Spire Church Farnham
CCTV Policy

Managing Trustee body: **Spire Church Farnham**
Property: **Farnham Methodist Church & Farnham United Reformed Church, South Street, Farnham**
Date: **24 March 2026**

1. Definitions

This section sets out definitions of key terms referred to in this policy:

"**You**" "**Your**" "**Data Users**" are those of our volunteers, ministers and staff whose work involves processing personal data. This will include those whose duties are to operate CCTV at the Property. Data Users must protect the data they handle in accordance with this policy and our Data Protection Policy.

"**We**" "**our**" are the Managing Trustees of the Property.

CCTV : means fixed and domed cameras designed to capture and record images of individuals and property and other surveillance systems to record, monitor, store, retrieve and delete images.
"**controller/s**": the person or organisation that determines when, why and how to process, personal data. It is responsible for establishing practices and policies in line with the GDPR and UK data protection legislation.

Trustees for Methodist Church Purposes are **controllers** for **personal data** used by staff and volunteers at Local Church, Circuit and District level. This is for routine, day to day data protection matters including the operation of CCTV cameras. The Methodist Church in Great Britain is the **controller** responsible for all data protection matters concerning safeguarding and, complaints and discipline issues for the whole Methodist Church and other data protection matters for which the Connexional Team are solely responsible. This would include where images from CCTV cameras are associated with any safeguarding and/or complaints and discipline concerns.

The "**appropriate controller**" is the **controller** for the matter in hand.

DPP: the Data Protection Policy for the Methodist Church (GDPR) available on the TMCP Website.

DSAR Policy: the Managing Trustees' Data Subject Access Request Policy available on the TMCP Website.

"data" is information which is stored electronically, or in certain paper-based filing systems. In respect of CCTV, this generally means video images. It may also include static pictures such as printed screen shots.

"data subject": a living, identified or identifiable individual about whom we hold **personal data** as a result of the operation of the Managing Trustees' CCTV.

ICO: Information Commissioner's Office.

ICO Code: the updated ICO Surveillance Camera Code of Practice that came into effect on 12 January 2022, the key principles of the ICO Code in the Annex to this policy.

GDPR: the General Data Protection Regulation ((EU) 2016/679). **Personal data** is subject to the safeguards specified in the GDPR.

Local Contact is the individual at the Local Church, Circuit or District who is responsible for day-to-day administration of data protection matters. The Local Contact for the purposes of this policy is Ian Sargeant who can be contacted by email at treasurer@spirechurchfarnham.org.uk OR post at Farnham URC, South Street Farnham GU9 7QU.

Managing Trustees means the people who, from time to time, have responsibility for the day-to-day control and management of the property, where the CCTV, the subject of this policy, is located, and who are ascertained in accordance with the provisions of Part II of Schedule 2 to the Methodist Church Act 1976.

Methodist Church in Great Britain, Methodist Church or Church refers to the united church or denomination known as the Methodist Church formed under the provisions of the Methodist Church Union Act 1929 and a deed of union on 20 September 1932.

"personal data": any information identifying a living individual or information relating to an individual that can be identified from that information/data (alone or in combination with other information in your hands or that can reasonably be accessed). This will include video images of identifiable individuals.

"processing" or "processed" or "process": any activity that involves the use of **personal data**. It includes obtaining, recording or holding the data, or carrying out any activity or set of activities on the data including organising, amending, retrieving, using, disclosing, erasing or destroying it. **Processing** also includes transmitting or transferring **personal data** to third parties. E.g. sharing member information by email and shredding when information is no longer required.

Property: the premises at which the CCTV is installed being Farnham Methodist Church, South Street Farnham GU9 7RN and Farnham United Reformed Church at South Street Farnham GU9 7QU.

Processors: are any person or organisation that is not a **data user** (or other employee) that processes data on our behalf and in accordance with our instructions (for example, a supplier which handles data on our behalf).

Retention Policy: the retention policies, schedules and processes for retaining information put in place by the **controller** from time to time.

Security Policy: the Security Policy for the Methodist Church available on the TMCP Website.

Surveillance systems: means any devices or systems designed to monitor or record images of individuals or information relating to individuals. The term includes CCTV systems as well as any technology that may be introduced in the future such as automatic number plate recognition (ANPR), body worn cameras, unmanned aerial systems and any other systems that capture information of identifiable individuals or information relating to identifiable individuals.

2. About This Policy - Introduction and Scope

2.1 We have decided to use CCTV cameras to view and record individuals on and around our premises in order to prevent crime and maintain a safe environment for members, ministers, volunteers, staff, lay workers, third parties such as community groups who use our buildings, visitors to our buildings and other third parties. 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, the DPP and the Security Policy.

2.2 The **controller**, has registered our use of CCTV with the ICO and we will seek to comply with its best practice suggestions including the ICO Code (see the key principles of the ICO Code in the Annex to this policy).

2.3 The purpose of this policy is to:

(a) outline why and how we will use CCTV, and how we will process data recorded by CCTV cameras.
(b) ensure that the legal rights of **data subjects**, relating to their personal data, are recognised and respected.

(c) assist **data users** in complying with their own legal obligations when working with personal data. In certain circumstances, misuse of information generated by CCTV or other surveillance systems could constitute a criminal offence.
(d) explain how to make and deal with a subject access request in respect of personal data created by CCTV.
(e) explain how to deal with a request for disclosure.

2.4 The Template CCTV Policy for Methodist Managing Trustees, on which this policy is based, is available from TMCP and has been developed to help Managing Trustees apply a consistent CCTV policy across the Methodist Connexion. This policy should be read in conjunction with the Managing Trustees' Privacy Notice and the DPP.

3. Who Does This Policy Apply To?

This policy applies to all our staff, lay workers, volunteers, ministers and other members who are involved in operating our CCTV cameras and other surveillance systems to record, monitor, store, retrieve and delete images. It also applies to anyone visiting and/or using our premises.

4. Who Is Responsible For This Policy?

4.1 Pursuant to paragraph 3 of the DPP:
(a) the Board of TMCP and the Methodist Church in Great Britain (whose responsibility is delegated by Conference to the Methodist Council with the work being carried out by the Connexional Team) have overall responsibility for the effective operation of this policy; and
(b) the Managing Trustees are responsible for overseeing its implementation at the Property and ensuring **data users** comply with this policy**.**

Questions about the content of this policy or suggestions for change should be reported to the **controller**.

4.2 Any questions you may have about the day-to-day application of this policy should be referred to your Local Contact or Data Champion in the first instance.

4.3 The Template CCTV Policy for Methodist Managing Trustees policy on which this policy is based is reviewed annually by the **controller**. We will review this policy annually in light of any amendments made to the Template and any changes in how we use the CCTV at the Property. The Managing Trustees, will also review the ongoing use of existing CCTV cameras at the Property at least every 12 months to ensure that their use remains necessary and appropriate, and that any surveillance system is continuing to address the needs that justified its introduction.

5. Reasons For The Use Of CCTV

5.1 We currently use CCTV around our church premises as outlined below. We believe that such use is necessary for legitimate purposes of the charity, including:
(a) to prevent crime and protect charity buildings and assets from damage, disruption, vandalism and other crime;
(b) for the personal safety of our members, ministers, volunteers, staff, lay workers, third parties who use our buildings, visitors to our buildings and other members of the public and to act as a deterrent against crime;
(c) to support law enforcement bodies in the prevention, detection and prosecution of crime;
(d) to assist in day-to-day management of the Property, including ensuring the health and safety of members, ministers, volunteers, staff, lay workers, third parties who use our buildings and others;

(e) to assist in the effective resolution of disputes which arise in relation to use of our Property including any car parking areas;
(f) to assist in the defence of any civil litigation, including employment tribunal proceedings and personal injury claims;

This list is not exhaustive and other purposes may be or become relevant.

6. Monitoring

6.1 CCTV monitors inside and outside of the Property perimeter boundaries including:

(a) Main entrance of the Methodist Church;
(b) Main entrance of the Methodist Church Hall;
(c) Main entrance of the United Reformed Church;
(d) Side entrance of the United Reformed Church building

24 hours a day and this data is continuously recorded.

6.2 Camera locations are chosen to minimise viewing of spaces not relevant to the legitimate purpose of the monitoring. As far as practically possible, CCTV cameras will not focus on private homes, gardens or other areas of private property.

6.3 Surveillance systems **will not** be used to record sound.

6.4 Images are monitored by authorised persons as required.

6.5 Data Users will be given appropriate training to ensure they understand and observe the legal requirements related to the processing of relevant data.

7. How We Will Operate Any CCTV

7.1 We will ensure that signs are displayed at the entrance of the surveillance zone to alert individuals that their image may be recorded. Such signs will contain details of the organisation (the Managing Trustee body) operating the system, the purpose for using the surveillance system and who to contact for further information (the Local Contact), where these things are not obvious to those being monitored.

7.2 Live feeds from CCTV cameras will only be monitored where this is reasonably necessary, for example to protect health and safety.

7.3 We will ensure that live feeds from cameras and recorded images are only viewed by approved volunteers or members of staff whose role requires them to have access to such data. Recorded images will only be viewed in designated, secure offices.

8. Use of data gathered by CCTV

8.1 In order to ensure that the rights of individuals recorded by the CCTV system are protected, we will ensure that data gathered from CCTV cameras is stored in a way that maintains its integrity and security. This may include encrypting the data, where it is possible to do so.

8.2 Given the large amount of data generated by surveillance systems, we may store video footage using a cloud computing system. We will take all reasonable steps to ensure that any cloud service provider maintains the security of our information, in accordance with industry standards.

8.3 We may engage data processors to process data on our behalf. We will ensure reasonable contractual safeguards are in place to protect the security and integrity of the data.

9. Retention and erasure of data gathered by CCTV

9.1 Data recorded by the CCTV system will be stored digitally. Data from CCTV cameras will not be retained indefinitely but will be permanently deleted once there is no reason to retain the recorded information. Exactly how long images will be retained for will vary according to the purpose for which they are being recorded. For example, where images are being recorded for crime prevention purposes, data will be kept long enough only for incidents to come to light. In all other cases, recorded images will be kept for no longer than 90 days. We will maintain a comprehensive log of when data is deleted.

9.2 At the end of their useful life, all images stored in whatever format will be erased permanently and securely. Any physical matter such as tapes or discs will be disposed of as confidential waste. Any still photographs and hard copy prints will be disposed of as confidential waste.

10. Use of additional surveillance systems

10.1 Prior to introducing any new surveillance system, including placing a new CCTV camera in any additional location(s), we will carefully consider if they are appropriate by carrying out a data privacy impact assessment (**DPIA**).

10.2 A DPIA is intended to assist us in deciding whether new surveillance cameras are necessary and proportionate in the circumstances and whether they should be used at all or whether any limitations should be placed on their use.

10.3 Any DPIA will consider the nature of the problem that we are seeking to address at that time and whether the surveillance camera is likely to be an effective solution, or whether a better solution exists. In particular, we will consider the effect a surveillance camera will have on individuals and therefore whether its use is a proportionate response to the problem identified.

10.4 No surveillance cameras will be placed in areas where there is an expectation of privacy (for example, in changing rooms) unless, in very exceptional circumstances, it is judged by us to be necessary to deal with very serious concerns.

11. Covert monitoring

11.1 We will never engage in covert monitoring or surveillance (that is, where individuals are unaware that the monitoring or surveillance is taking place) unless, in highly exceptional circumstances, there are reasonable grounds to suspect that criminal activity or extremely serious malpractice is taking place and, after suitable consideration, we reasonably believe there is no less intrusive way to tackle the issue.

11.2 In the unlikely event that covert monitoring is considered to be justified, it will only be carried out with the express authorisation of the **appropriate controller** in consultation with the District Data Champion (via District Office, 01293 813970, wendy.cory@methodistsoutheast.org). The decision to carry out covert monitoring will be fully documented and will set out how the decision to use covert means was reached and by whom. The risk of intrusion on innocent members, ministers, volunteers, staff, lay

workers, third parties such as community groups who use our buildings, visitors to our buildings and other third parties will always be a primary consideration in reaching any such decision.

11.3 Only limited numbers of people will be involved in any covert monitoring.

11.4 Covert monitoring will only be carried out for a limited and reasonable period of time consistent with the objectives of making the recording and will only relate to the specific suspected illegal or unauthorised activity.

12. Requests for disclosure

12.1 We may share data with other associated companies or organisations, for example shared services partners where we consider that this is reasonably necessary for any of the legitimate purposes set out above in paragraph 0. No images from our CCTV cameras will be disclosed to any other third party, without express permission being given by the Local Contact. Data will not normally be released unless satisfactory evidence that it is required for legal proceedings or under a court order has been produced.

12.2 In other appropriate circumstances, we may allow law enforcement agencies to view or remove CCTV footage where this is required in the detection or prosecution of crime.

12.3 We will maintain a record of all disclosures of CCTV footage.

12.4 No images from CCTV will ever be posted online or disclosed to the media.

13. Data subject access requests

13.1 Data subjects may make a request for disclosure of their personal information and this may include CCTV images (**data subject access request**). A data subject access request is subject to the statutory conditions from time to time in place

13.2 In order for us to locate relevant footage, any requests for copies of recorded CCTV images must include the date and time of the recording, the location where the footage was captured and, if necessary, information identifying the individual.

13.3 We reserve the right to obscure images of third parties when disclosing CCTV data as part of a data subject access request, where we consider it necessary to do so.

Data subject access requests

Please refer to the DSAR Policy for guidance on how to identify and deal with data subject access requests.

Managing Trustees should try to ensure that the design of the CCTV allows them to easily locate and extract personal data promptly to enable the **controller** to respond to data subject access requests and should also be designed to allow for the redaction of third party data where necessary.

Data subjects who make access requests must provide information which allows them to be identified as the subject of the information and for that information to be located on the organisation's system. It is suggested that the date, time and location of where the footage was captured, or the vehicle registration mark, if they are requesting information collected by ANPR cameras, is provided. (See the key principles of the ICO Code in the Annex to this policy.)

14. Complaints

14.1 If any members, ministers, volunteers, staff, lay workers, third parties, visitors to our buildings and other third parties has any concerns about our use of CCTV, they should speak to the Local Contact in the first instance.

14.2 Where this is not appropriate, or matters cannot be resolved informally, please contact the **appropriate controller**.

15. Requests to prevent processing

We recognise that, in rare circumstances, individuals may have a legal right to object to processing and in certain circumstances to prevent automated decision making (see Articles 21 and 22 of the UK General Data Protection Regulation). We believe this is unlikely to apply to the data processed through our use of the CCTV but for further information regarding this, please contact the **appropriate controller**.

Signed :  Name: Revd Philip M Simpkins

Date: 24 March 2026

To be reviewed: March 2027

ANNEX 1

UPDATED ICO SURVEILLANCE CAMERA CODE

The ICO's Surveillance Camera Code of Practice (ICO Code) came into effect on 12 January 2022. The ICO Code sets out 12 guiding principles for users of CCTV and surveillance systems to follow. These are summarised below and further detailed guidance on what each of these principles means in set out in the ICO Code itself (Link: Surveillance Camera Code of Practice (publishing.service.gov.uk)**):**

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 user 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.

ANNEX 2

Template Data Protection Impact Assessment (DPIA) for use by Methodist Managing Trustees considering use of CCTV at Methodist premises

This is a Template DPIA that can be used by Methodist Managing Trustees considering using CCTV at Methodist premises. Methodist Managing Trustees should consider the following points when deciding whether CCTV is the best way to improve security at the Property, bearing in mind the impact of the CCTV on people's freedom. These questions are adapted from the ICO's guidance to individuals considering using domestic CCTV to capture images inside their property boundary:

Managing Trustee body:

Trustees of The Spire Church Farnham, being a single congregation Local Ecumenical Project acting as the managing trustees of Farnham Methodist Church and Farnham United Reformed Church

Property:

Farnham Methodist Church, South Street Farnham GU9 7RN and Farnham United Reformed Church South Street Farnham GU9 7QU

Date: November 2024

Does the Managing Trustee body e.g. the Church Council really need CCTV?	Yes
Are there other things the Managing Trustee body could use to protect the Property, such as better locks, security lighting or an alarm system? Has a representative checked the local police advice about crime prevention?	Smart locking is also being installed.
What is the most privacy-friendly way to set up the CCTV system?	Discreetly located cameras only at point of entrances to the two buildings.
What areas does the Managing Trustee body want the cameras to capture? Do cameras need to capture images beyond the boundary of the Property?	Entrance/Exits from the two properties.
Can Managing Trustees position the cameras to avoid intruding on the Church's neighbours' property or any shared or public spaces?	Yes.
Does the CCTV system need to record the images, or is a live feed enough?	Recorded images are necessary to identify which of the hundreds of users of the properties could be causing problems.
Has the CCTV system got an audio-recording facility? If so, can this be disabled on the basis that audio recording is very privacy-intrusive?	Yes, the audio recording can be suppressed.
ADD ANY OTHER PARTICULAR POINTS YOU WILL CONSIDER	Recent incidents that have given rise to concerns for the safety of the properties and possible unauthorised use by third parties.