TWICKENHAM DISTRICT MASONIC COUNCIL LTD
Cole Court, 150 London Road, Twickenham, Middlesex TW1 1HD
Tel: 020-8892-1131 Fax: 020-8892-4266

CCTV POLICY

Policy last reviewed	July 2020
Approved by.	Board of Directors (BoD) Data Protection and Information Compliance Officer. (DPICO)
If you have any questions about this policy, please contact:	Data Protection and Information Compliance Officer. (DPICO)

This procedure is available in accessible format on request from the Centre/Duty Manager and the Data Protection Officer.

Table of Contents

1. Policy Statement

1.1. This Policy, agreed by the Board of Directors (BoD) seeks to ensure that the Close Circuit Television (CCTV) system operated by Twickenham District Masonic Centre Ltd (TDMC), 150 London Road, Twickenham, TW1 1HD is used in compliance with the law relating to data protection (currently the General Data Protection Regulation 2016/679 ("GDPR") and the Data Protection Act 2018 ("DPA 2018")) and includes the principles governing the processing of personal data as set out in this document.

It also seeks to ensure compliance with privacy law. It takes into account best practice as set out in codes of practice issued by the Information Commissioner and by the Home Office.

TDMC therefore uses CCTV only where it is necessary in pursuit of a legitimate aim, as set out in clause 1.2, and only if it is proportionate to that aim.

1.2. TDMC seeks to ensure, as far as is reasonably practicable, the security and safety of all members, staff, visitors and contractors to its property and premises.

TDMC therefore deploys CCTV to:

- promote a safe TDMC environment and to monitor the safety and security of its premises;
- assist in the prevention, investigation and detection of crime;
- assist in the apprehension and prosecution of offenders, including use of images as evidence in criminal proceedings;
  and
- assist in the investigation of breaches of its codes of conduct and policies by members, staff, outside hirers and contractors and where relevant and appropriate, investigating complaints.

1.3 This policy will be reviewed annually by the BoD to assess compliance with clauses 1.1 and 1.2 and to determine whether the use of the CCTV system remains justified.

2. Scope

2.1 This policy applies to all CCTV systems operated by TDMC.

2.2 This policy does not apply to any Webcam systems or audio-visual equipment temporarily set up in any of the rooms at TDMC.

2.3 This policy applies to all TDMC staff, contractors and agents who operate, or supervise the operation of, the CCTV system including the BoD.

3. Roles and Responsibilities

3.1 DPICO has the overall responsibility for this policy but has delegated day-to-day responsibility for overseeing its implementation to the staff identified in this policy. All relevant members of staff have been made aware of the policy and have received appropriate training.

3.2 DPICO is responsible for ensuring that the CCTV system including camera specifications for new installations complies with the law and best practice referred to in clause 1.1 of this policy. Where new surveillance systems are proposed, the BoD will consult with the DPICO to determine whether a prior privacy impact assessment is required. (Appendix 3).

3.3 Only the maintenance contractor for TDMC's CCTV system, appointed by the BoD is authorised to install and/or maintain it.

3.4 DPICO is responsible for the evaluation of locations where live and historical CCTV images are stored or available for viewing.
The list of such locations and the list of persons authorised to view CCTV images is maintained by DPICO.

3.5 The BoD or the Centre/Duty Manager are able to view but not record live images via secure access apps on their personal mobile phones.

4. System Description

4.1 The CCTV systems installed in and around TDMC cover building entrances, car parks, perimeters, external areas such as courtyards, internal areas such as The Bar area and some corridors and reception areas. They continuously record activities in these areas and some of the cameras may be set to motion detection.

4.2 CCTV Cameras are not installed in areas in which individuals would have an expectation of privacy such as toilets, changing facilities etc.

4.3 CCTV cameras are installed in such a way that they are not hidden from view. Signs are prominently displayed where relevant, so that members, staff, visitors and members of the public are made aware that they are entering an area covered by CCTV. The signs also contain contact details as well as a statement of purposes for which CCTV is used.

4.4 The contact details indicated on the CCTV signs around TDMC should be available to members of the public during normal business hours. The Centre/Duty Manager must be familiar with this document and the procedures to be followed in the event that an access request is received from a Data Subject or a third party.

5. Covert Recording

5.1 Covert recoding (i.e. recording which takes place without the individual's knowledge):

5.1.1 may only be undertaken in exceptional circumstances, for example to prevent or detect an unlawful act or other serious misconduct, and if is proportionate i.e. there is no other reasonable, less intrusive means of achieving those purposes;

5.1.2 may not be undertaken without the prior written authorisation of the Chairman of the BoD or in his absence the Company Secretary.
All decisions to engage in covert recording will be documented, including the reasons;

5.1.3 will focus only on the suspected unlawful activity or suspected serious misconduct and information obtained which is not relevant will be disregarded and where reasonably possible, deleted;
and

5.1.4 will only be carried out for a limited and reasonable period consistent with the particular purpose of the recording and will not continue after the investigation is completed.

6. Operating Standards

6.1 The operation of the CCTV system will be conducted in accordance with this policy.

6.2 Monitoring area.

6.2.1 No unauthorised access to the Monitoring area will be permitted at any time.

6.2.2 Other than BoD or the Centre/Duty Manager, access to the Monitoring area will be limited to:

- persons specifically authorised by the BoD or the Centre/Duty Manager;
- maintenance engineers;
- Police Officers where appropriate;
  and
- any other person with statutory powers of entry.
- This temporary access will be granted and limited to address an immediate problem.

6.2.3 Monitors are not visible from outside the monitoring area.

6.2.4 Before permitting access to the monitoring area, staff will satisfy themselves of the identity of any visitor and existence of the appropriate authorisation. All visitors are required to complete and sign the visitors' log, which includes details of their name, department and/or the organisation that they represent, the person who granted authorisation and the times of entry to and exit from the monitoring area. A log shall be retained setting out the following:

- person reviewing recorded footage;
- time, date and location of footage being reviewed; and
- purpose of reviewing the recordings.

6.3 Processing of Recorded Images

6.3.1 CCTV images will be displayed only to persons authorised to view them or to persons who otherwise have a right of access to them. Where authorised persons access or monitor CCTV images on workstation desktops or mobile apps, they must ensure that images are not visible to unauthorised persons for example by minimising screens when not in use or when unauthorised persons are present. Workstation/mobile screens must always be locked when unattended.

6.4 Quality of Recorded Images

6.4.1 Images produced by the recording equipment must be as clear as possible and therefore effective for the purpose for which they are intended. The standards to be met in line with the codes of practice referred to in clause 1 of these procedures are set out below:

- recording features such as the location of the camera and/or date and time reference must be accurate and maintained;
- cameras must only be situated so that they will capture images relevant to the purpose for which the system has been established;
- consideration must be given to the physical conditions in which the cameras are located i.e. additional lighting or infrared equipment may need to be installed in poorly lit areas;
- cameras must be properly maintained and serviced to ensure that clear images are recorded, and a log of all maintenance activities kept; and
- as far as practical, cameras must be protected from vandalism in order to ensure that they remain in working order. Methods used may vary from positioning at height to enclosure of the camera unit within a vandal resistant casing.

6.5 Retention and Disposal

6.5.1 CCTV images are not to be retained for longer than necessary, taking into account the purposes for which they are being processed. Data storage is automatically managed by the

CCTV digital records which overwrite historical data in chronological order to produce an approximate 28-day rotation in data retention.

6.5.2 Provided that there is no legitimate reason for retaining the CCTV images (such as for use in disciplinary and/or legal proceedings), the images will be erased following the expiration of the retention period.

6.5.3 All retained CCTV images will be stored securely.

7. Data Subjects Rights

7.1 Recorded images, if sufficiently clear, are considered to be the personal data of the individuals (Data Subjects) whose images have been recorded by the CCTV system.

7.2 Data Subjects have a right of access to the personal data under the GDPR and DPA 2018. They also have other rights under the GDPR and DPA 2018 in certain limited circumstances, including the right to have their personal data erased, rectified, to restrict processing and to object to the processing of their personal data.

7.3 Data Subjects can exercise their rights by submitting a request to the DPICO in writing along with evidence of their identity as detailed on:
https://ico.org.uk/your-data-matters/your-right-to-get-copies-of-your-data/preparing-and-submitting-your-subject-access-request/

7.4 On receipt of the request, the DPICO will liaise with the BoD and subject to clause 7.5, the DPICO will communicate the decision without undue delay and at the latest within one month of receiving the request from the Data Subject.

7.5 The period for responding to the request may be extended by two further months where necessary, taking into account the complexity and number of the requests. The DPICO will notify the Data Subject of any such extension within one month of receipt of the request together with reasons.

8. Third Party Access

8.1 Third party requests for access will usually only be considered in line with the GDPR and DPA 2018 in the following categories:

- legal representative of the Data Subject;
- law enforcement agencies including the Police;
- disclosure required by law or made in connection with legal proceedings;

and

- HR staff responsible for employees.

8.2 Legal representatives of the Data Subjects are required to submit to TDMC a letter of authority to act on behalf of the Data Subject and the request form (7.3) together with the evidence of the Data Subject's identity.

8.3 The DPICO will disclose recorded images to law enforcement agencies including the Police once in possession of a form certifying that the images are required for either:

- an investigation concerning national security;
- the prevention or detection of crime; or the apprehension or prosecution of offenders, and that the investigation would be prejudiced by failure to disclose the information.
- Where images are sought by other bodies/agencies with a statutory right to obtain information, evidence of that statutory authority will be sought before CCTV images are disclosed.

8.4 Every disclosure of the CCTV images is recorded in the CCTV Operating Log Book and contains:

• the name and number of the Police Officer or other relevant person in the case of other agencies/bodies receiving the copy of the recording;
• brief details of the images captured by the CCTV to be used in evidence or for other purposes permitted by this policy;
• the crime reference number where relevant;
and
• date and time the images were handed over to the Police or other body/agency.

8.5 Requests for CCTV images for staff disciplinary purposes (or complaints purposes) must be authorised by the BoD in consultation with the DPICO.

8.6 Requests for CCTV information under the Freedom of Information Act 2000 will be considered in accordance with that regime.

9. Complaint Procedure

9.1 Any complaints relating to the CCTV system should be directed in writing to the DPICO promptly and in any event within 7 days of the date of the incident giving rise to the complaint. A complaint will be responded to within a month following the date of its receipt. Records of all complaints and any follow-up action will be maintained by the relevant office.

If a complainant is not satisfied with the response they may appeal to the Chairman of the BoD or in their absence the Company Secretary

9.2 Complaints in relation to the release of images should be addressed to the Chairman of the BoD or in their absence the Company Secretary as soon as possible and in any event no later than three months from the event giving rise to the complaint.

9.3 If a complainant finds they are still not satisfied with the response, they should use the existing grievance procedure as laid down in the Employee Handbook.

10. Useful Links

The Information Commissioner's Code of Practice can be found at:
https://ico.org.uk/media/for-organisations/documents/1542/cctv-code-of-practice.pdf
The Home Office Code can be found at:
https://www.gov.uk/government/publications/surveillance-camera-code-of-practice.

Appendix 1 – Data Subject Access Request (DSAR)

Under data protection legislation (General Data Protection Regulation (GDPR) and Data Protection Act 2018 (DPA 2018)) TDMC must process personal data lawfully, fairly, transparently and for specified purposes (and not further processed in a way that's incompatible with those purposes).

Exemptions apply which allow TDMC to process (including disclosing) personal data in certain circumstances. However, there must always be a legal basis for the processing. TDMC will support you in making your request for disclosure of personal data. Please supply as much relevant information as possible. We will use it to help us:

- identify the data subject(s) and personal data relevant to your request,
- determine as a data controller whether or not we are able to process/disclose the personal data
  and
- document the request and provide an auditable trail.

□

Unless TDMC is satisfied that we are authorised to process the personal data by a legal basis in keeping with the data protection principles and data subject rights, or exemptions provided by the DPA 2018, we will be unable to disclose the personal data to you.

Under the GDPR, individuals have the right to obtain confirmation that their personal information is being processed.

11.2. All disks containing images belong to, and remain the property of, TDMC.

11.3. Individuals have the right to submit a Data Subject Access Request (DSAR) to gain access to their personal data in order to verify the lawfulness of the processing.

11.4. TDMC will verify the identity of the person making the request before any information is supplied.

11.5. A copy of the information will be supplied to the individual free of charge; however, TDMC may impose a 'reasonable fee' to comply with requests for further copies of the same information .

11.6. Where a DSAR has been made electronically, the information will be provided in a commonly used electronic format.

11.7. Requests by persons outside TDMC for viewing or copying disks, or obtaining digital recordings, will be assessed by the BoD, who will consult the DPO, on a case-by-case basis with close regard to data protection and freedom of information legislation.

11.8. Where a request is manifestly unfounded, excessive or repetitive, a reasonable fee will be charged.

11.9. All fees will be based on the administrative cost of providing the information.

11.10. All requests will be responded to without delay and at the latest, within one month of receipt.

11.11. In the event of numerous or complex requests, the period of compliance will be extended by a further two months. The individual will be informed of this extension, and will receive an explanation of why the extension is necessary, within one month of the receipt of the request.

11.12. Where a request is manifestly unfounded or excessive, TDMC holds the right to refuse to respond to the request. The individual will be informed of this decision and the reasoning behind it, as well as their right to complain to the ICO and to a judicial remedy, within one month of the refusal.

11.13. In the event that a large quantity of information is being processed about an individual, TDMC will ask the individual to specify the information the request is in relation to.

11.14. It is important that access to, and disclosure of, the images recorded by surveillance and CCTV footage is restricted and carefully controlled, not only to ensure that the rights of individuals are preserved, but also to ensure that the chain of evidence remains intact, should the images be required for evidential purposes.

11.15. Releasing the recorded images to third parties will be permitted only in the following limited and prescribed circumstances, and to the extent required or permitted by law:

- The police – where the images recorded would assist in a specific criminal inquiry.
- Prosecution agencies – such as the Crown Prosecution Service (CPS).
- Relevant legal representatives – such as lawyers and barristers
- Persons who have been recorded and whose images have been retained where disclosure is required by virtue of data protection legislation and the Freedom of Information Act 2000.

11.16. Requests for access or disclosure will be recorded and the BoD will make the final decision as to whether recorded images may be released to persons other than the police.

Appendix 2 – Definitions

Definitions of words/phrases used in relation to the protection of personal data and referred to in the text of the policy

CCTV – Closed-circuit television is the use of video cameras to transmit a signal to a specific place on a limited set of monitors. The images may then be recorded on video tape or DVD or other digital recording mechanism.

The Data Protection Acts – The Data Protection Acts 1988 and 2003 confer rights on individuals as well as responsibilities on those persons handling, processing, managing and controlling personal data. All school/ETB staff must comply with the provisions of the Data Protection Acts when collecting and storing personal information. This applies to personal information relating both to employees of the organisation and individuals who interact with the organisation.

Data - information in a form that can be processed. It includes automated or electronic data (any information on computer or information recorded with the intention of putting it on computer) and manual data (information that is recorded as part of a relevant filing system or with the intention that it should form part of a relevant filing system).

Personal Data – Data relating to a living individual who is or can be identified either from the data or from the data in conjunction with other information that is in, or is likely to come into, the possession of the data controller.

Access Request – this is where a person makes a request to the organisation for the disclosure of their personal data under Section 3 and/or section 4 of the Data Protection Acts.

Data Processing - performing any operation or set of operations on data, including: - Obtaining, recording or keeping the data, - Collecting, organising, storing, altering or adapting the data, - Retrieving, consulting or using the data, - Disclosing the data by transmitting, disseminating or otherwise making it available, - Aligning, combining, blocking, erasing or destroying the data.

Data Subject – an individual who is the subject of personal data.

Data Controller - a person who (either alone or with others) controls the contents and use of personal data.

Data Processor - a person who processes personal information on behalf of a data controller, but does not include an employee of a data controller who processes such data in the course of their employment, for example, this might mean an employee of an organisation to which the data controller out-sources work. The Data Protection Acts place responsibilities on such entities in relation to their processing of the data.

Appendix 3 – Privacy Impact Assessment

Before TDMC installs a new CCTV system, it is recommended that a documented privacy impact assessment is carried out. Carrying out such an assessment is less likely to introduce a system that contravenes the provisions of the Data Protection Acts 1988 & 2003. This is an important procedure to adopt as a contravention may result in action being taking against TDMC by the Office of the Data Protection Commissioner, or may expose TDMC to a claim for damages.

Some of the points that might be included in a Privacy Impact Assessment are:

- What is TDMC's purpose for using CCTV images? What are the issues/problems it is meant to address?
- Is the system necessary to address a pressing need, such as staff and Member safety or crime prevention?
- Is it justified under the circumstances?
- Is it proportionate to the problem it is designed to deal with?
- What are the benefits to be gained from its use?
- Can CCTV systems realistically deliver these benefits? Can less privacy-intrusive solutions, such as improved lighting, achieve the same objectives?
- Does TDMC need images of identifiable individuals, or could the system use other images which are not capable of identifying the individual?
- Will the system being considered deliver the desired benefits now and remain suitable in the future?
- What future demands may arise for wider use of images and how will they be addressed?
- Is TDMC the data controller for the entire CCTV system or will an external management company be employed. In which case specific legal advice may need to be sought)?
- Where a management company is employed, is TDMC satisfied that it complies with the Data Protection Acts with regard to the processing of images of staff, members and visitors to TDMC captured on any CCTV systems under its management?
- What are the views of those who will be under CCTV surveillance?
- What could be done to minimise intrusion for those whose images may be captured, particularly if specific concerns have been expressed?
- How have staff, members and visitors been assured by TDMC that they will not be monitored and that the CCTV system will be used only for the stated purposes?
- Can the location of each internal camera be justified in accordance with the overall purpose for the use of the CCTV system?
- Has appropriate signage been erected at the location of each internal camera indicating that recording is taking place and outlining the purpose of such recording?
- Who will have access to the system and recordings/images?
- What security measures are in place to protect the CCTV system and recordings/images?
- Are those who will have authorised access to the system and recordings/images clear about their responsibilities?
- Are the camera monitors kept out of view of staff, members and visitors and is access to the camera monitors restricted to a limited number on a 'need to know' basis?
- Is the room(s) which houses the camera monitors and the CCTV system securely locked when unattended?
- Does TDMC have a procedure in place to ensure that recordings/images are erased or deleted as soon as the retention period (28 days) has expired?
- Does TDMC have a procedure in place for handling requests for access to recordings/images.
- Does TDMC have a data protection policy? Has it been updated to take account of the introduction of a CCTV system?
- Does TDMC have a procedure in place to handle access requests seeking a copy of images recorded by the CCTV system?
- Has the right of access been communicated to staff, members and visitors?
- Has TDMC communicated its policy on the use of CCTV to staff, members and visitors and how has this been done?
- How are new members and new staff informed of TDMC's policy on the use of CCTV?