HEALTH EXCHANGE CIC
CCTV POLICY

Revision History

Version	*Revision Date*	*Revised by*	*Section Revised*
1.0	22/11/2019	Jennifer Jones-Rigby & Siyana Dimova	Initial Version

Document Control

Document Owner: ***Jennifer Jones-Rigby***	***Document No:*** ***1.0***	***Status:*** Approved	***Date Approved:*** ***22/11/2019***
Security Classification: Low	***Next Review Date:*** ***21/11/2021***	***Version:*** V 1.0	***Department:*** Data

Contents

INTRODUCTION

Health Exchange CIC LTD *(hereinafter referred to as the **"Company"**)* uses closed circuit television (CCTV) images to provide a safe and secure environment for employees and for visitors to the Company's business premises, such as clients, customers, contractors and suppliers, and to protect the Company's property.

This policy sets out the use and management of the CCTV equipment and images in compliance with:

- Human Rights Act 1998
- Data Protection Act 2018
- General Data Protection Regulation (2016/679 EU)
- In the picture: a data protection code of practice for surveillance cameras and personal information (CCTV Code of Practice)

The Company's CCTV facility records images only. There is no audio recording i.e. conversations are not recorded on CCTV (but see the section on covert recording).

PURPOSES OF CCTV

The purposes of the Company installing and using CCTV systems include:

- To assist in the prevention or detection of crime or equivalent malpractice.
- To assist in the identification and prosecution of offenders.
- To monitor the security of the Company's business premises.
- To ensure that health and safety rules and Company procedures are being complied with.
- To assist with the identification of unauthorised actions or unsafe working practices that might result in disciplinary proceedings being instituted against employees and to assist in providing relevant evidence.
- To promote productivity and efficiency.

LOCATION OF CAMERAS

Cameras are located at strategic points outside the Company's business premises - at the entrance and exit points, as well as the forecourt/car park. The Company has positioned the cameras so that they only cover communal or public areas on the Company's business premises and they have been sited so that they provide clear images. No camera focuses, or will focus, on toilets, shower facilities, changing rooms, staff kitchen areas, staff break rooms or private offices.

All cameras (with the exception of any that may be temporarily set up for covert recording) are also clearly visible.

Appropriate signs are prominently displayed so that employees, clients, customers and other visitors are aware they are entering an area covered by CCTV.

RECORDING AND RETENTION OF IMAGES

Images produced by the CCTV equipment are intended to be as clear as possible so that they are effective for the purposes set out above. Maintenance checks of the equipment are undertaken on a regular basis by IT Consultants to ensure it is working properly and that the media is producing high quality images.

Images may be recorded either in constant real-time (24 hours a day throughout the year), or only at certain times, as the needs of the business dictate.

As the recording system records digital images, any CCTV images that are held on the hard drive of a PC or server are deleted and overwritten on a recycling basis and, in any event, are not held for more than 30

calendar days. Exception being footage which must be kept for longer periods of time to comply with relevant laws – such as responses to SARs, or when requested by law enforcement agencies, others. Once a hard drive has reached the end of its use, it will be disposed of in line with company's policies.

Images that are stored on, or transferred on to, removable media such as CDs are erased or destroyed once the purpose of the recording is no longer relevant. In normal circumstances, this will be a period of one month. However, where a law enforcement agency is investigating a crime, images may need to be retained for a longer period.

ACCESS TO AND DISCLOSURE OF IMAGES

Access to, and disclosure of, images recorded on CCTV is restricted. This ensures that the rights of individuals are retained. Images can only be disclosed in accordance with the purposes for which they were originally collected.

The images that are filmed are recorded centrally and held in a secure location. Access to recorded images is restricted to the operators of the CCTV system and to those nominated staff members who are authorised to view them in accordance with the purposes of the system. Viewing of recorded images will take place in a restricted area to which other employees will not have access when viewing is occurring. If media on which images are recorded are removed for viewing purposes, this will be documented.

Disclosure of images to other third parties will only be made in accordance with the purposes for which the system is used and will be limited to:

- The police and other law enforcement agencies, where the images recorded could assist in the prevention or detection of a crime or the identification and prosecution of an offender or the identification of a victim or witness.
- Prosecution agencies, such as the Crown Prosecution Service.
- Relevant legal representatives.
- Line managers involved with Company disciplinary and performance management processes.
- Individuals whose images have been recorded and retained (unless disclosure would prejudice the prevention or detection of crime or the apprehension or prosecution of offenders).

The Managing Director of the Company (or another senior manager, company's IG Lead or DPO acting in their absence) is the only person who is permitted to authorise disclosure of images to external third parties such as law enforcement agencies.

All requests for disclosure and access to images will be documented, including the date of the disclosure, to whom the images have been provided and the reasons why they are required. If disclosure is denied, the reason will be recorded in line with company's SAR policy

INDIVIDUALS' ACCESS RIGHTS

Under the UK's data protection laws, including the General Data Protection Regulation (GDPR), individuals have the right on request to receive a copy of the personal data that the Company holds about them, including CCTV images if they are recognisable from the image.

If you wish to access any CCTV images relating to you, you must make a written request to the Company's Data Protection Officer [Data Representative]. This can be done by using this email address ig@healthexchange.org.uk ; or write to us at Health Exchange CIC LTD, Avoca Court, 27 Moseley Road, Digbeth, Birmingham B12 0HJ. The Company will usually not make a charge for such a request, but we may charge a reasonable fee if you make a request which is manifestly unfounded or excessive, or is repetitive. Your request must include the date and approximate time when the images were recorded and the location of the particular CCTV camera, so that the images can be easily located and your identity can be established as

the person in the images.

The Company will usually respond promptly and in any case within one month of receiving a request. However, where a request is complex or numerous the Company may extend the one month to respond by a further two months.

The Company will always check the identity of the individual making the request before processing it and may refuse access to CCTV footage if the individual requesting the information has no right to to request such information (in line with company's SAR policy).

The Data Protection Officer [Data Representative] will first determine whether disclosure of your images will reveal third party information as you have no right to access CCTV images relating to other people.

If the Company is unable to comply with your request because access could prejudice the prevention or detection of crime or the apprehension or prosecution of offenders, you will be advised accordingly.

COVERT RECORDING

The Company will only undertake covert recording with the written authorisation of the CEO or COO acting in their absence where there is good cause to suspect that criminal activity or equivalent malpractice is taking, or is about to take, place and informing the individuals concerned that the recording is taking place would seriously prejudice its prevention or detection.

Covert monitoring may include both video and audio recording.

On this basis the Company will only undertake covert monitoring if it has carried out a data protection impact assessment which has addressed the following:

- the purpose of the covert recording;
- the necessity and proportionality of the covert recording;
- the risks to the privacy rights of the individual(s) affected by the covert recording;
- the time parameters for conducting the covert recording
- the safeguards and/or security measures that need to be put in place to ensure the covert recording is conducted in accordance with the data protection laws, including the GDPR.

If after undertaking the data impact assessment the Company considers there is a proportionate risk of criminal activity, or equivalent malpractice taking place or about to take place, and if informing the individuals concerned that the recording is taking place would seriously prejudice its prevention or detection, the Company will covertly record the suspected individual(s). In doing this the Company will rely on the protection of its own legitimate interests as the lawful and justifiable legal basis for carrying out the covert recording.

Before the covert recording commences the Company will ensure that CEO or COO acting in their absence) agrees with the findings of the data protection assessment and provides written authorisation to proceed with the covert recording.
Covert monitoring may include both video and audio recording.

Covert monitoring will only take place for a limited and reasonable amount of time consistent with the objective of assisting in the prevention and detection of particular suspected criminal activity or equivalent malpractice. Once the specific investigation has been completed, covert monitoring will cease.

Information obtained through covert monitoring will only be used for the prevention or detection of criminal activity or equivalent malpractice. All other information collected in the course of covert monitoring will be deleted or destroyed unless it reveals information which the Company cannot reasonably be expected to ignore.

STAFF TRAINING

The Company will ensure that all employees handling CCTV images or recordings are trained in the operation and administration of the CCTV system and on the impact of the laws regulating data protection and privacy with regard to that system. For instance, there will be a guide on operating CCTV available for nominated staff members to use.

IMPLEMENTATION

The Company's Data Protection Officer [Data Representative] is responsible for the implementation of and compliance with this policy and the operation of the CCTV system and they will conduct a regular review of the Company's use of CCTV. Any complaints or enquiries about the operation of the Company's CCTV system should be addressed to them. The Senior Management Team of the Company is responsible for approving changes to the operation of the CCTV and this policy in line with the business needs of the Company.

DATA PROTECTION

The Company will process the personal data collected in connection with the operation of the CCTV policy in accordance with its data protection policy and any internal privacy notices in force at the relevant time. Inappropriate access or disclosure of this data will constitute a data breach and should be reported immediately to the Company's Data Protection Officer [Data representative] in accordance with the Company's data protection policy. Reported data breaches will be investigated and may lead to sanctions under the Company's disciplinary procedure.