HIGHAM WITH MERSTON PAROCHIAL CHURCH COUNCIL

CCTV Policy

For the purposes of this policy the meaning of the words is to be those ascribed to them in the glossary below.

Glossary

CCTV means fixed and domed cameras designed to capture and record images of individuals and property.

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 Controller means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the Processing of Personal Data. It is responsible for establishing practices and policies in line with the GDPR. The Incumbent and/or the PCC are the Data Controllers of all Personal Data relating to Data Subjects.

Data Processor means a natural or legal person, public authority, agency or other body which processes Personal Data on behalf of and with authority from the Data Controller.

Data Subject: a living, identified or identifiable individual about whom we hold Personal Data. Data Subjects may be nationals or residents of any country and may have legal rights regarding their Personal Data.

Data Users are those whose work involves processing Personal Data. This will include those whose duties are to operate CCTV cameras and other surveillance systems to record, monitor, store, retrieve and delete images. Data Users must protect the data they handle in accordance with this policy and our GDPR and Data Protection Policy.

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

Personal Data is any information relating to an identified or identifiable natural person (Data Subject) who can be identified, directly or indirectly by reference to an identifier such as a name, identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person. Personal Data includes Sensitive Personal Data and Pseudonymised Personal Data but excludes anonymous data or data that has had the identity of an individual permanently removed. Personal Data can be factual (for example, a name, email address, location or date of birth) or an opinion about that person's actions or behaviour. This will include video images of identifiable individuals.

Processing means anything done with Personal Data, such as collection, recording, structuring, storage, adaptation or alteration, retrieval, use, disclosure, dissemination or otherwise making available, restriction, erasure or destruction.

Pseudonymisation or Pseudonymised: replacing information that directly or indirectly identifies an individual with one or more artificial identifiers or pseudonyms so that the person, to whom the data relates, cannot be identified without the use of additional information which is meant to be kept separately and secure.

Sensitive Personal Data: information revealing racial or ethnic origin, political opinions, religious or similar beliefs, trade union membership, physical or mental health conditions, sexual life, sexual orientation, biometric or genetic data, and Personal Data relating to criminal offences and convictions

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.

1. Policy Statement

1.1 We believe that CCTV and other Surveillance Systems have a legitimate role to play in helping to maintain a safe and secure environment for all. However, we recognise that this may raise concerns about the effect on individuals and their privacy. This policy is intended to address such concerns. Images recorded by Surveillance Systems are Personal Data which must be processed in accordance with data protection laws. We are committed to complying with our legal obligations and ensuring that the legal rights of Data Subjects, relating to their Personal Data, are recognised and respected.

1.2 This policy is intended to assist Data Controllers and Data Processors 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.

2. About this Policy

2.1 We currently use CCTV cameras to view and record activity within the scope of our Surveillance System. This policy outlines why we use CCTV, how we will use CCTV and how we will process data recorded by CCTV cameras to ensure we are compliant with data protection law and best practice

2.2 We recognise that information that we hold about individuals is subject to data protection legislation. The images of individuals recorded by CCTV cameras are Personal Data and therefore subject to the legislation. We are committed to complying with all our legal obligations and seek to comply with best practice suggestions from the Information Commissioner's Office (**ICO**).

2.3 This policy covers all Data Controllers, Data Processors and Data Users and may also be relevant to all Data Subjects.

2.4 The Data Controller takes compliance with this policy very seriously. Failure to comply puts Data Subjects whose Personal Data is being Processed at risk and carries the risk of significant civil and criminal sanctions for the Processor, and the Data Controller and may in some circumstances amount to a criminal offence by the Processor.

If a Processor breaches this policy, then authority to Process Personal Data for and on behalf of the Data Controller may be terminated with immediate effect.

3. Personnel Responsible

3.1 The Data Controller has overall responsibility for ensuring compliance with relevant legislation and the effective operation of this policy

3.2 Responsibility for keeping this policy up to date has been delegated to the Policies Committee.

4. Reasons for the use of CCTV
We currently use CCTV as outlined below. We believe that such use is necessary for legitimate purposes, including:

(a) to protect buildings and assets from damage, disruption, vandalism and prevent crime;

(b) for the personal safety of Data Subjects 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, including ensuring the health and safety of Data Subjects;

(e) to assist in the effective resolution of disputes which arise in the course of disciplinary or grievance proceedings and

(f) to assist in providing evidence in any civil litigation, including employment tribunal proceedings.

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

5. Monitoring
5.1 CCTV monitors:
a) the exterior of the building in areas at the North and South West;
b) the interior of the church
for 24 hours a day and this data is continuously recorded.

5.2 Surveillance systems will not be used to record sound.

5.3 Images are monitored by authorised personnel.

5.4 Data Processors using surveillance systems will be given appropriate training to ensure they understand and observe the legal requirements related to the Processing of relevant data.

6. How we will operate any CCTV
Where CCTV cameras are in place, signs will be displayed to alert individuals that their image may be recorded.

7. Use of Data Gathered by CCTV

7.1 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.

7.2 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.

8. Retention and Erasure of Data gathered by CCTV

8.1 Data recorded by the CCTV system will be stored. Data from CCTV cameras will not be retained indefinitely but will be overwritten automatically when storage reaches capacity.

8.2 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.

9. Use of Additional Surveillance Systems

9.1 Prior to introducing any new CCTV camera in any workplace location, we will carefully consider if they are appropriate by carrying out a privacy impact assessment (**PIA**).

9.2 A PIA 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.

9.3 Any PIA 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.

9.4 No surveillance cameras will be placed in areas where there is an expectation of privacy (for example, in toilets).

10. Ongoing Review of CCTV Use

We will ensure that the ongoing use of existing CCTV cameras in the workplace is reviewed periodically to ensure that their use remains necessary and appropriate, and that any Surveillance System is continuing to address the needs that justified its introduction.

11. Requests for Disclosure

11.1 No Personal Data from our CCTV cameras will be disclosed to any third party. Data will not normally be released unless satisfactory evidence that it is required for legal proceedings or under a court order has been produced.

11.2 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.

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

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

12. Subject Access Requests

12.1 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 and should be made in writing, in accordance with our Data Protection policy.

12.2 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.

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

13. Requests to Prevent Processing

We recognise that, in rare circumstances, individuals may have a legal right to object to processing (see Article 21 of the General Data Protection Regulation). For further information regarding this, please contact the Data Controller.

July 2018