CCTV POLICY

Introduction

Under the **Protection of Freedoms Act 2012** the processing of personal data captured by CCTV systems (including images identifying individuals) is governed by the **General Data Protection Regulation (GDPR)** and the Information Commissioner's Office (ICO) has issued a code of practice on compliance with legal obligations under that Act.

Objectives and targets

This CCTV policy explains how G.English Electronics (Gelec) will operate its CCTV equipment and comply with the current legislation.

Action plan

Gelec uses CCTV equipment to provide a safer, more secure environment for staff and to prevent vandalism and theft. Essentially it is used for:

- The prevention, investigation and detection of crime.
- The apprehension and prosecution of offenders (including use of images as evidence in criminal proceedings).
- Safeguarding public and staff safety.
- Monitoring the security of the site.

Gelec does not use the CCTV system for covert monitoring.

Location

Cameras are located in those areas where the company has identified a need and where other solutions are ineffective. The CCTV system is used solely for purposes(s) identified above and is not used to routinely monitor staff conduct.

Maintenance

The CCTV system is maintained by SGN Fire & Security (contractor) under an annual maintenance contract that includes periodic inspections.

The contractors are responsible for:

- Ensuring the company complies with its responsibilities in relation to guidance on the location of the camera.
- Ensuring the date and time reference are accurate.
- Ensuring that suitable maintenance and servicing is undertaken to ensure that clear images are recorded.
- Ensuring that cameras are protected from vandalism in order to ensure that they remain in working order.

Identification

In areas where CCTV is used the company will ensure that there are prominent signs placed at both the entrance of the CCTV zone and within the controlled area.

The signs will:
- Be clearly visible and readable.
- Contain details of the organisation operating the scheme, the purpose for using CCTV and who to contact about the scheme.
- Be an appropriate size depending on context.

Type of equipment

The standard CCTV cameras in use record visual images only and do not record sound.

Administration

The data controller, Steve Bunn, has responsibility for the control of images and deciding how the CCTV system is used. The company has notified the Information Commissioner's Office of both the name of the data controller and the purpose for which the images are used. All operators and employees with access to images are aware of the procedures that need to be followed when accessing the recorded images.
All operators are trained in their responsibilities under the CCTV Code of Practice. Access to recorded images is restricted to staff that need to have access in order to achieve the purpose of using the equipment. All access to the medium on which the images are recorded is documented. All employees are aware of the restrictions in relation to access to, and disclosure of, recorded images.

Image storage, viewing and retention

Recorded images will be stored in a way that ensures the integrity of the image and in a way that allows specific times and dates to be identified. Access to live images is restricted to the CCTV operator unless the monitor displays a scene which is in plain sight from the monitored location. Recorded images can only be viewed in a restricted area by approved staff. The recorded images are viewed only when there is suspected criminal activity and not for routine monitoring of staff or visitors unless the camera(s) are installed to monitor the safe movement of persons through a designated area eg corridors (these areas will be identifiable by clear signs).
The company reserves the right to use images captured on CCTV where there is activity that cannot be expected to ignore such as criminal activity, potential gross misconduct, or behaviour which puts others at risk. Images retained for evidential purposes will be retained in a locked area accessible by the system administrator only. Where images are retained, the system administrator will ensure the reason for its retention is recorded, where it is kept, any use made of the images and finally when it is destroyed.
Neither the Data Protection Act nor the Information and Records Management Society prescribe any specific minimum or maximum periods which apply to CCTV recorded images. The company ensures that images are not retained for longer than is necessary. Once the retention period has expired, the images are removed or erased.

Disclosure

Disclosure of the recorded images to third parties can only be authorised by the data controller. Disclosure will only be granted:
- If its release is fair to the individuals concerned.
- If there is an overriding legal obligation (eg information access rights).
- If it is consistent with the purpose for which the system was established.

All requests for access or for disclosure are recorded. If access or disclosure is denied, the reason is documented. NB: Disclosure may be authorised to law enforcement agencies, even if a system was not established to prevent or detect crime, if withholding it would prejudice the prevention or detection of crime.

Subject access requests

Individuals whose images are recorded have a right to view images of themselves and, unless they agree otherwise, to be provided with a copy of the images. If the company receives a request under the **General Data Protection Regulation** (GDPR) it will comply with requests within 30 calendar days of receiving the request. The company may charge a fee for the provision of a copy of the images. As a general rule, if the viewer can identify any person other than, or in addition to, the person requesting access, it will be deemed personal data and its disclosure is unlikely as a Freedom of Information request.
Those requesting access must provide enough detail to allow the operator to identify that they are the subject of the images, and for the operator to locate the images on the system. Requests for access should be addressed to the data controller. Refusal to disclose images may be appropriate where its release is:

- Likely to cause substantial and unwarranted damage to that individual.
- To prevent automated decisions from being taken in relation to that individual. Monitoring and evaluation

The company undertakes regular audits to ensure that the use of CCTV continues to be justified. The audit includes a review of:

- Its stated purpose.
- The location.
- The images recorded.
- Storage length.
- Deletion.

Reviewing

The efficiency of this policy will be reviewed annually by Management. If the company decides to change the way in which it uses CCTV, it will inform the Information Commissioner within 28 days.