Leeds Bradford Airport

From the heart of Yorkshire

CLOSE CIRCUIT TELEVISION ("CCTV") POLICY

Date created: 5 April 2024

Functional owner: General Counsel

1. About this policy

1.1 At Leeds Bradford Airport Limited (**LBA**), safeguarding and handling your personal information in a compliant way is important to us. We understand and respect the importance of guarding your privacy and are committed to protecting your personal information. This policy outlines what you should expect when LBA collects your personal data (in the form of static or moving imagery) when you are in our airport and on our property. We are committed to not only protecting your personal data, but also to providing a safe and secure experience whilst passing through our airport.

1.2 When you enter our airport facilities or our land, we collect static or moving imagery via Close Circuit Television (**CCTV**) or Surveillance Systems. We collect imagery through the use of CCTV and Automatic Number Plate Recognition (**ANPR**), these cameras are located throughout the airport grounds/road networks in both landside and airside locations.

1.3 We use CCTV cameras to view and record individuals in, on and around our airport in order to maintain a safe environment for staff, business partners, suppliers, passengers and visitors. However, we recognise that the images of individuals recorded by CCTV cameras are personal data which must be processed in accordance with data protection legislation. As a controller, we have registered our use of CCTV with the Information Commissioner's Office (**ICO**) and seek to comply with its best practice suggestions.

1.4 The purpose of this policy is to:

(a) outline why and how we will use CCTV and other Surveillance Systems, and how we will process the data recorded;

(b) ensure that the legal rights of staff, business partners, passengers and other users of the airport, relating to their personal data, are recognised and respected;

(c) 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

(d) explain how to make a subject access request in respect of personal data created by CCTV.

1.5 This policy does not form part of any contract of employment or other contract to provide services, and we may amend it at any time.

1.6 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.

2. Who does this policy apply to?

2.1 This policy applies to all employees, officers, consultants, self-employed contractors, casual workers, agency workers, volunteers and interns.

3. Who is responsible for this policy?

3.1 The board of directors has overall responsibility for the effective operation of this policy and has delegated responsibility for overseeing its implementation to the General Counsel (**GC**). Suggestions for changes to this policy should be reported to the GC.

3.2 Any questions you may have about the day-to-day application of this policy should be referred to the Legal team in the first instance.

3.3 This policy is reviewed annually by the GC. We will also review the ongoing use of existing CCTV cameras at the airport at least every 12 months to ensure that their use remains necessary and appropriate, and that any Surveillance System is continuing to address the needs that justified its introduction.

4. Definitions

4.1 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.

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 controller of all personal data used in our business for our own commercial purposes.

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).

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.

Monitored Areas: means:

i. entry to and exit from our estate including our car parks;

ii. all public areas within the terminal and the external airside areas with public access;

iii. the exterior of the terminal;

iv. the landside and airside buses;

v. all internal and external operational areas of the airport; and

vi. offsite meet and greet parking storage facilities.

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.

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.

Processors: are any person or organisation that is not a data user (or other employee of a controller) that processes data on our behalf and in accordance with our instructions (for example, a supplier which handles data on our behalf).

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, ANPR as well as any technology that may be introduced in the future such as unmanned aerial systems and any other systems that capture information of identifiable individuals or information relating to identifiable individuals.

5. Reasons for the use of CCTV

5.1 We currently use CCTV and Surveillance Systems around the airport in the Monitored Areas 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, business partners, suppliers, passengers, visitors and other users of our airport and to act as a deterrent against crime;

(c) to support our staff, business partners and law enforcement bodies in the prevention, detection and prosecution of crime or potential crime;

(d) to assist in day-to-day management and the airport operations, including ensuring the health and safety of staff, business partners, passengers and other users of the airport and queue monitoring and management;

(e) for the protection of our land and assets;

(f) to assist in the effective resolution of disputes which arise in the course of disciplinary or grievance proceedings;

(g) to support and monitor the security measures in place at the airport;

(h) to assist in the investigation and effective resolution of incidents which occur at the airport including but not limited to injuries and complaints;

(i) to monitor the use of and access to and from our car parks;

(j) ANPR, to identify a vehicle's registration to grant a vehicle access to a car park and to monitor the entrance and exit times of a vehicle in our drop off facilities;

(k) to maintain safe and clear access to routes around the airport;

(l) to ensure compliance with the Department for Transport, Civil Aviation Authority and other statutory control authority requirements;

(m) to respond to a request exercised under the individual rights under the UK General Data Protection Regulation and the Data Protection Act; and

(n) to assist in the defence of any civil litigation, including employment tribunal proceedings.

This list is not exhaustive and other purposes may be or become relevant.

6. Monitoring

6.1 CCTV and Surveillance Systems monitor the Monitored Areas 24 hours a day by authorised personnel 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.

6.3 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.

7. How we will operate any CCTV

7.1 We will ensure that signs are displayed at the entrance of surveillance zones 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.

7.2 Live feeds from cameras and recorded images will be monitored at all times where this is reasonably necessary, and we will ensure that live feeds are only viewed by approved members of staff whose role requires them to have access to such data.

7.3 Recorded images will only be viewed in accordance with LBA policy by authorised personnel and will only be released on request by third parties following approval by LBA's Security and Legal teams.

8. Use of data gathered by CCTV

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. This may include encrypting the data, where it is possible to do so.

8.2 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.

8.3 We may 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 data gathered by CCTV

9.1 Data recorded by the CCTV system will be stored digitally on Network Video Recorders in the CCTV equipment room. 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 required in connection with an investigation and disciplinary/grievance, data will be kept long enough only for matter to be dealt with. In all other cases, recorded images will be kept for no longer than 31 days. We will maintain a comprehensive log of when data is deleted.

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.

10. Use of additional Surveillance Systems

10.1 Prior to introducing any new Surveillance System, including placing a new CCTV camera in any area other than a Monitored Area, we will carefully consider if they are appropriate in line with the operational requirements of LBA's CCTV strategy.

10.2 No surveillance cameras will be placed in areas where there is an expectation of privacy (for example, in changing rooms or 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) unless, in highly exceptional circumstances, there are reasonable grounds to suspect that criminal activity or extremely serious malpractice is taking place and, after suitable consideration, we reasonably believe there is no less intrusive way to tackle the issue.

11.2 In the unlikely event that covert monitoring is considered to be justified, it will only be carried out with the express authorisation of the Chief Operating Officer or the GC or their nominated representative. The decision to carry out covert monitoring will be fully documented and will set out how the decision to use covert means was reached and by whom. The risk of intrusion on innocent workers will always be a primary consideration in reaching any such decision.

11.3 Only limited numbers of people will be involved in any covert monitoring.

11.4 Covert monitoring will only be carried out for a limited and reasonable period of time consistent with the objectives of making the recording and will only relate to the specific suspected illegal or unauthorised activity.

12. Requests for disclosure

12.1 Our CCTV and Surveillance Systems footage may be shared with authorised third-party organisations (as listed below) provided they have completed our CCTV Footage Request Form and in order to assist in investigating an incident which occurred at the airport or on our land. The release of this footage to the authorised third-party organisation (listed below) must first be approved in writing by the Security and Legal teams.

(a) Border Force (part of the Home Office)

(b) Airport Personnel

(c) Airlines

(d) Baggage systems operators

(e) Police and/or law enforcement agencies and/or other statutory agencies

(f) Vehicle Control Services Limited (who manage our car parks).

12.2 No images from our CCTV cameras will be disclosed to any other third party, without express permission being given by the Security and Legal teams. Data will not normally

be released unless satisfactory evidence that it is required to investigate an incident and/or for legal proceedings or under a court order has been produced.

12.3 We will maintain a record of all disclosures of CCTV footage.

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

13. Subject access requests

13.1 Data subjects may make a request for disclosure of their personal information and this may include CCTV images (**DSAR**).

13.2 A DSAR is subject to the statutory conditions from time to time in place and should be made in writing by completing our Subject Access Request form which is available here.

13.3 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.

13.4 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. Complaints

14.1 If any member of staff has any concerns about our use of CCTV, they should email CCTV@lba.co.uk in the first instance.

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

15. Requests to prevent processing

15.1 We recognise that, in rare circumstances, individuals may have a legal right to request erasure of personal data concerning them or to restrict the processing of their personal data. Any member of staff who considers that these rights apply to them in relation to our use of CCTV should email CCTV@lba.co.uk in the first instance.