

AIR CULINAIRE WORLDWIDE UK LIMITED

AIR CULINAIRE WORLDWIDE VIDEO SURVEILLANCE (CCTV) PRIVACY NOTICE

Last updated: 08-Sep-2025

1. Introduction

- 1.1 This Video Surveillance (CCTV) Privacy Notice ("**Notice**") explains how Air Culinaire Worldwide UK Limited ("**ACW**", "**we**", "**us**", "**our**") collect, share and use any information that, alone or in combination with other information, relates to you ("**Personal Data**") in your capacity as an employee, contractor or visitor ("you" and "your") at ACW's premises. For the purposes of this Notice, in using CCTV and vehicle dashcams, the Personal Data process relates to your recorded image.
- 1.2 ACW, as a data controller is responsible for ensuring that the processing of Personal Data complies with applicable data protection law, specifically with the EU and UK General Data Protection Regulation, the UK's Data Protection Act, 2018 and the UK's Data Use and Access Act 2025.
- 1.3 This Notice also sets out the rights that you have in relation to the Personal Data that we process about you and how you can exercise them.
- 1.4 ACW treats compliance with its privacy obligations seriously. This is why we have developed this Notice, which describes the standards that ACW applies to protect Personal Data.

Please take the time to read this Notice carefully. If you have any questions or comments, please contact :

dataprivacy@univ-wea.com.

2.Scope

This Notice outlines why we use CCTV and other video capture technology including dashcams ("**CCTV**"), how we

use CCTV and how we process your Personal Data recorded by CCTV cameras to ensure we are compliant with data protection law and best practice.

3. Purpose of Processing

3.1 ACW uses CCTV for a number of purposes, including:

- To comply with legal or regulatory obligations
- To detect, prevent or reduce the incidence of crime
- To ensure compliance with ACW's policies at its premises
- To create a safer environment at ACW's premises
- To gather evidence by a fair and accountable method
- To monitor and assist with health and safety and other serious occurrences
- To detect, prevent and reduce the incidence of any incidents and any internal conduct and performance matters which can lead to ACW's disciplinary procedure being initiated as well as investigation of such matters
- To support authorized parties including the police force, UK Border Force, the CAA, aviation authorities, air traffic control functions, airport operators and airport security

3.2 An incident may include theft, damage to property, an employee disciplinary investigation, violence, breaches of law, regulations or policies applicable to ACW and other incidents that may impact upon the safety of people or property within ACW's premises as determined by ACW Management from time to time.

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

4. Lawful Bases for Processing

Employees, contractors and visitors have legitimate expectations of reasonable privacy within ACW's premises. Where the use of CCTV is not a legal obligation, ACW has other obligations and responsibilities, which it must comply with and balance against the privacy rights of data subjects, particularly in respect of incidents affecting ACW. These obligations include protecting the vital interests of individuals and relying on ACW's legitimate interest to use CCTV for the purposes of

securing and protecting its premises as well as individuals at its premises.

5. Position of cameras

5.1 ACW's CCTV surveillance monitors the internal areas as well as the external areas of the ACW building (excluding those areas where we are not legally permitted to record (for example toilets)).

5.2 The CCTV system does not record sound.

5.3 In addition, vehicle dashcams are used to record images inside and outside of vehicles when vehicles are used at our premises.

5.4 Images are monitored by authorized personnel.

6. How we will operate any CCTV

6.1 Where CCTV cameras are positioned, signs are prominently displayed to alert individuals that their image may be recorded. Such signs contain details of ACW, as the controller operating the CCTV system, the purpose for using the surveillance system, who to contact for further information, and a hyperlink to this Notice.

6.2 The CCTV system is regularly maintained in accordance with the manufacturer's instructions.

7. Use and retention of data gathered by CCTV

Access to footage

Images captured by ACW's CCTV system are kept on the CCTV system. For operational purposes, and in accordance with the stated purposes of the CCTV system, only designated employees, trained in their duties, have access to live footage.

Access to recordings

For operational purposes and in accordance with the stated purposes of ACW's CCTV system, only designated employees shall have access to CCTV recordings. We may permit the viewing (or sharing of copies) of CCTV records with third

parties such as the Police and employees where this is appropriate for security reasons or in connection with a serious incident, subject in each case to approval by Data Protection Officer.

Downloading of recorded material

Data should only be downloaded or saved if it forms part of an investigation into a serious incident including an employee's conduct or performance matter. Requests to view or receive copies of CCTV recordings must be approved by Data Protection Officer.

At the end of their useful life, all images downloaded for a legitimate purpose in whatever format, are erased permanently and securely. Any physical matter such as tapes or discs are disposed of as confidential waste. Any photographs and hard copy prints are disposed of as confidential waste.

8. Retention and erasure of data gathered by CCTV

Recordings of CCTV are held for the period set out below and then overwritten, unless there is a legitimate reason for downloading the footage (e.g. for the purposes of investigating alleged employee misconduct, for the investigation of an alleged or suspected crime etc.):

- CCTV: a maximum of 60 days
- Dashcam footage: a minimum rolling-basis of 90 days

The footage is then deleted as soon as the purpose for its download has been achieved (unless ACW is under legal obligation to retain such footage).

9. Use of additional CCTV cameras

9.1 Any assessment will consider the nature of the problem that we are seeking to address at that time and whether a CCTV camera is likely to be an effective solution, or whether a better or less intrusive solution exists. In particular, we will consider the effect the CCTV cameras will have on individuals and therefore whether its use is a proportionate response to the problem identified.

9.2 No surveillance cameras will be placed in areas where there is an expectation of privacy (for example, in changing rooms or washrooms).

10. Covert monitoring

- 10.1 ACW 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.
- 10.2 In the unlikely event that covert monitoring is considered to be justified, any authorization to use covert monitoring will be documented in writing. The authorization will include confirmation that covert monitoring is required to obtain evidence of suspected criminal activity in a specific case, an assessment of the alternative methods of obtaining the evidence and the permitted duration of the covert recording. The authorization will be regularly reviewed, for example, every 28 days, to assess whether it is continued to be required or should cease.
- 10.3 Only a limited number of people will be involved in any covert monitoring.

11. Sharing of personal data

- 11.1 ACW may share personal data about employees, contractors, visitors and other individuals processed by ACW in accordance with this policy with:
- ACW employees (where authorized to receive such information).
 - ACW group entities.
 - Service providers providing services to ACW (e.g. companies engaged by ACW provide maintenance on security services or hosting services).
 - Police and other crime prevention and law enforcement agencies as well as public and local authorities.

- Legal advisers and insurers in respect of any claim or incident involving ACW.
- Aviation authorities, air traffic control functions, airport operators and airport security.
- Data subjects in accordance with their rights.

11.2 Personal data will only be shared where necessary for the purposes specified in this Notice and in accordance with legal and regulatory requirements applicable to ACW.

12. Security

12.1 **Technical Protective Measures:** We have put in place appropriate security measures to prevent personal data from being accidentally lost, used or accessed in an unauthorized way, altered or disclosed. This includes the fact that access to the CCTV system is password protected.

12.2 We have put in place procedures to deal with any suspected personal data breach and will notify any affected individuals and/or the regulator where appropriate.

13. Training

All staff with access to the CCTV system receive periodic training on data protection, security practices, and appropriate handling of personal data.

14. Individuals' Rights

14.1 The law provides individuals (data subjects) with the following rights in relation to their personal data held by ACW:

14.2 The right to:

request access to their personal data (commonly known as a "data subject access request"). This enables them to receive a

copy of the personal data we hold about them and to check that we are lawfully processing it.

- request correction of the personal data that we hold about them. This enables them to have any incomplete or inaccurate information we hold about them corrected.
- request erasure of their personal data in certain circumstances. This enables them to ask us to delete or remove personal data where there is no good reason for us continuing to process it. Data subjects also have the right to ask us to delete or remove their personal data where they have exercised their right to object to processing (see below); and
- request the restriction of processing of their personal data. This enables them to ask us to suspend the processing of personal data about them, for example if they want us to establish its accuracy or the reason for processing it.
- In addition, a data subject may object to the processing of their personal data where we are relying on a legitimate interest (or those of a third party) and there is something about their particular situation which makes them want to object to processing on this ground.

14.3 These rights are not absolute and are subject to various conditions under applicable data protection and privacy legislation and the laws and regulations to which ACW is are subject to.

14.4 We will deal with any requests made from data subjects to exercise their above rights in accordance with the law.

14.5 A data subject has the right to make a complaint at any time to the ICO, the UK data protection regulator. The ICO can be contacted by telephone on 0303 123 1113 or by post as follows: Information Commissioners Office, Wycliffe House, Water Lane, Wilmslow, Cheshire, SK9 5AF or via email at casework@ico.org.uk. ACW would, however, appreciate the chance to deal with any concerns before the data subject approaches the ICO using the detail in.

15. Contact Us

Any queries or complaints about the CCTV system should be addressed dataprivacy@univ-wea.com.