Windlesham Field of Remembrance

CCTV policy

CONTENTS

1. About this policy

1.1 We use CCTV cameras to view and record individuals on and around our premises to maintain a safe environment for staff and visitors using to the Field of Remembrance. 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 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 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 staff, relating to their personal data, are recognised and respected;

(c) assist the committee 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; and

(d) explain how to make a subject access request in respect of personal data created by CCTV.

1.3 This policy has been agreed with the Field of Remembrance Management Committee ("Committee").

1.4 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.

1.5 A breach of this policy by the data controller will lead to an investigation, and the breach reported to the Information Commissioners Office (ICO).

2. Who does this policy apply to?

2.1 This policy applies to anyone visiting the Field of Remembrance.

3. Who is responsible for this policy?

3.1 The Committee has overall responsibility for the effective operation of this policy.

3.2 Any questions you may have about the day-to-day application of this policy should be referred to the Committee in the first instance.

3.3 This policy is reviewed annually by the Committee. We will also review the ongoing use of existing CCTV cameras 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.

4. Definitions

4.1 For the purposes of this policy, the following terms have the following meanings:

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

Controllers: are the people who, or organisations which, determine the way any personal data is processed. They are responsible for establishing practices and policies to ensure compliance with the law. We are the controller of all personal data used in our business for our own commercial purposes.

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 subjects: means all living individuals about whom we hold personal information because of the operation of our CCTV (or other surveillance systems).

Data users: are those of our committee members 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 Data Protection Policy.

Personal data: means data relating to a living individual who can be identified from that data (or other data in our possession). This will include video images of identifiable individuals.

Processing: is any activity which involves the use of data. It includes obtaining, recording, or holding data, or carrying out any operation on the data including organising, amending, retrieving, using, disclosing, or destroying it. Processing also includes transferring personal data to third parties.

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

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.

5. Reasons for the use of CCTV

5.1 We currently use CCTV around our site as outlined below. We believe that such use is necessary for legitimate business purposes, including:

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

(b) for the personal safety of staff, visitors 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, including ensuring the health and safety of all those accessing or using the Field of Remembrance;

(e) to assist in the effective resolution of disputes which may arise;

(f) to assist in the defence of any civil litigation,

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

6. Monitoring

6.1 CCTV monitors the car park, main entrance and secondary exits 24 hours a day and this data is continuously recorded. CCTV cameras located at the rear of the building only operate on evenings and weekends.

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 may be monitored by authorised personnel 24 hours a day, every day of the year.

6.5 Individuals using surveillance systems 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 CCTV

7.1 Where CCTV cameras are placed around the site, we will ensure that signs are displayed at the entrance of the surveillance zone to alert individuals that their image may be recorded. The signs will contain details of the organisation operating the system, the purpose for using the surveillance system and who to contact for further information, 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 members of the Committee whose role requires them to have access to such data.

7.4 In February each year the Management Committee will approve the list of members authorised to view CCTV images. The list of members may be amended during the year in the event that one of those members leaves the committee.

8. Use of data gathered by CCTV

8.1 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 using a cloud computing system. 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 location, we will carefully consider if they are appropriate by carrying out a data protection 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. 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. Requests for disclosure

11.1 No images from our CCTV cameras will be disclosed to any third party, without express permission being given by the Committee. Data will not normally be released unless satisfactory evidence has been produced that it is required for legal proceedings or under a court order.

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 to the Committee.

12.2 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

13.1 We recognise that, in rare circumstances, individuals may have a legal right to request erasure of personal data concerning them or to restrict the processing of their personal data. Any member of the public who considers that these rights apply to them in relation to our use of CCTV should speak to a member of the Committee in the first instance.