

## CCTV Policy - Caban cyf

### 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.

**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.

**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 and our Data Protection Policy.

**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).

**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.

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

3.2 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).

3.3 This policy covers all employees, directors, officers, consultants, contractors, freelancers, volunteers, interns and may also be relevant to members of the public.

3.4 This policy is non-contractual and does not form part of the terms and conditions of any employment or other contract. We may amend this policy at any time. The policy will be regularly reviewed to ensure that it meets legal requirements, relevant guidance published by the ICO and industry standards.

3.5 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.

### **4. Personnel responsible**

4.1 The board of directors have overall responsibility for ensuring compliance with relevant legislation and the effective operation of this policy. Day-to-day operational responsibility for CCTV cameras and the storage of data recorded is the responsibility of the Executive Director.

### **5. Reasons for use of CCTV and surveillance systems**

5.1 We currently use CCTV on and 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 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 much of the exterior of our premises 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.

## **7. How we will operate 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 Live feeds from CCTV cameras will only be monitored where it is reasonably necessary for the security and management of the business.

7.3 We will ensure that recorded images are only viewed by approved members of staff whose role requires them to have access to such data. Recorded images will only be viewed by those authorised to do so. 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. Use of data gathered by CCTV or surveillance systems**

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.

## **9. Retention and erasure of data gathered by CCTV or surveillance systems**

9.1 Data recorded by our surveillance systems will be stored on secure internal servers. 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 62 days.

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.

9.3 Video clips relating to specific incidents may be retained for longer periods where required as specified in our Data Protection Policy (eg for investigations in relation to disciplinary or legal disputes or Health and Safety incidents).

## **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.

10.2 Consideration will be given as to 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 We 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, toilets) 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)

## **12. Ongoing review of CCTV and surveillance systems use**

12.1 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. Requests for disclosure**

13.1 No images from our CCTV cameras will be disclosed to any other third party (other than the police), without express permission being given by a 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.

13.2 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.

**13.3** We will maintain a record of all disclosures of CCTV footage.

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

## **14. Subject Access Requests**

**14.1** 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 or Customer Privacy Notice.

**14.2** 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.

**14.3** 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.

**14.5** Payment of a £10 fee (which is non-refundable if the request is declined) must accompany all data subject access requests. Requests will be processed within 40 calendar days of receipt of the fee.

## **15. Complaints**

**15.1** If any member of staff has questions about this policy or any concerns about our use of CCTV, then they should speak to their line manager.

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

## **16. Requests to prevent processing**

**16.1** 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 (see Articles 21 and 22 of the General Data Protection Regulation). For further information regarding this, please refer to our Data Protection Policy or Customer Privacy Notice.