Richard Edwards Group
CCTV Policy

Contents

1. Introduction

1.1 Richard Edwards Group is the trading name of RE Group Accountants Limited "The Firm" has in place a CCTV surveillance system "the CCTV system" across its offices. This policy details the purpose, use and management of the CCTV system at the Firm and details the procedures to be followed in order to ensure that the Firm complies with relevant legislation and the current Information Commissioner's Office Code of Practice.

1.2 The Firm will have due regard to the Data Protection Act 1998, the General Data Protection Regulation (GDPR) and any subsequent data protection legislation, and to the Freedom of Information Act 2000, the Protection of Freedoms Act 2012 and the Human Rights Act 1998. Although not a relevant authority, the Firm will also have due regard to the Surveillance Camera Code of Practice, issued under the Protection of Freedoms Act 2012 and in particular the 12 guiding principles contained therein.

1.3 This policy is based upon guidance issued by the Information Commissioner's Office, 'In the picture: A data protection code of practice for surveillance cameras and personal information'[1] ("the Information Commissioner's Guidance").

[1] https://ico.org.uk/media/for-organisations/documents/1542/cctv-code-of-practice.pdf

2. CCTV System overview

2.1 The CCTV system is owned by RE Group Accountants Limited, The Maltings, Rosemary Lane, Halstead, Essex, CO9 1HZ and managed by the Firm. Under the Data Protection Act 1998 the Firm is the 'data controller' for the images produced by the CCTV system. The Firm is registered with the Information Commissioner's Office and the registration number is Z7447258. The CCTV system operates to meet the requirements of the Data Protection Act and the Information Commissioner's Guidance.

2.2 The IT manager is responsible for the overall management and operation of the CCTV system, including activities relating to installations, recording, reviewing, monitoring and ensuring compliance with this policy.

2.3 Signs are placed at all entrances in order to inform staff, clients, and visitors that CCTV is in operation.

2.4 The IT manager is responsible for ensuring that adequate signage is erected in compliance with the ICO CCTV Code of Practice.

2.5 Cameras are sited to ensure that they cover all entrances to the Firm's premises as far as is possible.

2.6 Cameras are not sited to focus on external areas but may capture some images of the area immediately outside of the premises due to the focus on the buildings entrances.

2.7 The CCTV system is intended to operate between the hours of 17:30 and 08:00 Monday to Friday and 24 hours a day on Saturdays, Sundays and Public Holidays.

2.8 Any proposed new CCTV installation is subject to a Privacy Impact Assessment.

2.9 Further information regarding the number and location of CCTV cameras is available on request from the IT Manager.

3. Purposes of the CCTV system

3.1 The principal purpose of the Firm's CCTV system is as follows:
- for the prevention, reduction, detection and investigation of crime and other incidents;

3.2 The CCTV system will be used to observe the Firm's premises under surveillance in order to identify incidents requiring a response. Any response should be proportionate to the incident being witnessed.

3.3 The Firm seeks to operate its CCTV system in a manner that is consistent with respect for the individual's privacy.

4. Monitoring and Recording

4.1 Cameras may be monitored by Directors of the Firm or the IT Manager from anywhere in the world during the hours of operation. This will normally only occur in the event someone has triggered the security alarm however the Firm reserves the right to monitor the footage at any time if there are reasonable grounds to do so.

4.2 Images are recorded for 7 days by "Netgear" using Amazon cloud servers based in the EU.

4.3 The cameras installed provide images that are of suitable quality for the specified purposes for which they are installed.

4.4 All images recorded by the CCTV System remain the property and copyright of the Firm.

4.5 The monitoring of staff activities will be carried out in accordance with Part 3 of the Employment Practices Code.[2]

[2] https://ico.org.uk/media/for-organisations/documents/1064/the_employment_practices_code.pdf

5. Compliance with Data Protection Legislation

5.1 In its administration of its CCTV system, the Firm complies with the Data Protection Act 1998. Due regard is given to the data protection principles embodied in the Data Protection Act. These principles require that personal data shall be:

(a) processed fairly and lawfully;

(b) held only for specified purposes and not used or disclosed in any way incompatible with those purposes;

(c) adequate, relevant and not excessive;

(d) accurate and kept up to date;

(e) kept no longer than necessary for the particular purpose;

(f) processed in accordance with the rights of individuals;

(g) kept secure; and

(h) be kept within the European Economic Area unless the recipient country ensures an adequate level of protection.

5.2 With immediate effect, the Firm will also comply with the General Data Protection Regulation. Due regard will be given to the data protection principles contained within Article 5 of the GDPR which provide that personal data shall be:

(a) processed lawfully, fairly and in a transparent manner;

(b) collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes;

(c) adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed;

(d) accurate and, where necessary, kept up to date;

(e) kept in a form which permits identification of the data subjects for no longer than is necessary for the purposes for which the personal data are processed;

(f) processed in a manner that ensures appropriate security of the personal data, including protection against unauthorized or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organizational measures.

6. Applications for disclosure of images

Applications by individual data subjects

6.1 Requests by individual data subjects for images relating to themselves "Subject Access Request" should be submitted in writing to the Firm's Data Protection Manager together with proof of identification.

6.2 In order to locate the images on the Firm's system, sufficient detail must be provided by the data subject in order to allow the relevant images to be located and the data subject to be identified.

6.3 Where the Firm is unable to comply with a Subject Access Request without disclosing the personal data of another individual who is identified or identifiable from that information, it is not obliged to comply with the request unless satisfied that the individual has provided their express consent to the disclosure, or if it is reasonable, having regard to the circumstances, to comply without the consent of the individual.

Access to and disclosure of images to third parties

6.4 A request for images made by a third party should be made in writing to the IT Manager.

6.5 In limited circumstances it may be appropriate to disclose images to a third party, such as when a disclosure is required by law, in relation to the prevention or detection of crime or in other circumstances where an exemption applies under relevant legislation.

6.6 Such disclosures will be made at the discretion of the IT Manager, with reference to relevant legislation and where necessary, following advice from the Firm's Designated Members.

6.7 Where a suspicion of misconduct arises and at the formal request of the Staff Partner, the IT Manager may provide access to CCTV images for use in staff disciplinary cases.

6.8 A record of any disclosure made under this policy will be held on the CCTV management system, itemising the date, time, camera, requestor, authoriser and reason for the disclosure.

7. Retention of images

7.1 Unless required for evidential purposes, the investigation of an offence or as required by law, CCTV images will be retained for no longer than 7 days from the date of recording. Images will be automatically overwritten after this point.

7.2 Where an image is required to be held in excess of the retention period referred to in 7.1, the IT Manager or their nominated deputy, will be responsible for authorising such a request.

7.3 Images held in excess of their retention period will be reviewed on a three monthly basis and any not required for evidential purposes will be deleted.

7.4 Access to retained CCTV images is restricted to the IT Manager and the Designated Members of the firm unless otherwise authorised.

8. Complaints procedure

8.1 Complaints concerning the Firm's use of its CCTV system or the disclosure of CCTV images should be made in writing to the IT Manager.

9. Monitoring Compliance

9.1 All staff involved in the operation of the Firm's CCTV System will be made aware of this policy and will only be authorised to use the CCTV System in a way that is consistent with the purposes and procedures contained therein.

10. Policy review

10.1 The Firm's usage of CCTV and the content of this policy shall be reviewed annually by the IT Manager with reference to the relevant legislation or guidance in effect at the time. Further reviews will take place as required.

Implementation of the Policy

This policy is effective as of 30 July 2018. No part of the Policy is retrospective in effect and applies to matters occurring on or after 31 July 2018.

This Policy has been approved and authorised by:

Name: **Nigel Sheldrake**

Position: **Managing Partner**

Date: **1 June 2019**

Due for review by: **31 May 2020**

Signature: