CCTV Policy

Document Control	
Document Type:	Policy
Department:	Data Protection
Relevancy:	Group-wide
Owner:	Information Services
Approver:	LTE Group Executive Team
Published Date:	2/03/2023
Version:	3
Security Classification:	External
Last Review Date:	28/02/2023
Next Review Date:	28/02/2024

Contents

1. Related documents

- Data Protection Policy
- LTE Group Privacy Notice - Colleagues, Workers & Contractors
- TMC Privacy Notice
- Total People Privacy Notice
- UCEN Privacy Notice

2. Introduction

LTE Group ("**LTE**") ("**we**", "**are**", "**us**") has closed circuit television surveillance systems (the "**CCTV system**", "**CCTV**") in place across its sites. This policy details the purpose, use and management of the CCTV system, alongside the procedures to be followed in order to ensure that we are compliant with relevant legislation.

LTE Group is registered with the **Information Commissioner's Office** ("**ICO**") and we will have due regard to the **Data Protection Act 2018** ("**DPA**") and the **UK General Data Protection Regulation** ("**GDPR**"), ensuring that our processing under this Policy meets the relevant requirements. We will also consider our obligations in relation to the **Freedom of Information Act 2000**, the **Protection of Freedoms Act 2012**, the **Human Rights Act 1998** and the **Surveillance Camera Code of Practice**.

This Policy and the procedures therein apply to all CCTV and covert installations, and any other system capturing recordings of identifiable individuals for the purpose of viewing and/or recording the activities of such individuals. CCTV recordings are recorded and accessed in strict accordance with this Policy. We seek to operate our CCTV system in a manner that is consistent with respect for individuals' privacy.

This Policy will be reviewed regularly by the **Data Protection Officer** ("**DPO**") and **Assistant Principal for Foundation Learning and Student Support** ("**Assistant Principal**") to ensure compliance to current and relevant legislation.

CCTV is currently in operation at the following LTE Group locations:

- **The Manchester College/UCEN Manchester campuses:** City Campus, Harpurhey, Nicholls, Openshaw, Shena Simon, Wythenshawe

3. Purposes of the CCTV system

The main purposes of LTE's CCTV systems are crime prevention, safeguarding, site security, to comply with legal obligations, and to assist in the investigation of suspected breaches of policy/procedure by staff, students, or the general public.

Under the DPA 2018, we are the '**Data Controller**' for the recordings produced by the CCTV system. Our lawful basis for this activity is that we have a *legitimate interest* to undertake this kind of personal data processing. Where we are reliant on the lawful basis of legitimate interest, we are obligated to undertake an assessment to ensure that the interests of data subjects are balanced against our own interests. Our Legitimate Interest Assessment is as follows:

Purpose	The main purposes of our CCTV systems are crime prevention, safeguarding, site security, to comply with legal obligations, and to assist in the investigation of suspected breaches of policy/procedure by staff, students or the general public. CCTV enables an operator to assess whether behaviour is suspicious, to identify if they are the suspect or victim of a crime or whether they match an identity as described in the case of a missing person for example. • To demonstrate a duty of care to students, staff and site visitors • To protect internal and external property of both LTE Group/Total People and its visitors • As a deterrent, e.g. to discourage anti-social behaviour and vandalism • To monitor active incidents and coordinate responses • To provide assistance in the detection and prevention of crime • To provide reassurance to site visitors • To create a secure and safe environment for all • To support our safeguarding responsibilities • To support access control systems • To provide a 'technical measure' under GDPR to protect paper and electronic personal data stored on sites
Necessity	The recording of these recordings will be used for the detection and prevention of crime, as well as to consider the safety within the site. Recordings can be reviewed to consider what has happened and if any corrective action either inside or outside of the organisation needs to be taken. There is no less intrusive way to achieve the same result. This is a standard procedure for the UK and one that is endorsed by law enforcement and other public safety bodies
Balance	There may or may not be a relationship with the individuals that are captured on CCTV. However, it is generally accepted that the data subjects will be at the site to enter, or fulfil a contractual obligation with LTE Group/Total People. Individuals would expect us to use their data in this way. This is the expected function of this type of system and in line with public perception, as well as standard operating practice governed by codes of conduct from the ICO, Home Office and law enforcement bodies.

	We are happy to explain the processing to them and it is outlined in the relevant Privacy Notices. The impact will be low to the individual, unless they have committed a crime, at which point their data would be reported to law enforcement and other authorities like the ICO or HSE as appropriate. If this data were to get into the public domain then it could be damaging to these parties, depending on their behaviour or conduct. It could also impact their rights or freedoms based on legal case, insurance claim or law enforcement intervention. As such, we have a CCTV Policy in place that outlines the strict handling and disclosure process for CCTV recordings. There are organisational and technical safeguards that are in place for the equipment, the use of recordings and any lawful processing / usage of this data. For example, only our Information Services department have administration rights to the CCTV system, meaning that opeartors cannot delete or edit the recordings obtained. Additionally, the **CCTV Policy** contains clear guidance on the process for download or disclosure of recordings. Individuals may object to this processing, and have the right to do so. This may mean that they are unable to use our services.

4. CCTV system overview

The CCTV system is operational for 24 hours a day, every day of the year. Cameras are sited to cover premises as far as possible. Cameras are installed throughout sites including roadways, car parks, and buildings (internally and externally). Cameras are not sited to focus on private residential areas. Where cameras overlook residential areas, privacy screens will be fitted.

Signage is in place around sites to inform staff, students, visitors, and members of the public that CCTV is in operation. The signage indicates who the CCTV system is managed by, its purpose, and relevant contact details. The relevant Facilities departments are responsible for ensuring that adequate signage is erected on their sites.

A Data Protection Impact Assessment (DPIA) has been undertaken in relation to this type of data processing. Any proposed new CCTV installation will also be subject to a new DPIA and must be raised with the DPO and Information Services prior to any commencement of procurement of new CCTV installation.

Access to retained CCTV recordings is restricted and the process is outlined in this Policy. Recordings are not permitted to be downloaded from the system without permission from the DPO.

4.1. The Manchester College/UCEN Manchester

The CCTV system is owned by LTE Group. The system vendor is HikCentral.

The Assistant Principal, alongside the DPO, are responsible for the overall management and operation of the CCTV system, including activities relating to recording, monitoring, storage, and secure destruction.

Information Services possess administration rights to the CCTV system. The DPO will authorise Information Security to grant authorised colleagues access to the CCTV system.

The DPO will provide advice and guidance on personal data-related matters.

Information Services and Facilities are responsible for procurement and installations.

Together, all departments ensure compliance with this Policy.

5. Monitoring and recording

Cameras are not monitored, unless responding to an active incident identified on the CCTV monitors.

CCTV monitors are housed in a designated and secure location, with limited colleague access. The monitors will be switched off unless responding to an incident, in line with the above listed purposes of the CCTV system. The CCTV will still be recording in the background when the monitors are switched off.

Some sites also have remote access capability, where designated colleagues can access the CCTV system through an online portal.

Recordings are recorded locally and are viewable by only designated and trained staff members.

The cameras installed provide recordings that are of suitable quality for the specified purposes for which they are installed. The recordings remain on the system for a short time. This can vary between a minimum of 28 days up to 90 days, depending on disc storage space, which is affected by how many cameras are operational.

All recordings remain the property and copyright of LTE Group.

5.1. Covert recording

The use of covert cameras will be restricted to rare occasions when a series of criminal acts have taken place within a particular area that is not otherwise fitted with CCTV. A request for the use of covert cameras will clearly state the purpose and reasons for use and must be submitted for review by the DPO.

Covert recording will only take place if informing the individual(s) concerned would seriously prejudice the reason for making the recording and where there are reasonable grounds to suspect that illegal or unauthorised activity is taking place. All such monitoring will be fully documented by the requestor and will only take place for a limited and reasonable period.

6. Compliance with data protection legislation

In our administration of the CCTV systems, we will comply with the Data Protection Act 2018. Due regard is given to the data protection principles embodied in the DPA 2018 and UK GDPR These principles require that personal data shall be:

1. Used lawfully, fairly and in a transparent way
2. Collected only for valid purposes that we have clearly explained to you and not used in any way that is incompatible with those purposes
3. Relevant to the purposes we have told you about and limited only to those purposes
4. Accurate and kept up to date
5. Kept only as long as necessary, for the purposes we have told you about
6. Kept securely

6.1. Monitoring compliance

All staff involved in the operation of the CCTV system will be made aware of this Policy and the DPIA; and will only be authorised to use the CCTV system in a way that is consistent with the purposes and procedures contained therein.

All staff with responsibility for accessing, recording, disclosing, or otherwise processing CCTV recordings will be required to undertake data protection training.

7. Subject access requests and disclosure of recordings

Any person whose data we process may request access to their own personal data at any time, this includes CCTV recordings. **Any such requests should be made directly to the DPO dpo@ltegroup.co.uk. Any request made to any other colleagues (including those permitted to access the CCTV system) must be immediately redirected to the DPO for action.** The DPO will respond to requests without undue delay, and within one month of receiving the request.

To locate the recordings on the system sufficient detail must be provided by the individual, in order to allow the relevant recordings to be located and the individual to be identified. This could include date, time, description of persons/events, etc.

The DPO may liaise with other colleagues who are authorised to access CCTV to facilitate the request.

Where we are unable to comply with a Subject Access Request without disclosing the personal data of another individual who is identified or identifiable from that information, we are not obliged to comply with the request unless satisfied that the other 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.

7.1. Third party disclosure

In limited circumstances it may be appropriate to disclose recordings to a third party, such as when a disclosure is required by law in relation to the prevention or detection of crime, to investigate suspected breaches of internal policies or procedures, or in other circumstances where an exemption applies under relevant legislation. Such disclosures will be made at the discretion of the DPO, with reference to relevant legislation.

Where a suspicion of misconduct or criminal activity arises, and at the formal request of the Investigating Officer or HR Manager/Advisor, we may provide access to CCTV recordings for use in disciplinary cases.

A record of any disclosure made under this Policy will be held with the DPO.

8. Retention of recordings

Recordings remain on the system for a short time. This can vary between a minimum of 28 days up to 90 days, depending on disc storage space, which is affected by how many cameras are operational.

Unless required for the investigation of an offence, or as required by law, CCTV recordings will be retained for no longer than one calendar month from the date of recording. Recordings will be automatically overwritten after this point.

Where an image is required to be held in excess of the standard retention period the DPO will be responsible for authorising such a request.

Recordings held in excess of the retention period will be reviewed on a monthly basis and any not required for specific and lawful purposes will be deleted.

9. Complaints

If you are unhappy with how we have handled your personal data in relation to our CCTV system you may lodge a formal complaint with the following department:

The Company Secretary & General Counsel
Executive Suite
LTE Group
Ashton Old Road
Manchester
M11 2WH

dpo@ltegroup.co.uk

If you do not wish to discuss this with us, or you are unhappy with our response, you also have the right to lodge a complaint with a supervisory authority, the Information Commissioner's Office (ICO). This can be done through live chat on the ICO website, or via the telephone:

www.ico.org.uk/livechat

0303 123 1113

More information on the ICO's complaint procedure can be accessed at: https://ico.org.uk/make-a-complaint/

10. Policy review

LTE's usage of CCTV, the content of this policy, and the DPIA, shall be reviewed annually by the DPO and Assistant Principal, with reference to the relevant legislation or guidance in effect at the time.