Security Office, 4A Essex Court, Middle Temple, London EC4Y 9AJ. The Security Office is staffed 24 hours a day, 365 days per year by trained, uniformed Security Officers.

Installed at the Security Office are Home Office licensed radio systems, which link the Security Control room with Security Officers who provide foot patrols around the Inn and who are able to respond to incidents that have been identified on the CCTV monitors.

Unlawful access to the data and images from the CCTV cameras is restricted by the following measures: -

- Separate IT network from the Inn's other systems;
- Swipe card access restrictions to the Security Office;
- Security Office manned on a 24/7 basis

# Objectives

## Objectives of the system

To assist in providing a safe and secure environment for the benefit of those who might visit, work, or live within Middle Temple. Subject to the MT CCTV Policy, the CCTV system **will not** be used to invade the privacy of any individual residence, business, or other private premises, buildings, or land. The CCTV cameras are placed so as to be able to view public areas and other internal areas within Middle Temple buildings.

Within the MT CCTV Policy, the CCTV system will only be used for the following purposes:

- To reduce the fear of crime and to provide reassurance to the Inn's tenants, residents, staff, and visitors that their security is important.
- To deter and detect crime, public disorder, and anti-social behaviour.
- To identify, apprehend, and prosecute offenders in relation to crime, public disorder, and anti-social behaviour.
- To provide the Inn with evidence that will support any criminal and/or civil action taken by the appropriate authorities.
- To assist with staff discipline, although the Inn will only use CCTV images in a staff disciplinary case when there is a suspicion of misconduct that is being actively investigated by the HR Department. The CCTV system will not be used to generally monitor staff activity.
- To monitor and assist with parking and traffic management issues.
- To assist in the monitoring and deployment of staff during emergency situations.
- Upon receipt of a formal written request, to assist Police and other law enforcement agencies with the pursuit of their objectives.

## Covert filming or monitoring

Covert monitoring will not normally be considered unless in certain exceptional circumstances, such as suspected criminal activity. Where covert monitoring has been authorised, it will be:

- Targeted to a specific area or individual(s);
- Time limited; and

- Managed in accordance with the published guidance issued by the ICO ('The Employment Practices Code').

A decision to employ covert monitoring will be taken after consultation between the Under Treasurer, the Director of Corporate Services (in their capacity as the Inn's Data Protection Officer, or in their absence by the Information Governance & Records Manager), and the Security Manager. In circumstances where the suspected criminal behaviour is being perpetrated by a member or members of staff, the Head of Human Resources will also be consulted before a decision to use covert monitoring is made.

It is stressed that the use of covert monitoring will only be authorised in exceptional circumstances involving suspected criminal activity in order to support any criminal investigation by the Police or Security Services.

## Data Protection

Middle Temple is committed to complying with the requirements of the General Data Protection Regulation (GDPR) and the Data Protection Act 2018 (DPA2018) and intends to operate the CCTV system in accordance with the data protection principles set out in the GDPR.

The standards, which must be met if the requirements of the GDPR are to be satisfied, are based on the data protection principles set out in Article 5 of the GDPR, which are:

1. Personal data shall be processed lawfully, fairly and in a transparent manner;

2. Personal data shall be collected for specified, explicit and legitimate purposes only, and will not be processed it in a way that is incompatible with those legitimate purposes;

3. Only personal data that is adequate, relevant and necessary for the relevant purposes shall be processed;

4. Personal data must be accurate and must be kept up to date; reasonable steps must be taken to ensure that inaccurate personal data are deleted or corrected without delay;

5. Personal data can be kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the data are processed; and

6. Appropriate technical and organisational measures must be taken to ensure that personal data are kept secure and protected against unauthorised or unlawful processing, and against accidental loss, destruction or damage.

The Inn, as the Data Controller in most cases where personal data is processed, is also responsible to demonstrate compliance with the data protection principles. A Data Protection Impact Assessment ('DPIA') will be completed to identify and manage any privacy risks resulting from the use of CCTV cameras. Prior to introducing any new cameras, the Security Manager will conduct a new DPIA, with the support of the Director of Corporate Services or the Information Governance & Records Manager. The results of the DPIA will determine whether or not any new cameras can be installed.

All members of staff involved in operating the CCTV system will be made aware of the objectives identified in the MT CCTV Policy and will only be permitted to use the CCTV system to achieve those objectives.

The Inn has appointed a Data Protection Officer. Their contact details are:

Data Protection Officer,
The Honourable Society of the Middle Temple,
Treasury Offices,
Ashley Building,
Middle Temple Lane,
London.
EC4Y 9BT

Email: Data.protection@middletemple.org.uk

## CCTV Guiding Principles

The Inn has adopted the 12 guiding principles of the SCC Code, namely:

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.

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 that compares against a reference database for matching purposes should be accurate and kept up-to-date.

Middle Temple recognises the importance of strict guidelines in relation to access to and disclosure of recorded images and all members of staff should be aware of the restrictions relating to this, as set out in the MT CCTV Policy, and the rights of individuals under GDPR/DPA2018 and the SCC Code.

# Administration

## CCTV

It is the responsibility of the Security Manager to:

- Select camera sites and initial areas to be viewed.
- Be responsible for carrying out the initial DPIA and being aware of the associated data protection requirements.
- Be responsible for the annual review of CCTV systems and associated DPIAs in order to ensure compliance with applicable legislation.
- Take responsibility for management and control of the images and support decisions on how these can be used.
- Ensure the CCTV system is secure and can only be viewed by authorised personnel.
- Ensure that the procedures of the MT CCTV Policy comply with GDPR/DPA 2018 and the SCC Code.
- Introduce a CCTV incident log and record of Police or other Statutory Authority requests for images.
- Ensure adequate signage is erected.
- Clearly communicate the specific purposes of the recording of and use of images and the objectives of the MT CCTV Policy to all Security staff.
- Carry out annual audits to check that procedures are being complied with.

It is the responsibility of the individual Security Officers to:

- Ensure that targeting of individuals with the CCTV cameras is only conducted when there is a reasonable suspicion that the person falls within one of the objectives set out in the MT CCTV Policy, e.g. committing a criminal offence or engaging in anti-social behaviour.
- Not to interfere with the siting or positioning of CCTV cameras within the Middle Temple site.

It is the responsibility of the Data Protection Officer to: -

- Liaise with the Security Manager in conducting DPIAs; advising as appropriate.
- Decide how CCTV images may be used or shared with third-parties.
- Support the Security Manager in matters concerning data protection.

## Storing and Viewing Images

All images recorded on the CCTV system are digitally stored on computer/server hard drives and, although the images are searchable, it is not possible to tamper with or alter them in any way. The supplier of the CCTV equipment, who also provides support through a maintenance contract, has access to the images and this is managed through a data protection contract addendum agreed between them and the Inn.

In the event that the Police require CCTV images to support an ongoing investigation, such images can be 'burnt' onto an encrypted CD/DVD/USB Device/External hard drive for evidence in court. This would require the prior completion of the necessary paperwork to allow the transfer of images.

CCTV images are retained for a period of 30 days after which they are over-written with new images on a continual basis.

Viewing of live images on monitors is restricted to Security Officers and to other personnel, who are authorised to do so by the Under Treasurer, the Security Manager, and the Data Protection Officer.

Individuals who are authorised to view images may do so in the privacy of the Security Office under appropriate supervision.

Requests to view images or to disclose images to third parties should be made in writing to the Security Manager. The Police and the Security Services have their own procedures that will be followed and any documentation provided by them will be retained by the Security Manager. Any internal requests for image disclosure will be logged by the Security Manager following receipt of duly authorised documentation.

## Disclosure of images to third parties

The following guidelines will be adhered to in relation to the disclosure of images to third parties.

- Disclosure will be in line with the objectives of the MT CCTV Policy.
- Disclosure will be controlled under the supervision of the Security Manager and the Data Protection Officer.

- A log book of image requests will be maintained by the Security Manager that will itemise the date, time(s), CCTV camera, the person copying the image(s), the person(s) receiving the image(s), and the reason for the disclosure of the image(s). The log book will be kept in the Security Office, which has access controls in place to prevent unauthorised entry.

- The appropriate disclosure documentation from the Police or Security Services will be attached to each log entry, as appropriate.

- Images **must not** be forwarded to the media or be placed on the internet or otherwise distributed without specific and prior written approval of the Under Treasurer and the Data Protection Officer acting in compliance with the law and the MT CCTV Policy. Failure to comply with this requirement will result in disciplinary action being taken against the individual concerned. Images will only be released to the media for legitimate purposes (e.g. such as the identification of data subjects in connection with a criminal investigation) and in liaison with the Police or Security Services.

- Any other image requests should be sent to the Security Manager, who will liaise with the Data Protection Officer to ensure compliance with data protection legislation. In certain, limited, circumstances, it may be appropriate to release images to a third party. In those circumstances, an assessment will be made of that third-party's requirements and the privacy and rights of the data subject(s) depicted in such images.

- The Inn has discretion to refuse any third party request for images unless there is an over-riding legal obligation to do so, such as a court order or a Subject Access Request. Once an image, or series of images, has been disclosed to a third party, such as the Police or the Security Services, then they become the data controller for their copy of that image or series of images. It is the responsibility of the third party to comply with the GDPR/DPA2018 in relation to any further disclosures that may be required.

## Signage

Appropriate signage has been erected at all entrances to Middle Temple and at other locations where CCTV cameras are in use. The signage includes a warning that CCTV cameras are in use.

It is the responsibility of the Security Manager to ensure that adequate signage is erected to comply with the guidance issued by the Information Commissioner's Office.

## Disclosure of images to the data subject (Subject Access Requests)

Individuals whose images are recorded have a right to view those images of themselves, or their vehicles, and, unless they agree otherwise, to be provided with a copy of those images. All such requests are handled by the Inn's Data Protection Officer, in liaison with the Security Manager, and in compliance with the Inn's published data protection policy.

- In accordance with data protection legislation, all such requests for images must be provided within one month of the request being received.

- Individuals who request images must provide proof of identity and sufficient details that allow Middle Temple to identify them as the subject of the images and to assist with locating the relevant image(s) on the CCTV system.

- All requests for images will be logged for record keeping purposes.

- If images of third parties are also shown within the requested image(s) of the data subject who has made the access request, consideration must be given as to whether or not there is a need to obscure the images of those third parties, taking into account the rights of data subjects detailed in data protection legislation.

## Access to / Disclosure of CCTV Images

Middle Temple respects the right of individuals to confirm the accuracy of any personal data that is being processed by the Inn, as detailed in data protection legislation.

An exceptions to this is where disclosure would simultaneously disclose data about another individual, unless that person has provided their own consent to the disclosure.

Any Data Subject wishing to gain access to personal data held about them by the Inn may do so by the submission of a request, in writing, to the Data Protection Officer on each occasion that access is requested. Middle Temple aims to comply with requests for access to personal data as quickly as possible, but will ensure that it is provided within one month of the request being received. Where Middle Temple receives large numbers of requests, or especially complex requests, the time limit may be extended by a maximum of two further months.

Requests should be made to:

**Data.protection@middletemple.org.uk** or by writing to:

Data Protection Officer
The Honourable Society of the Middle Temple
Treasury Office
Ashley Building
Middle Temple Lane
London
EC4Y 9BT

## Freedom of Information

Part II of Schedule 1 of The Freedom of Information Act 2000 ('the FOIA'), or the equivalent legislation applicable in Scotland, provides that only information produced by the Under Treasurer of the Middle Temple in his capacity as a Local Authority is covered by the FOIA. It does not extend to information generated by the Inn as a private body. The Under Treasurer of the Inn exercises a small number of local authority functions, with the remainder being delegated to the responsibility of the City of London. Information about which functions are still provided by the Inn and which are delegated to the City of London can be found on the Inn's website here:
**https://www.middletemple.org.uk/about-us/freedom-of-information**

Freedom of Information requests are dealt with by the Information Governance & Records Manager. Requests should be made by writing to:

Information Governance & Records Manager
The Honourable Society of the Middle Temple
The Treasury Office
Ashley Building
Middle Temple Lane
London EC4Y 9BT
Or email: **FOI@middletemple.org.uk**

Section 40 of the FOIA contains a two-part exemption relating to information about individuals. If we receive a request for CCTV images then the Inn will consider the following: -

- Are the images those of the individual making the request? If so, then that information is exempt from the FOIA. The request will be treated as a data protection Subject Access Request, as explained above.

- Are the images of other people? These can be disclosed only if disclosing the information in question does not breach data protection principles.

- Does the request relate to the Inn's local authority functions? If it relates to the Inn's private functions, then the Inn may not release the requested information.

## Use of the CCTV Systems

All Security staff and other authorised personnel (see above) must receive a copy of the MT CCTV Policy and confirm that they have read it and understand its requirements prior to being instructed on the operation of the CCTV system.

All personnel authorised to use the CCTV systems are required to have read and agreed to comply with Middle Temple's data protection policy.

The CCTV system can be used to observe the Inn and areas under surveillance and identify incidents that require a response. The appropriate response will be determined by Security staff.

CCTV surveillance will be carried out in accordance with the stated objectives of the MT CCTV Policy.

CCTV monitors are viewed only by authorised personnel.

Copying images from the CCTV system with the use of a mobile device is strictly prohibited unless it is carried out by the Police or the Security Services who have provided the necessary documentation to carry out such copying. Any member of staff who copies images from the CCTV system will be subject to disciplinary action.

**Any deliberate failure by Middle Temple staff to comply with the provisions of the MT CCTV Policy may result in disciplinary action being taken.**

A copy of the MT CCTV Policy will be made available to anyone on written request and also posted on the Inn's website.

Any complaints in relation to the use of the CCTV system should be sent to the Security Manager, who will investigate the allegation or complaint. Any complaints in relation to the disclosure of images should be made in writing to the Data Protection Officer.

## Document control

| | |
|---|---|
| Author | Martin Dolby, Security Manager |
| Owner | Martin Dolby, Security Manager |
| Approval Body | Executive Management Team |
| Date Approved | January 2020 |
| Document Number | 1.03F |

## Revision History

| Version | Date | Author(s) | Changes |
|---|---|---|---|
| 1.02D | 31 July 2019 | Martin Dolby, Security Manager | Code of Practice rewritten, including GDPR requirements |
| 1.03D | 21 August 2019 | Andrew Hopkin, Director of Corporate Services<br>Sarah Cates, Information Governance & Records Manager | Review of draft |
| 1.03F | 08 January 2020 | Martin Dolby, Security Manager<br>Andrew Hopkin, Director of Corporate Services<br>Sarah Cates, Information Governance & Records Manager | Discussion and review of previous document |