# CCTV

**Document Control:**

| | |
|---|---|
| Policy Reference: | GF14 |
| Version Number: | 03 |
| Author: | Jess Cantrill |
| Reviewed By: | T. O'Boye |
| Verified By: | Toni Nye |
| Date of Last Review: | Apr 2024 |
| Date of Next Review: | Apr 2025 |

**Revision History:**

| Version Number | Version Date | Nature of Change | Date Approved |
|---|---|---|---|
| 01 | Sep 2019 | Policy re-written | Sep 2019 |
| 02 | May 2022 | Policy rebranded & updated in line with current BCP. | May 2022 |
| 03 | Apr 2024 | Policy Review | Apr 2024 |
| | | | |

**Contents:**

## 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.

1.3. This procedure does not form part of any employee's contract of employment and it may be amended at any time. We may also vary this procedure, including any time limits, as appropriate in any case.

## 2. Definitions

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

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

2.1.2. 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.

2.1.3. 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).

2.1.4. 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.

2.1.5. Data 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 data controller of all personal data used in our business for our own commercial purposes.

2.1.6. 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, any Privacy Notice and /or Data Protection Policy and any other associated data protection materials we may provide.

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

2.1.8. 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.

2.1.9. 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 that capture information of identifiable individuals or information relating to identifiable individuals.

## 3. Who Is Covered By The Procedure?

3.1. This policy covers all employees, directors, officers, consultants, contractors, freelancers, volunteers, interns, casual workers, zero hours workers and agency workers and may also be relevant to visiting members of the public.

## 4. Who Is Responsible For Implementing This Procedure?

4.1. The Board 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 Board. Day-to-day operational responsibility for CCTV cameras and the storage of data recorded is the responsibility of the Director

4.2. Responsibility for keeping this policy up to date is delegated via the Senior Leadership Team or the DPO.

4.3. Our Data Protection Officer and Data Controller for the purposes of GDPR is Wendy Barber.

## 5. About This Policy

5.1. 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. This policy also explains how to make a subject access request in respect of personal data created by CCTV.

5.2. We recognise that information that 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 committed to complying with all our legal obligations and seek to comply with best practice suggestions from the Information Commissioner's Office (ICO).

5.3. A breach of this policy may, in appropriate circumstances, be treated as a disciplinary matter. Following investigation, a breach of this policy may be regarded as misconduct leading to disciplinary action, up to and including dismissal.

## 6. Reasons For The Use Of CCTV

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

6.1.1. To prevent crime and protect buildings and assets from damage, disruption, vandalism and other crime;

6.1.2. For the personal safety of staff, visitors and other members of the public and to act as a deterrent against crime;

6.1.3. To support law enforcement bodies in the prevention, detection and prosecution of crime;

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

6.1.5. To assist in the effective resolution of disputes which arise in the course of disciplinary or grievance proceedings;

6.1.6. To assist in the defence of any civil litigation, including employment tribunal proceedings;

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

## 7. Monitoring

7.1. CCTV monitors the exterior of the building and both the main entrance and secondary exits along with communal areas 24 hours a day and this data is continuously recorded.

7.2. 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.

7.3. Surveillance systems will also be used to record sound.

7.4. Images are monitored by authorised personnel 24 hours a day every day of the year.

7.5. Staff using surveillance systems will be given appropriate training to ensure they understand and observe the legal requirements related to the processing of relevant data.

## 8. How We Will Operate Any CCTV

8.1. 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.

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

8.3. 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.

## 9. Use Of Data Gathered By CCTV

9.1. 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.

9.2. 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.

9.3. 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.

## 10. Retention And Erasure Of Data Gathered By CCTV

10.1. 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.

10.2. Data from CCTV cameras if not retained, will only be stored for a maximum of 90 days before auto-deleting in real time. This may be as little as 7 days as determined by the age and capability of the system.

10.3. 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 on a legal basis only for incidents to come to light. We will maintain a comprehensive log of when data is deleted.

10.4. 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.

## 11. Use Of Additional Surveillance Systems

11.1. 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 Data Protection Impact Assessment (DPIA).

11.2. 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.

11.3. 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.

11.4. 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.

## 12. Covert Monitoring

12.1. 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.

12.2. In the unlikely event that covert monitoring is considered to be justified, it will only be carried out with the express authorisation of the Operations Director and the DPO. 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 workers will always be a primary consideration in reaching any such decision.

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

12.4. 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.

## 13. Ongoing Review Of CCTV Use

13.1. 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.

13.2. We will review the use of CCTV cameras in the workplace at least annually in our ICO Annual Internal Audit.

## 14. Requests For Disclosure

14.1. We will share data with other group companies and other associated companies or organisations, for example shared services partners where we consider that this is reasonably necessary for any of the legitimate purposes.

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

14.3. 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.

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

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

## 15. Subject Access Requests

15.1. 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 which can be found in the staff handbook within the data protection policy.

15.2. 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.

15.3. 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.

## 16. Complaints

16.1. 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 Director in the first instance.

16.2. Where this is not appropriate or matters cannot be resolved informally, employees should use our formal grievance procedure.

## 17. Requests To Prevent Processing

17.1. 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.

## 18. Monitoring And Review

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

18.2. Line Managers and team leaders will be responsible for general monitoring of these guidelines. Transgression will be reviewed with individual staff members, but in some cases, it may be appropriate to record examples for discussion as part of staff training or discussion at team meetings. Significant and/or repeated breaches of this policy will lead to disciplinary action, up to and including dismissal.