



USEL

CCTV Policy

DOCUMENT MANAGEMENT

The purpose of this section is to provide details of the official versions and controls relating to the management of the CCTV Policy.

KEY PERSONNEL

Role	Responsible Person	Responsible Action
Author	Compliance Manager	Draft
Manager	DPO – Data Protection Officer	Review
Owner	Board	Approval

DOCUMENT HISTORY

Version	Date	Reason for update
1.0	Jan 2018	Draft for Review
2.0	Mar 2018	Updated based on DPO feedback
3.0	May 2024	Removal of manager names
4.0	Feb 2026	Review from Data Protection Officer (DPO)

CCTV policy

1. Introduction

USEL uses closed circuit television (CCTV) video images to: provide a safe and secure environment for employees and for visitors to USEL's business premises, such as clients, customers, contractors and suppliers; and to protect USEL's property.

This policy sets out the use and management of the CCTV equipment and images in compliance with the Data Protection Act 2018 & General Data Protection Regulations (GDPR 2018) and the CCTV Code of Practice, which is available on the ICO Website <https://ico.org.uk/media/1542/cctv-code-of-practice.pdf>

USEL's CCTV facility records video images only. There is no audio recording i.e. conversations are not recorded on CCTV

2. Purposes of CCTV

The purposes of USEL installing and using CCTV systems

Provide a safe and secure environment for employees, contractors, customers and visitors. To support health and safety incident response and investigation where relevant.

- To assist in the prevention or detection of crime or equivalent malpractice **NOTE:** all internal recordings are for insurance purposes only and as agreed with Union Representatives, will not be used to discipline or monitor the performance of employees;
- To assist in the identification and prosecution of offenders; and
- To monitor the security of USEL's business premises.

Our lawful basis for processing CCTV footage is legitimate interests (Article 6(1)(f) UK GDPR). We have carried out and retain a Legitimate Interests Assessment (LIA) demonstrating that processing is necessary for the purposes above and that our interests are not overridden by the rights and freedoms of individuals. Where footage is shared with law enforcement, the relevant provisions of the Data Protection Act 2018 also apply.

3. Location of cameras

Cameras are located at strategic points throughout USEL's business premises, principally at the Entrance and Exit points, Recycling and Factory areas. The internal cameras are located in the Factory and Recycling areas of the building only, due to the higher risk associated in relation to Health & Safety in these areas. USEL has positioned the cameras internally and externally so that they only cover communal or public areas on USEL's business premises and so that they provide clear images. No camera focuses on, or will focus on, toilets, shower facilities, changing rooms, staff kitchen areas, staff break rooms or private offices.

No use is made of concealed cameras.

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

4. Recording and retention of images

Video 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 to ensure it is working properly and that the media is producing high quality Video images.

Video Images are recorded in real-time (24 hours a day throughout the year).

As the recording system records digital video images, any CCTV images that are held on a secure storage device are deleted and overwritten on a recycling basis and, in any event, are not usually held

for more than 30 days to view for authorized reasons. Once a storage device has reached the end of its use, it will be erased prior to disposal.

Video 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 (this is only done for requests from authorized bodies e.g. insurance company or police). In normal circumstances, this will be a period of 30 days, however, where a law enforcement agency is investigating a crime, video images may need to be retained for a longer period.

5. Access to and disclosure of images

Access to, and disclosure of, video images recorded on CCTV is restricted to authorized personnel (system administrators and nominated managers). This ensures that the rights of individuals are observed. Video Images will 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 access-controlled room with risk informed controls in place. A monitoring station for external CCTV only is located at our reception desk. Access to recorded images is restricted to the operators of the CCTV system and to those managers who are authorized 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, this will only happen when a warrant has been issued by the police.

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.
- Insurers.
- Relevant legal representatives.
- 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 CEO of USEL (or The Head of Operations and IT Manager acting in their absence) is the only person who is permitted to authorize 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.

6. Individuals' access rights

Under the Data Protection Act 2018 & UK GDPR, individuals have the right on request to receive a copy of the personal data that USEL holds about them, including CCTV images if they are recognizable from the image.

If you wish to access any CCTV images relating to you, you must make a written or verbal request to USEL's Data Protection Officer, at USEL, 182-188 Cambrai Street, Belfast, BT13 3JH Tel 028 9035 6600. 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.

We will respond without undue delay and within one calendar month of receipt of the request (this may be extended by up to two further months for complex requests, in which case we will notify the requester within the first month).

USEL will always check the identity of the individual making the request before processing it.

The Data Protection Officer 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. In this case, the images of third parties may need to be obscured if it would otherwise involve an unfair intrusion into their privacy. This will be informed by the guidance in place from the ICO

If USEL 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, where possible, be advised accordingly.

7. Staff training

USEL will ensure that only those who are trained in the operation and administration of the CCTV system and on the impact of the Data Protection Act 1998, with regard to that system, will handle CCTV images or recordings.

8. Implementation

Any loss, unauthorized access, or inappropriate disclosure of footage is treated as a potential personal data breach and escalated in line with our Data Protection and Information Security Incident Procedure. Where required, we will notify the ICO within 72 hours and affected individuals without undue delay.

USEL's Data Protection Officer is responsible for the implementation of and for monitoring and oversight of compliance with this policy with regard to the operation of the CCTV system. They will regular reviews of USEL's use of CCTV. Any complaints or enquiries about the operation of CCTV system should be addressed to them in the first instance.