

## CCTV POLICY

### 1. INTRODUCTION

- (a) This Policy sets out how Luton Rising Airport Limited ("we", "our", "us", "Luton Rising") uses CCTV and processes CCTV images in accordance with the UK General Data Protection Regulation (**UK GDPR**) and the Data Protection Act 2018.
- (b) The purpose of this policy is to:
  - (i) outline why and how we will use CCTV, and how we will process data recorded by CCTV cameras;
  - (ii) ensure that the legal rights of individuals, relating to their personal data, are recognised and respected;
  - (iii) 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; and
  - (iv) explain how to make a subject access request in respect of personal data created by CCTV.
- (c) Some of Luton Rising's personal data is processed by Luton Council and this policy is intended to supplement the Council's data retention schedule and should be read in conjunction with them. In any instance of conflict, the Council's policies shall take precedence.

### 2. SCOPE

- (a) This Policy applies to all Luton Rising personnel ("you", "your"). You must read, understand and comply with this Policy when processing personal data on our behalf and attend training on its requirements. This Policy sets out what we expect from you for Luton Rising to comply with applicable law. Your compliance with this Policy is mandatory. Any breach of this Policy may result in disciplinary action.

### 3. RESPONSIBILITY

- (a) All individual business areas are responsible for ensuring all personnel comply with this Policy and need to implement appropriate practices, processes, controls and training to ensure that compliance.
- (b) The Data Protection Officer (**DPO**) is responsible for overseeing this Policy and, as applicable, developing any related policies and procedures. The DPO can be contact by emailing [DataProtection@lutonrising.org.uk](mailto:DataProtection@lutonrising.org.uk).
- (c) Please contact the DPO with any questions about the operation of this Policy or the UK GDPR or if you have any concerns that this Policy is not being or has not been followed.

### 4. DEFINITIONS

- (a) For the purposes of this policy, the following terms have the following meanings:
  - (i) **CCTV**: means fixed and domed cameras designed to capture and record images of individuals and property.
  - (ii) **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).

Version 1 implemented:

May 2022

Version 2 implemented:

December 2025

Review Date: December 2027

- (iii) **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.
- (iv) **Data controllers:** are the 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. Luton Rising is the data controller of all personal data used in our business for our own commercial purposes.
- (v) **Data processors:** is any organisation that processes data on our behalf and in accordance with our instructions (for example, a supplier which handles data on our behalf).
- (vi) **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.
- (vii) **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 such as automatic number plate recognition (ANPR), body worn cameras, unmanned aerial systems and any other systems that capture information of identifiable individuals or information relating to identifiable individuals.

## 5. REASONS FOR CCTV USE

- (a) We currently use CCTV at our office premises and on the Luton DART (Direct Air-Rail Transit) for legitimate business purposes, including:
  - (i) to prevent crime and protect buildings and assets from damage, disruption, vandalism and other crime;
  - (ii) for staff training purposes and for the personal safety of staff, visitors, DART passengers and other members of the public and to act as a deterrent against crime;
  - (iii) to detect, prevent and/or reduce harassment and disorder;
  - (iv) to support law enforcement bodies in the prevention, detection and prosecution of crime;
  - (v) to assist in day-to-day management, including ensuring the health and safety of staff and others, including crowd management; and
  - (vi) to assist in the defence of any civil litigation or the resolution of disputes.
- (b) This list is not exhaustive and other purposes may be or become relevant.

## 6. MONITORING

- (a) CCTV monitors the interior and exterior of our premises and the Luton DART 24 hours a day and this data is continuously recorded.
- (b) Camera locations are chosen to minimise viewing of spaces not relevant to the legitimate purpose of the monitoring.
- (c) Images are monitored by authorised personnel during working hours.

Version 1 implemented:

May 2022

Version 2 implemented:

December 2025

Review Date: December 2027

- (d) Staff using surveillance systems are given appropriate training to ensure they understand and observe the legal requirements related to the processing of relevant data.

## **7. OPERATION OF CCTV**

- (a) Where CCTV cameras are in use, we will ensure that signs are displayed at the entrance of the surveillance zone to alert individuals that their image may be recorded. The 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.
- (b) Live feeds from CCTV cameras will only be monitored where this is reasonably necessary, for example to protect health and safety.
- (c) 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.

## **8. USE OF DATA COLLECTED BY CCTV**

- (a) 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.
- (b) 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.
- (c) We will 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.

## **9. RETENTION AND ERASURE OF CCTV DATA**

- (a) 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. Exactly how long images will be retained for will vary according to the purpose for which they are being recorded. In most cases, recorded images will be kept for no longer than 31 days. Some CCTV data may be retained beyond 31 days if so required for investigative or evidential purposes. We will maintain a comprehensive log of when data is deleted.
- (b) 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.

## **10. DATA PROTECTION IMPACT ASSESSMENTS**

- (a) 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**).
- (b) 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.

Version 1 implemented:  
May 2022

Version 2 implemented:  
December 2025

Review Date: December 2027

- (c) 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.
- (d) 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.
- (e) Further guidance on the use of DPIAs can be found in Luton Rising's Data Protection Impact Assessment Procedure.

## **11. REQUESTS FOR DISCLOSURE**

- (a) No images from our CCTV cameras will be disclosed to any third party, without express permission being given by the Executive Director, Governance. Data will not normally be released unless satisfactory evidence that it is required for legal proceedings or under a court order has been produced.
- (b) 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.
- (c) We will maintain a record of all disclosures of CCTV footage.

## **12. SUBJECT ACCESS REQUESTS**

- (a) Individuals may make a request for disclosure of their personal information and this may include CCTV images (**subject access request**). Any subject access request received must be sent to the Data Protection Officer upon receipt in accordance with Luton Rising's Subject Access Request Procedure.
- (b) 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.
- (c) 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.

## **13. COMPLAINTS**

- (a) Any complaints made in relation to Luton Rising's use of CCTV must be directed to the Shared Services Manager in the first instance and, if necessary, to the Data Protection Officer.

## **14. REQUESTS TO PREVENT PROCESSING**

- (a) 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 UK General Data Protection Regulation). For further guidance, please see Luton Rising's Data Subject Rights Procedure.

## **15. CHANGES TO THIS POLICY**

We keep this Policy under regular review and will be reviewed every 2 years, unless there is a change in the law which requires this Policy to be reviewed earlier.

## **16. RELATED POLICIES AND PROCEDURES**

- (a) This Policy is implemented in conjunction with the following other policies and procedure:

- (i) IT Security Policy

Version 1 implemented:

May 2022

Version 2 implemented:

December 2025

Review Date: December 2027

- (ii) Data Breach Procedure
- (iii) Data Subject Rights Procedure
- (iv) Subject Access Request Procedure
- (v) Data Protection Policy
- (vi) Data Protection Impact Assessment Procedure
- (vii) Data Retention Policy

Version 1 implemented:  
May 2022  
Version 2 implemented:  
December 2025  
Review Date: December 2027