CCTV POLICY STATEMENT

1. PURPOSE AND SCOPE

1.1 Purpose

FloPlast Ltd (referred to as "we", "us", "our") uses closed circuit television (CCTV) images to provide a safe and secure environment for staff, customers, suppliers, and visitors and to protect company property.

This document sets out the accepted use and management of the CCTV equipment and images to ensure that we comply with relevant data protection and privacy laws including: the General Data Protection Regulation 2016 and the Data Protection Act 2018 (together referred to as the "GDPR"), and related laws including but not limited to, the Human Rights Act 1998 ("CCTV Laws").

This policy has been produced in line with the Information Commissioner's Office ("ICO") CCTV Code of Practice.

We reserve the right to change this policy at any time and will notify all members of staff of those changes via email.

1.2 Scope

CCTV digital images (if they show an identifiable person) constitute personal data, and are covered by the GDPR, as well as all other CCTV Laws. This policy should be read alongside our Data Privacy Policy, the provisions of which should be always adhered to. A copy of our Data Privacy Policy can be found in the Human Resources the policies folder within the public drive.

This policy relates to the use and management of CCTV throughout our premises, in relation to cameras sited at all factories and depots. This policy covers the use of both static recording cameras and Unmanned Aerial Vehicles (drone) imagery.

2. METHOD OF ANNOUNCEMENT (Distribution)

New Starters:
Distribution will be via the employment handbook and induction.

Managers:
Managers are notified of amendments / new issue via email with reference to the local p drive. Managers must also ensure that it is brought to the attention of their staff without access to emails through local communication forums.

Employees:
Employees are notified via email. In addition, the policy will be placed on the relevant notice boards and notified through local communication forums.

Contractors/ Visitors:
Via the site induction

2.1 Your responsibility to comply with this policy

The Data Protection Champion ("DPC") is responsible for ensuring compliance with this policy. That post is held by Neil Harrison privacy@floplast.co.uk. Any questions about the operation of this policy or any concerns that the policy has not been followed should be referred to the DPC.

The ICO has regulatory oversight of the application of this policy within our organisation and is ultimately responsible for ensuring compliance with it, the GDPR and CCTV Laws.

All staff including but not limited to employees, workers, contractors, self-employed consultants, agency workers, must comply with this policy and any document referenced in it. Failure to do so may expose us and our staff to serious civil and/or criminal liability.

Your failure to comply with this policy will constitute an act of misconduct or gross misconduct if severe enough, which may result in disciplinary action, up to and including dismissal. Contract staff and consultants may face the termination of their contract.

Staff must not allow personal data to be transferred to a person or entity (whether a group company or a third party) located outside the EEA (meaning the 27 EU member states, the UK, Norway, Iceland, and Liechtenstein) without the prior written approval of the DPC. Please refer to our Data Privacy Policy for further details.

3. PURPOSE OF CCTV

We have considered and determined that the purposes for which the CCTV is deployed are legitimate as well as being reasonable, appropriate, and proportionate. We currently use CCTV at FloPlast's sites for the following purposes and on the legal bases set out in our Data Privacy Policy. We have installed CCTV systems to:

- deter crime;
- assist in the prevention and detection of crime;
- assist with the identification, apprehension, and prosecution of offenders;
- to assist in day-to-day management (including monitoring security and health and safety at our facilities / stores / offices / yard areas / etc);
- to assist specific operational management processes (including the use of Unmanned Aerial Vehicle (drone) footage to view otherwise inaccessible locations e.g., roof areas);
- to investigate suspected breaches of our various policies and procedures where it may be construed as gross misconduct;
- to assist in the effective resolution of disputes which arise during disciplinary or grievance proceedings; and
- 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.

The CCTV system will NOT be used:

- to provide recorded images for the world-wide-web, advertising or marketing;
- for any automated decision taking;
- staff performance assessment;
- staff time keeping; or
- monitoring private and residential areas / premises. Before installing and using CCTV systems on our premises, the following steps have been considered
- assess and document the appropriateness of and reasons for using CCTV;
- establish and document the purpose of the proposed scheme;
- establish and document who is responsible for day-to-day compliance with this policy;
- ensure signage is displayed to inform individuals that CCTV is in operation, and that CCTV operations are covered in our various privacy policies including but not limited to our Workforce Privacy Notice; and
- keep a record of the CCTV installed and used.

4. COVERT RECORDING / MONITORING OF STAFF

We, and / or authorised staff (including authorised third parties) should ordinarily only undertake covert recording in exceptional circumstances and in accordance with the GDPR and ICO Guidelines. Covert recording will not be authorised without prior consultation with the DPC. Covert surveillance is carried out in an appropriate and compliant manner to ensure that the subjects of the surveillance are unaware that it is, or may be, taking place. Any such covert monitoring must only be carried out for a limited and reasonable amount of time consistent with the objectives of monitoring, and only for the prevention of a specific suspected unauthorised activity (e.g., anti-fraud, theft, etc.). All such occasions must be fully documented showing who made the decision to use covert monitoring and why.

All our maintained cameras must otherwise be readily visible to any person in the vicinity with suitable signage displayed.

As their usage is to monitor the general activities happening in the vicinity, such monitoring is not covert, and authorisation is not required. If the CCTV cameras target a particular individual, and are being used to monitor that individual's activities, that becomes a specific operation and will require authorisation.

5. POSITIONING CAMERAS AND MONITORING

CCTV monitors the interior and exterior of all FloPlast's buildings and the exterior of all factory-based offices. The CCTV is active 24 hours a day and this data is continuously recorded. Images are monitored by authorised staff 24 hours a day, every day of the year. Camera operators will receive training and access to written procedures for maintaining and respecting the privacy of residents (both business and residential), staff and customers / contractors.

Camera locations must be chosen to minimise viewing of spaces not relevant to the legitimate purpose of monitoring. As far as practically possible, no cameras will focus on residential or private accommodation or property. Camera locations must be chosen to minimise viewing of spaces not relevant to the legitimate purpose of monitoring. As far as practically possible, no cameras will focus on residential or private accommodation or property.

Apart from exceptional circumstances as noted above, cameras must not be hidden from view and must be sited in such a way as to ensure that they only monitor spaces intended to be covered.

If, for any reason, any neighbouring domestic areas that border our premises are included in the camera view, the occupants of the property should be consulted prior to any recording or recording for those areas will be disabled / blacked out.

The installation of cameras in areas in which individuals would have an expectation of privacy will not be authorised under this policy, except where there are exceptional circumstances, and subject to approval by the DPC, responsible for the area subject to the planned covert monitoring.

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.

We must clearly display signs in the vicinity of the cameras so that staff, visitors, and customers / contractors are aware they are entering an area covered by CCTV. Our CCTV signs must state:

- that we are responsible for the CCTV scheme;
- the purpose(s) of the CCTV scheme and how the recordings may be used;
- contact details for queries regarding the CCTV scheme.

6. ADDITIONAL SURVEILLANCE SYSTEMS

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).

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.

Any DPIA will consider the nature of the problem that we are seeking to address at that time and whether the use of surveillance systems is likely to be an effective solution, or whether a better solution exists. We will consider the effects of the surveillance system use on individuals and therefore, whether its use is a proportionate response to the problem identified.

7. IMAGE QUALITY

Images produced by the equipment must be as clear as possible so that they are effective for the purpose(s) for which they are intended.

The following standards must be adhered to:

- after installation, make an initial check of the equipment to ensure it works properly;
- ensure that digital images or tapes, where used, are of good quality;
- we will not continue to use media once it becomes clear that the quality of the images has begun to deteriorate;
- where time / date of images are recorded, these should be accurate and documented to ensure accuracy;
- site the cameras so they will capture images relevant to the purpose(s) for which the scheme has been established;
- assess whether it is necessary to carry out constant real-time recording, or only at certain times when suspect activity usually occurs or is likely to occur;
- cameras should be properly maintained and serviced, and maintenance logs kept;
- protect cameras from vandalism so that they are kept in working order; and
- in the event that cameras break down or are damaged, there should be clear responsibility for getting them repaired and working within a specific time period.

8. DATA / IMAGE RETENTION

Images and recording logs must be retained and disposed of in accordance with our Retention and Disposal Policy.

For digital recording systems, CCTV images held on the hard drive of a PC or server will be overwritten on a recycling basis once the drive is full, and in any event, will not be held for more than 30 days, without prior authorisation by the DPC for reasons which are recorded and notified to the DPC. Where a request is received, you should ensure steps are taken to safeguard any footage which may otherwise be deleted. Images stored on removable media such as CDs / data sticks / external hard drives will be erased or destroyed once the purpose of the recording is no longer relevant unless it is required to be retained for legal / compliance reasons in accordance with our Retention and Disposal Policy.

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.

All digital recordings will be security sealed and placed in a safe or access-controlled location e.g., server room. Recording media no longer in use will be securely destroyed. If images are used for any disciplinary purpose or other legal reason, the footage should be retained securely in the relevant case file.

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. ACCESS TO IMAGES

9.1 Staff images

Staff images will only be accessed if an event occurs that we cannot be expected to ignore, such as criminal activity, fraud, gross misconduct, or behaviour that puts others at risk.

Access to recorded images will be restricted to requests from the DPC / authorised CCTV controllers at each site / plant managers (or above) or equivalent level and restricted to their own locations and will not be made more widely available. The request, date, time, and the reason for authorisation for release of images and CCTV footage will have to be recorded by authorised CCTV controllers at each site, using the correct documentation for audit purposes.

After approving such requests, the DPC / authorised CCTV controllers at each site / plant managers or above will make the necessary access arrangements.

Where possible, viewing of recorded images should always take place in a restricted or secure area to which other members of staff will not have access while viewing is occurring. If media on which images are recorded are removed for viewing purposes, this should be documented, and a record should be kept. Images retained for evidence should be securely stored with limited access for authorised staff only.

The following information must be documented when media are removed for viewing:

- the date and time they were removed;
- the name of the person removing the media;
- the name(s) of the person(s) viewing the images;
- the name of the department to which the person viewing the images belongs to, or the person's organisation if they are from an outside organisation (e.g., Police);
- the reason for viewing the images; and
- the date and time the media were returned to the system or secure storage (if applicable).

This information will be logged on the CCTV Register.

9.2 Police requests

If a police officer requests images from our CCTV system in relation to an investigation that has not been initially reported by the business, then please refer them to the DPC. It may be that we are required to disclose the images, or we have a discretion to do so.

This information will be logged on the CCTV Register.

9.2.1 Access

Access to and disclosure of images recorded on CCTV will be restricted and carefully controlled. This will ensure that the rights of individuals are protected and ensure that the images can be used as evidence if required.

Images may only be disclosed in accordance with the purposes for which they were originally collected.

Our Data Privacy Policy should also be consulted in relation to the capture, storage, access to and disposal of personal data - in this case images of an identifiable individual.

9.2.2 Disclosure

Disclosures to third parties will only be made in accordance with the purpose(s) for which the system is used and will be limited to:

- police and other law enforcement agencies, where the images recorded could assist in a specific criminal enquiry and / or the prevention of terrorism and disorder;
- prosecution agencies (such as the Crown Prosecution Service).
- relevant legal representatives of people whose images have been recorded and retained (unless disclosure to the individual would prejudice criminal enquiries or criminal proceedings).
- individuals who have been caught on our CCTV in accordance with a request made such as one described at section 9 below
- in exceptional cases, for others (such as insurers) to assist in identification of a victim, witness, or perpetrator in relation to a criminal incident; and
- staff involved with our disciplinary processes.

Executive board members are the only persons who can authorise disclosure of information to the police or other law enforcement agencies.

All requests for disclosure should be documented for audit purposes. If disclosure is denied, the reason should also be recorded in the CCTV Register.

In addition to the information documented when gaining access to the images, the following should be documented if any images are disclosed:

- if the images are being removed from the CCTV system or secure storage to another area - the location to which they are being transferred;
- any crime incident number, if applicable; and
- the signature of the person to whom the images have been transferred.

10. SUBJECT ACCESS RIGHTS (ACCESS TO INDIVIDUALS' OWN IMAGE / FOOTAGE)

The GDPR gives individuals the right to access personal data about themselves, including CCTV images and footage.

All requests for access to images by individuals (when they are asking for access to images of themselves) should be addressed to the DPC in a written format such as email or letter:

Please refer to our Data Subject Rights Policy for further details.

10.1 Subject access requests for images / footage

Requests for access to CCTV images/footage must be made in writing and must include:

- the full name and address of the person making the request (the "data subject");
- a personal description of the data subject and / or details of what they were wearing to ensure we can locate the individual, and only relevant images are disclosed;
- the approximate date and time when the images were recorded to allow for searching;
- the location where the images were recorded; and We cannot charge for a subject access request unless it meets one of the exceptions set out in our Data Subject Rights Policy.

Requests from an individual for CCTV images or footage must be handled, and responded to, in accordance with our Data Subject Rights Policy.

Staff responsible for CCTV systems will record and respond to such requests and where the request itself is made by a member of staff, the DPC will ensure that HR is involved to an appropriate level.

If we cannot comply with the request, the reasons for not being able to comply must be documented. The data subject will be advised of these in writing.

Particular care should be exercised when images / footage of other people is included in the scope of footage for disclosure – their images / footage should be redacted / obscured unless there is an expectation that their images / footage would be released in such circumstances. Protection (i.e., non-disclosure) is appropriate in most circumstances.

If there is any doubt about what information must be provided to enquirers, please contact the DPC.

10.2 Request to prevent processing

An individual has the right to request a prevention of processing where this is likely to cause substantial and unwarranted damage or distress to that or another individual. All such requests should be addressed in the first instance to the DPC, who will provide a written response within 1 month of receiving the request, setting out their decision on the request. A copy of the request and response will be retained for an appropriate period deemed reasonable by us on a case-by-case basis

11. RESPONSIBILITY FOR CCTV SYSTEMS – STAFF TRAINING

The DPC will nominate suitable and qualified managers or senior members of each site with the day-to-day responsibility of the systems and the training of staff responsible for operating or administering CCTV. However, for systems operated by us, the overall responsibility lies with the DPC.

The assigned managers responsible for the CCTV system will liaise with the DPC to determine whether disclosure of the images will reveal third-party information.

If a member of staff believes that there has been a breach of the GDPR or any CCTV laws, they must contact either the DPC or their line manager as a matter of urgency.

12. COMPLAINTS

Complaints and enquiries about the operation of our CCTV systems should be made in line with our Grievance Procedure.

Enquiries relating to the GDPR, or CCTV Laws should be addressed to the DPC at privacy@floplast.co.uk.

If a complainant or enquirer is not satisfied with the response received, they should write to the ICO, details of how to do so can be found on their website: www.ico.org.uk. It is our obligation to ensure that this line of appeal is notified both in relevant privacy policies and when responding to issues or complaints.

13. ENFORCEMENT AND COMPLIANCE

All authorised users of our surveillance technology and its underlying data are required to adhere to strict controls around the use of CCTV, and failure to use the CCTV system for any other purposes other than those specifically indicated will be subject to a full investigation and could lead to disciplinary action up to and including dismissal without notice.

The misuse of our surveillance systems and unauthorised use of images and CCTV footage may constitute a criminal offence. Thus, concerns regarding the use of CCTV should either be shared in trust with a line manager or in accordance with our Whistleblowing Policy if a member of staff is not comfortable with escalating concerns via their line manager.