Background:

1.1 **KEL – TECH ENGINEERING (WATERFORD) LIMITED ["the Company"]** uses closed circuit television **["CCTV"]** images for various purposes as part of the operation of its business. Those purposes include, but are not limited to, the monitoring of its premises, the prevention, identification and reduction of crime and unauthorised conduct, the provision of a safe and secure environment for employees, customers and visitors, the implementation of its Health & Safety at Work Policy (and all other Company policies), the enforcement of the provisions of the Contracts of Employment of its employees, the monitoring of their performance in discharge of their duties thereunder and to prevent the loss or damage to Company property.

1.2 CCTV surveillance at the Company premises is intended for the purposes of set out above.

1.3 The system comprises of 49 fixed cameras.

1.4 The CCTV system is owned and operated by the Company and its development and operation will be determined from time to time by its Directors.

1.5 The CCTV is monitored centrally from the premises of the Company by approved personnel (and is also on a central computer maintained at its said premises.

1.6 This policy outlines the use by the Company of CCTV and how it complies with all applicable and relevant legislation.

1.7 All authorised 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. All employees are aware of the restrictions in relation to access to, and disclosure of, recorded images.

1.8 The Company operates this policy so as to ensure that it complies with all relevant legislation and further to ensure that it is used responsibly and safeguards both trust and confidence in its continued use.

1.8 The use of the CCTV system will be conducted in a professional, ethical and legal manner and any diversion of the use of CCTV security technologies for other purposes is prohibited by this policy.

1.10 CCTV monitoring of public areas for security purposes will be conducted in a manner consistent with all existing policies adopted by the Company including its employee Contracts of Employment, its Dignity at Work Policy, Codes of Practice for dealing with complaints of Bullying & Harassment and Sexual Harassment and other relevant policies, including the provisions set down in equality and workplace legislation.

Justification for Use of CCTV:

2.1 The use of CCTV for the purposes set out herein has reasonably been deemed to be justified by the Directors of the Company.

Data Protection Impact Assessments:

3.1 Where new CCTV systems or cameras are to be installed, the Company will carry out a full Data Protection Impact Assessment identifying risks related to the installation and ensuring full compliance with data protection legislation. This may involve the need for consultation with staff but the Company is not obliged to do so.

3.2 Where existing CCTV systems are in operation as of the date hereof the Company will endeavour (but shall not be obliged) to carry out a full Data Protection Impact Assessment on any upgrade or replacement of the system or within a 3 year period from the date of the implementation of General Data Protection Regulations **["GDPR"]**, whichever is sooner.

Location of Cameras:

4.1 Cameras will be sited so they only capture images relevant to the purposes for which they are installed and care will be taken to ensure that reasonable privacy expectations are not violated.

4.2 The Company will ensure that the location of equipment is carefully considered to ensure that images captured comply with GDPR. The Company will make every effort to position cameras so that their coverage is restricted to its property and premises (including the factory floor of its premises) but this may include outdoor areas.

4.3 Use of CCTV to monitor areas where individuals would have a reasonable expectation of privacy would be difficult to justify. The Company, accordingly, has endeavoured to select locations for the installation of CCTV cameras which are least intrusive to protect the privacy of individuals.

4.4 Cameras placed so as to record external areas are positioned in such a way as to prevent or minimise recording of passers-by or of another person's private property.

4.5 CCTV Video Monitoring and Recording of Public Areas may include the following: • Protection of Company buildings and property: The building's perimeter, entrances and exits, lobbies and corridors, special storage areas, office locations, receiving areas for goods/services • Monitoring of Access Control Systems: Monitor and record restricted access areas at entrances to buildings and other areas • Verification of Security Alarms: Intrusion alarms, exit door controls, external alarms • Criminal Investigations (carried out by police): Robbery, burglary and theft surveillance

Covert Surveillance:

5.1 The Company will not engage in covert surveillance save in exceptional circumstances as may be reasonably determined from time to time by its Directors.

Notification:

6.1 A copy of this CCTV Policy will be provided on request to staff and visitors to the Company premises and will be made available on the Company website.

6.2 The location of CCTV cameras will also be indicated and adequate signage will be placed at each location in which a CCTV camera(s) is sited to indicate that CCTV is in operation.

6.3 Adequate signage will also be prominently displayed at the entrance to the Company premises. Signage shall include the name and contact details of the data controller as well as the specific purpose(s) for which the CCTV camera is in place in each location. Appropriate locations for signage will include: • at entrances to premises i.e. external doors, • reception area • at or close to each internal camera and the factory floor remises themselves.

Storage and Retention:

7.1 The images captured by the CCTV system will be retained for a maximum of 90 days, except where the image identifies an issue and is retained specifically in the context of an investigation/prosecution of that issue in which it shall be held and maintained pending the determination of same.

7.2 The images/recordings will be stored in a secure environment with a log of access kept.

7.3 Access will be restricted to authorised personnel. Supervising the access and maintenance of the CCTV System is the responsibility of Declan Walsh or such other person or person as the Company may nominate from time to time. This function may be delegated from time to time to another member of the management team of the Company.

7.4 In certain circumstances, the recordings may also be viewed by other individuals in order to achieve the objectives set out above. When CCTV recordings are being viewed, access will be limited to authorised individuals on a need-to-know basis.

7.5 Files/Tapes/DVDs will be stored in a secure environment with a log of access to tapes kept. Access will be restricted to authorised personnel. Similar measures will be employed when using disk storage, with automatic logs of access to the images created.

Access:

8.1 Recorded footage and the monitoring equipment will be securely stored in a restricted area. Unauthorised access to that area will not be permitted at any time. The area will be locked when not occupied by authorised personnel. A log of access to footage will be maintained.

8.2 Access to the CCTV system and stored images will be restricted to authorised personnel only.

8.3 When accessing images two authorised members of staff must be present. A written record of access will be made. Records of access will be kept.

8.4 A record of the date of any disclosure request along with details of who the information has been provided to (the name of the person and the organisation they represent), why they required it and how the request was dealt with will be made and kept, in case of challenge.

8.5 Data will be provided to those requests authorised in a permanent format where possible. If this is not possible the data subject will be offered the opportunity to view the footage.

8.6 In relevant circumstances, CCTV footage may be accessed: (i) An Garda Siochana, where the Company (or its agents) are required by law to make a report regarding the commission of a suspected crime; or (ii) Following a request by the An Garda Siochana when a crime or suspected crime has taken place and/or when it is suspected that illegal/anti-social behaviour is taking place on the premises of the Company or (iii) To the HSE and/or any other statutory body charged with any statutory function; or (iv) To assist the management of the Company in establishing any alleged breach (by any person) of any Company policy or Contract of Employment; or (v) To data subjects (or their legal representatives), pursuant to a Subject Access Request or (vi) To individuals (or their legal representatives) subject to a court order and (vii) To the Company insurers where the insurance company reasonably requires same.

Subject Access Requests (SAR):

9.1 Individuals have the right to request access to CCTV footage relating to themselves under GDPR.

9.2 Individuals submitting requests for access will be asked to provide sufficient information to enable the footage relating to them to be identified. For example, date, time and location.

9.3 The Company will respond to requests within 30 calendar days of receiving the request.

9.4 The Company reserves the right to refuse access to CCTV footage where this would prejudice the legal rights of other individuals or jeopardise an on-going investigation.

9.5 A record of the date of the disclosure along with details of who the information has been provided to (the name of the person and the organisation they represent) and why they required it will be made.

9.6 In giving a person a copy of their data, the Company will provide a still/series of still pictures, a tape or a disk with relevant images. However, other images of other individuals will be obscured before the data is released.

9.7 Where footage contains images relating to 3rd parties, the Company will take appropriate steps to mask and protect the identities of those individuals.

Complaints:

10.1 Complaints and enquiries about the operation of CCTV within the Company should be directed to Declan Walsh in the first instance.

Staff Training:

11.1 Staff authorised to access the CCTV system will be trained to comply with this policy. Staff will understand that all information relating to the CCTV images must be handled securely.

11.2 Staff will receive appropriate training to enable them to identify and handle different requests according to regulations.

11.3 Staff misuse of surveillance system information will lead to disciplinary proceedings.

Responsibilities:

12.1 Declan Walsh (or nominated deputy) will: • Ensure that the use of CCTV systems is implemented in accordance with the policy set down by the Company • Oversee and co-ordinate the use of CCTV monitoring for safety and security purposes within the Company •

Ensure that all existing CCTV monitoring systems will be evaluated for compliance with this policy • Ensure that the CCTV monitoring at the Company is consistent with the highest standards and protections • Review camera locations and be responsible for the release of any information or recorded CCTV materials stored in compliance with this policy • Maintain a record of access (e.g. an access log) to or the release of tapes or any material recorded or stored in the system • Ensure that the perimeter of view from fixed location cameras conforms to this policy both internally and externally • Give consideration to employees and visitors to the premises of the Company feedback/complaints regarding possible invasion of privacy or confidentiality due to the location of a particular CCTV camera or associated equipment • Ensure that all areas being monitored are not in breach of an enhanced expectation of the privacy of individuals within the premises of the Company and be mindful that no such infringement is likely to take place • Co-operate with the Health & Safety Officer of the Company in reporting on the CCTV system in operation at the premises of the Company • Ensure that external cameras are non-intrusive in terms of their positions and views of neighbouring residential housing and comply with the principle of "Reasonable Expectation of Privacy" • Ensure that monitoring footage are stored in a secure place with access by authorised personnel only • Ensure that images recorded on tapes/DVDs/digital recordings are stored for a period not longer than 90 days and are then erased unless required as part of a criminal investigation or court proceedings (criminal or civil). • Ensure that when a zoom facility on a camera is being used, there is a second person present with the operator of the camera to guarantee that there is no unwarranted invasion of privacy • Ensure that camera control is solely to monitor suspicious behaviour, criminal damage etc accepting that this may include monitoring individual performance • Ensure that camera control is not infringing an individual's reasonable expectation of privacy in public areas.

DATED THIS 27th DAY OF FEBRUARY 2020

BY ORDER OF THE MANAGEMENT OF THE COMPANY