CCTV Policy

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 our staff and visitors. 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 staff, relating to their personal data, are recognised and respected.

1.2 This policy is intended to assist staff 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. DEFINITIONS

2.1 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.
- 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 as a result of the operation of our CCTV (or other surveillance systems).
- 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.
- Controllers: are the people who, or organisations which, determine the manner in which 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 users: are those of our employees 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 Data Protection Policy.
- Data processors: are any person or organisation that is not a data user (or other employee of a controller) that processes data on our behalf and in accordance with our instructions (for example, a supplier which handles data on our behalf).
- 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.

- 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.

3. ABOUT THIS POLICY

3.1 We currently use CCTV cameras to view and record individuals on and around our premises. 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.

3.2 We recognise that information we hold about individuals is subject to data protection legislation. The images of individuals recorded by CCTV cameras in the workplace are personal data and therefore subject to the legislation. We are a controller, and we have registered our use of CCTV with the Information Commissioner. We are committed to complying with our legal obligations and seek to comply with best practice suggestions from the Information Commissioner's Office (ICO).

3.3 This policy covers all employees and other individuals working and/or visiting our premises.

3.4 The policy will be regularly reviewed to ensure that it meets legal requirements, relevant guidance published by the ICO and industry standards.

4 PERSONNEL RESPONSIBLE

4.1 The Chief Executive officer has overall responsibility for ensuring compliance with relevant legislation and the effective operation of this policy. Day-to-day management responsibility for deciding what information is recorded, how it will be used and to whom it may be disclosed has been delegated to the Data Protection Officer and the Chief People Officer. Day-to-day operational responsibility for CCTV cameras and the storage of data recorded is the responsibility of the Facilities Coordinator.

5 REASONS FOR THE USE OF CCTV

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

5.1.1 to prevent crime and protect buildings and assets from damage, disruption, vandalism and other crime;

5.1.2 for the personal safety of staff, visitors and other members of the public and to act as a deterrent against crime. #

5.1.3 to support law enforcement bodies in the prevention, detection and prosecution of crime;

5.1.4 to assist in day-to-day management, including ensuring the health and safety of staff and others;

5.1.5 to assist in the effective resolution of disputes which arise in the course of disciplinary or grievance proceedings;

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

6 MONITORING

6.1 CCTV monitors the exterior of the building and the main entrance 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 Images are monitored by authorised personnel during working hours only.

7 HOW WE WILL OPERATE ANY CCTV

7.1 Where CCTV cameras are placed in the workplace, 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 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 We will ensure that live feeds from cameras and recorded images are only viewed by approved members of staff whose role requires them to have access to such data. This may include HR staff involved with disciplinary or grievance matters. 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 securely stored and will be retained for 30 days from the date of recording unless required for a longer period for any of the following reasons:

a) Evidence of a crime, incident, accident or health & safety event.
b) Disciplinary or internal investigation.
c) Subject Access Requests or legal/litigation obligations.

Once footage is no longer required, it will be permanently deleted or destroyed in a secure manner, and the deletion documented

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 workplace location, we will carefully consider if they are appropriate by carrying out a privacy impact assessment (PIA).

10.2 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

10.3 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.

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 ONGOING REVIEW OF CCTV USE

11.1 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.

12 REQUESTS FOR DISCLOSURE

12.1 We may share data with other group companies where we consider that this is reasonably necessary for any of the legitimate purposes set out above in Paragraph 5.1.

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

12.3 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.

12.4 We will maintain a record of all disclosures of CCTV footage subject to document retention guidelines. CCTV Policy V2 October 2025 PUBLIC

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

13 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 and should be made in writing, in accordance with Smart Energy Training Subject Access Request and Request for Information Policy.

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 subject access request, where we consider it necessary to do so.

14 COMPLAINTS

14.1 If any member of staff has questions about this policy or any concerns about our use of CCTV, then they should speak to their manager OR the Data Protection Officer and Chief People Officer in the first instance.

14.2 Where this is not appropriate or matters cannot be resolved informally, employees should follow the Smart Energy Training Complaints Process

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 GDPR). For further information regarding this, please contact the Data Protection Officer.

Version control number	Smart-Energy-08-PD-105
Version	V2
Last review date	2/10/25
Next review date	2/10/26
Policy Owner	Patrick Richter
Signed by Chief Executive Officer	 Gregg Scott Chief Executive Officer