MJP ELECTRICAL GROUP LTD
www.mjpelectricalgroup.com

GDPR POLICY

Policy Aim

This policy sets out the obligations of the company regarding data protection and the rights of data subjects in respect of their personal data under Data Protection Law (all legislation and regulations in force from time to time regulating the use of personal data and the privacy of electronic communications including, but not limited to:

• EU Regulation 2016/679 General Data Protection Regulation ("GDPR")
• The Data Protection Act 2018
• And any successor legislation or other directly applicable EU regulation relating to data protection and privacy for as long as, and to the extent that, EU law has legal effect in the UK).

This Policy sets out the Company's obligations regarding to the:

• Collection
• Processing
• Transfer
• Storage
• Disposal of personal data

The procedures and principles set out herein must be followed at all times by the Company, its employees, agents, contractors, or other parties working on behalf of the Company.

Scope

MJP Electrical Group LTD is committed not only to the letter of the law, but also to the spirit of the law and places high importance on the correct, lawful, and fair handling of all personal data, respecting the legal rights, privacy, and trust of all individuals with whom it deals. The company is responsible for administering this Policy and for developing and implementing any applicable related policies, procedures, and/or guidelines. All management are responsible for ensuring that all employees, agents, contractors, or other parties working on behalf of the company comply with this policy and, where applicable, must implement such practices, processes, controls, and training as are reasonably necessary to ensure such compliance. Any questions relating to this Policy or to Data Protection Law should be referred to senior management. They should always be consulted in the following cases:

• If there is any uncertainty relating to the lawful basis on which personal data is to be collected, held, and/or processed.
• If consent is being relied upon to collect, hold, and/or process personal data.
• If there is any uncertainty relating to the retention period for any type(s) of personal data.
• If any new or amended privacy notices or similar privacy-related documentation are required.
• If any assistance is required in dealing with the exercise of a data subject's rights (including, but not limited to,

the handling of subject access requests)
• If a personal data breach (suspected or actual) has occurred.
• If there is any uncertainty relating to security measures (whether technical or organisational) required to protect personal data.
• If personal data is to be shared with third parties (whether such third parties are acting as data controllers or data processors)
• If personal data is to be transferred outside of the EEA and there are questions relating to the legal basis on which to do so
• When any significant new processing activity is to be carried out, or significant changes are to be made to existing processing activities, which will require a Data Protection Impact Assessment
• When personal data is to be used for purposes different to those for which it was originally collected
• If any automated processing, including profiling or automated decision-making, is to be carried out; or
• If any assistance is required in complying with the law applicable to direct marketing.

The Data Protection Principles

This Policy aims to ensure compliance with Data Protection Law. The GDPR sets out the following principles with which any party handling personal data must comply. Data controllers are responsible for, and must be able to demonstrate, such compliance.

All personal data must be:

Processed lawfully, fairly, and in a transparent manner in relation to the data subject collected for specified, explicit, and legitimate purposes and not further processed in a manner that is incompatible with those purposes. Further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be considered to be incompatible with the initial purposes; adequate, relevant, and limited to what is necessary in relation to the purposes for which it is processed; accurate and, where necessary, kept up to date. Every reasonable step must be taken to ensure that personal data that is inaccurate, having regard to the purposes for which it is processed, is erased, or rectified without delay; kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data is processed. Personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes, or statistical purposes, subject to implementation of the appropriate technical and organisational measures required by the GDPR in order to safeguard the rights and freedoms of the data subject; processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction, or damage, using appropriate technical or organisational measures.

The Rights of Data Subjects

The GDPR sets out the following key rights applicable to data subjects:
• The right to be informed;
• The right of access
• The right to rectification
• The right to erasure (also known as the 'right to be forgotten')
The right to restrict processing
The right to data portability
The right to object; and Rights with respect to automated decision-making and profiling.

Lawful, Fair, and Transparent Data Processing

Data Protection Law seeks to ensure that personal data is processed lawfully, fairly, and transparently, without adversely affecting the rights of the data subject. Specifically, the GDPR states that processing of personal data shall be lawful if at least one of the following applies:
• The data subject has given consent to the processing of their personal data for one or more specific purposes
• The processing is necessary for the performance of a contract to which the data subject is a party, or to take steps at the request of the data subject prior to entering into a contract
• The processing is necessary for compliance with a legal obligation to which the data controller is subject
• The processing is necessary to protect the vital interests of the data subject or of another natural person
• The processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the data controller; or
• The processing is necessary for the purposes of the legitimate interests pursued by the data controller or by a third party, except where such interests are overridden by the fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child.
If the personal data in question is special category personal data at least one of the following conditions must be met:
• The data subject has given their explicit consent to the processing of such data for one or more specified purposes (unless EU or EU Member State law prohibits them from doing so)
• The processing is necessary for the purpose of carrying out the obligations and exercising specific rights of the data controller or of the data subject in the field of employment, social security, and social protection law (insofar as it is authorised by EU or EU Member State law or a collective agreement pursuant to EU Member State law which provides for appropriate safeguards for the fundamental rights and interests of the data subject);
• The processing is necessary to protect the vital interests of the data subject or of another natural person where the data subject is physically or legally incapable of giving consent

• The data controller is a foundation, association, or other non-profit body with a political, philosophical, religious,

or trade union aim, and the processing is carried out in the course of its legitimate activities, provided that the processing relates solely to the members or former members of that body or to persons who have regular contact with it in connection with its purposes and that the personal data is not disclosed outside the body without the consent of the data subjects;
• The processing relates to personal data which is manifestly made public by the data subject
• The processing is necessary for the conduct of legal claims or whenever courts are acting in their judicial capacity
• The processing is necessary for substantial public interest reasons, on the basis of EU or EU Member State law which shall be proportionate to the aim pursued, shall respect the essence of the right to data protection, and shall provide for suitable and specific measures to safeguard the fundamental rights and interests of the data subject;
• The processing is necessary for the purposes of preventative or occupational medicine, for the assessment of the working capacity of an employee, for medical diagnosis, for the provision of health or social care or treatment, or the management of health or social care systems or services on the basis of EU or EU Member State law or pursuant to a contract with a health professional, subject to the conditions and safeguards referred to in Article 9(3) of the GDPR;
• The processing is necessary for public interest reasons in the area of public health, for example, protecting against serious cross-border threats to health or ensuring high standards of quality and safety of health care and of medicinal products or medical devices, on the basis of EU or EU Member State law which provides for suitable and specific measures to safeguard the rights and freedoms of the data subject (in particular, professional secrecy); or • The processing is necessary for archiving purposes in the public interest, scientific or historical research purposes, or statistical purposes in accordance with Article 89(1) of the GDPR based on EU or EU Member State law which shall be proportionate to the aim pursued, respect the essence of the right to data protection, and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject.

Consent

If consent is relied upon as the lawful basis for collecting, holding, and/or processing personal data, the following shall apply:
• Consent is a clear indication by the data subject that they agree to the processing of their personal data. Such a clear indication may take the form of a statement or a positive action. Silence, pre-ticked boxes, or inactivity are unlikely to amount to consent.
• Where consent is given in a document which includes other matters, the section dealing with consent must be kept clearly separate from such other matters.
• Data subjects are free to withdraw consent at any time and it must be made easy for them to do so. If a data subject withdraws consent, their request must be honoured promptly.

• If personal data is to be processed for a different purpose that is incompatible with the purpose or purposes for which that personal data was originally collected that was not disclosed to the data subject when they first

provided their consent, consent to the new purpose or purposes may need to be obtained from the data subject.
• If special category personal data is processed, the Company shall normally rely on a lawful basis other than explicit consent. If explicit consent is relied upon, the data subject in question must be issued with a suitable privacy notice to capture their consent.
• In all cases where consent is relied upon as the lawful basis for collecting, holding, and/or processing personal data, records must be kept of all consents obtained in order to ensure that the Company can demonstrate its compliance with consent requirements.

Specified, Explicit, and Legitimate Purposes

The Company collects and processes the personal data set out in this Policy. This includes:
• personal data collected directly from data subjects
The Company only collects, processes, and holds personal data for the specific purposes set out in this Policy (or for other purposes expressly permitted by the GDPR). Data subjects must be kept informed always of the purpose or purposes for which the Company uses their personal data.

Adequate, Relevant, and Limited Data Processing

The Company will only collect and process personal data for and to the extent necessary for the specific purpose or purposes of which data subjects have been informed (or will be informed). Employees, agents, contractors, or other parties working on behalf of the Company may collect personal data only to the extent required for the performance of their job duties and only in accordance with this Policy. Excessive personal data must not be collected. Employees, agents, contractors, or other parties working on behalf of the Company may process personal data only when the performance of their job duties requires it. Personal data held by the Company cannot be processed for any unrelated reasons.

Accuracy of Data and Keeping Data Up to Date

The Company shall ensure that all personal data collected, processed, and held by it is kept accurate and up to date. The accuracy of personal data shall be checked when it is collected and at regular intervals thereafter. If any personal data is found to be inaccurate or out-of-date, all reasonable steps will be taken without delay to amend or erase that data, as appropriate.

Data Retention

The Company shall not keep personal data for any longer than is necessary considering the purpose or purposes

for which that personal data was originally collected, held, and processed. When personal data is no longer required, all reasonable steps will be taken to erase or otherwise dispose of it without delay.

Secure Processing

The Company shall ensure that all personal data collected, held, and processed is kept secure and protected against unauthorised or unlawful processing and against accidental loss, destruction, or damage. All technical and organisational measures taken to protect personal data shall be regularly reviewed and evaluated to ensure their ongoing effectiveness and the continued security of personal data. Data security must always be maintained by protecting the confidentiality, integrity, and availability of all personal data as follows:

• Only those with a genuine need to access and use personal data and who are authorised to do so may access and use it

• Personal data must be accurate and suitable for the purpose or purposes for which it is collected, held, and processed; and

• Authorised users must always be able to access the personal data as required for the authorised purpose or purposes.

Accountability and Record-Keeping

The Data Protection Officer is responsible for administering this Policy and for developing and implementing any applicable related policies, procedures, and/or guidelines. The Company shall always follow a privacy by design approach when collecting, holding, and processing personal data. Data Protection Impact Assessments shall be conducted if any processing presents a significant risk to the rights and freedoms of data subjects. All employees, agents, contractors, or other parties working on behalf of the Company shall be given appropriate training in data protection and privacy, addressing the relevant aspects of Data Protection Law, this Policy, and all other applicable Company policies.

The Company's data protection compliance shall be regularly reviewed and evaluated. The Company shall keep internal records of all personal data collection, holding, and processing, which shall incorporate the following information:

• The name and details of the Company, its Data Protection Officer, and any applicable third-party data transfers (including data processors and other data controllers with whom personal data is shared)

• The purposes for which the Company collects, holds, and processes personal data

• The Company's legal basis or bases (including, but not limited to, consent, the mechanism(s) for obtaining such consent, and records of such consent) for collecting, holding, and processing personal data

• Details of the categories of personal data collected, held, and processed by the Company, and the categories of data subject to which that personal data relates

• Details of any transfers of personal data to non-EEA countries including all mechanisms and security safeguards

• Details of how long personal data will be retained by the Company (please refer to the Company's Data

Retention Policy)
• Details of personal data storage, including location(s)
• Detailed descriptions of all technical and organisational measures taken by the Company to ensure the security of personal data.

Data Subject Access

Data subjects may make subject access requests ("SARs") at any time to find out more about the personal data which the Company holds about them, what it is doing with that personal data, and why. Employees wishing to make a SAR should do using a Request Form, sending the form to the Company's Data Protection Officer Responses to SARs must normally be made within one month of receipt, however, this may be extended by up to two months if the SAR is complex and/or numerous requests are made. If such additional time is required, the data subject shall be informed. All SARs received shall be handled by the Company's Data Protection Officer. The Company does not charge a fee for the handling of normal SARs. The Company reserves the right to charge reasonable fees for additional copies of information that has already been supplied to a data subject, and for requests that are manifestly unfounded or excessive, particularly where such requests are repetitive.

Rectification of Personal Data

Data subjects have the right to require the Company to rectify any of their personal data that is inaccurate or incomplete. The Company shall rectify the personal data in question, and inform the data subject of that rectification, within one month of the data subject informing the Company of the issue. The period can be extended by up to two months in the case of complex requests. If such additional time is required, the data subject shall be informed.
If any affected personal data has been disclosed to third parties, those parties shall be informed of any rectification that must be made to that personal data.

Erasure of Personal Data

Data subjects have the right to request that the Company erases the personal data it holds about them in the following circumstances:
• It is no longer necessary for the Company to hold that personal data with respect to the purpose(s) for which it was originally collected or processed.
• The data subject wishes to withdraw their consent to the Company holding and processing their personal data.
• The data subject objects to the Company holding and processing their personal data (and there is no overriding legitimate interest to allow the Company to continue doing so)
• The personal data has been processed unlawfully.
• The personal data needs to be erased for the Company to comply with a legal obligation

Unless the Company has reasonable grounds to refuse to erase personal data, all requests for erasure shall be complied with, and the data subject informed of the erasure, within one month of receipt of the data subject's request. The period can be extended by up to two months in the case of complex requests. If such additional time is required, the data subject shall be informed. In the event that any personal data that is to be erased in response to a data subject's request has been disclosed to third parties, those parties shall be informed of the erasure (unless it is impossible or would require disproportionate effort to do so).

Personal Data Collected, Held, and Processed

The following personal data is collected, held, and processed by the Company (for details of data retention, please refer to the Company's Data Retention Policy):
• Name
• Address
• Telephone number
• Email address
• Other data collected that could directly or indirectly identify you
Data Security - Transferring Personal Data and Communications
The Company shall ensure that the following measures are taken with respect to all communications and other transfers involving personal data:
• All emails containing personal data must be encrypted
• All emails containing personal data must be marked "confidential"
• Personal data may be transmitted over secure networks only; transmission over unsecured networks is not permitted in any circumstances.
• Personal data may not be transmitted over a wireless network if there is a wired alternative that is reasonably practicable.
• Personal data contained in the body of an email, whether sent or received, should be copied from the body of that email, and stored securely. The email itself should be deleted. All temporary files associated therewith should also be deleted.
• Where personal data is to be sent by facsimile transmission the recipient should be informed in advance of the transmission and should be waiting by the fax machine to receive the data.
• Where personal data is to be transferred in hardcopy form it should be passed directly to the recipient
• All personal data to be transferred physically, whether in hardcopy form or on removable electronic media shall be transferred in a suitable container marked "confidential"

Data Security - Storage

The Company shall ensure that the following measures are taken with respect to the storage of personal data:
• All electronic copies of personal data should be stored securely using passwords and data encryption.
• All hardcopies of personal data, along with any electronic copies stored on physical, removable media should be stored securely in a locked box, drawer, cabinet, or similar.

• All personal data stored electronically should be backed up with backups stored onsite. All backups should be encrypted
• No personal data should be stored on any mobile device (including, but not limited to, laptops, tablets, and smartphones), whether such device belongs to the Company or otherwise
• No personal data should be transferred to any device personally belonging to an employee, agent, contractor, or other party working on behalf of the Company and personal data may only be transferred to devices belonging to agents, contractors, or other parties working on behalf of the Company where the party in question has agreed to comply fully with the letter and spirit of this Policy and of the GDPR (which may include demonstrating to the Company that all suitable technical and organisational measures have been taken);

Data Security - Disposal

When any personal data is to be erased or otherwise disposed of for any reason (including where copies have been made and are no longer needed), it should be securely deleted and disposed of. For further information on the deletion and disposal of personal data.

Data Security - Use of Personal Data

The Company shall ensure that the following measures are taken with respect to the use of personal data:
• No personal data may be shared informally and if an employee, agent, contractor, or other party working on behalf of the Company requires access to any personal data that they do not already have access to, such access should be formally requested
• No personal data may be transferred to any employee, agent, contractor, or other party, whether such parties are working on behalf of the Company or not, without authorisation
• Personal data must always be handled with care and should not be left unattended or on view to unauthorised employees, agents, contractors, or other parties at any time.
• If personal data is being viewed on a computer screen and the computer in question is to be left unattended for any period, the user must lock the computer and screen before leaving it.
• Where personal data held by the Company is used for marketing purposes, it shall be the responsibility to ensure that the appropriate consent is obtained and that no data subjects have opted out, whether directly or via a third-party service such as the TPS;

Data Security - IT Security
The Company shall ensure that the following measures are taken with respect to IT and information security:
• All passwords used to protect personal data should be changed regularly and should not use words or phrases that can be easily guessed or otherwise compromised. All passwords must contain a combination of uppercase and lowercase letters, numbers, and symbols.
• Under no circumstances should any passwords be written down or shared between any employees, agents, contractors, or other parties working on behalf of the Company, irrespective of seniority or department. If a

password is forgotten, it must be reset using the applicable method. IT staff do not have access to passwords.
• All software (including, but not limited to, applications and operating systems) shall be kept up to date. The Company's IT staff shall be responsible for installing all security-related updates as soon as reasonably and practically possible unless there are valid technical reasons not to do so
• No software may be installed on any Company-owned computer or device without the prior approval of the

Organisational Measures

The Company shall ensure that the following measures are taken with respect to the collection, holding, and processing of personal data:
• All employees, agents, contractors, or other parties working on behalf of the Company shall be made fully aware of both their individual responsibilities and the Company's responsibilities under Data Protection Law and under this Policy, and shall be provided with a copy of this Policy;
• Only employees, agents, contractors, or other parties working on behalf of the Company that need access to, and use of, personal data in order to carry out their assigned duties correctly shall have access to personal data held by the Company;
• All sharing of personal data shall comply with the information provided to the relevant data subjects and, if required, the consent of such data subjects shall be obtained prior to the sharing of their personal data.
• All employees, agents, contractors, or other parties working on behalf of the Company handling personal data will be appropriately trained to do so.
• All employees, agents, contractors, or other parties working on behalf of the Company handling personal data will be appropriately supervised.
• All employees, agents, contractors, or other parties working on behalf of the Company handling personal data shall be required and encouraged to exercise care, caution, and discretion when discussing work-related matters that relate to personal data, whether in the workplace or otherwise;
• Methods of collecting, holding, and processing personal data shall be regularly evaluated and reviewed.
• All personal data held by the Company shall be reviewed periodically.
• The performance of those employees, agents, contractors, or other parties working on behalf of the Company handling personal data shall be regularly evaluated and reviewed.
• All employees, agents, contractors, or other parties working on behalf of the Company handling personal data will be bound to do so in accordance with the principles of Data Protection Law and this Policy by contract.

• All agents, contractors, or other parties working on behalf of the Company handling personal data must ensure that any and all of their employees who are involved in the processing of personal data are held to the same conditions as those relevant employees of the Company arising out of this Policy and Data Protection Law;
• Where any agent, contractor or other party working on behalf of the Company handling personal data fails in their obligations under this Policy that party shall indemnify and hold harmless the Company against any costs, liability, damages, loss, claims or proceedings which may arise out of that failure;

Data Breach Notification

All personal data breaches must be reported immediately to the Company's Data Protection Officer. If an employee, agent, contractor, or other party working on behalf of the Company becomes aware of or suspects that a personal data breach has occurred, they must not attempt to investigate it themselves. All evidence relating to the personal data breach in question should be carefully retained. If a personal data breach occurs and that breach is likely to result in a risk to the rights and freedoms of data subjects (e.g. financial loss, breach of confidentiality, discrimination, reputational damage, or other significant social or economic damage), the Data Protection Officer must ensure that the Information Commissioner's Office is informed of the breach without delay, and in any event, within 72 hours after having become aware of it. In the event that a personal data breach is likely to result in a high risk to the rights and freedoms of data subjects, the Data Protection Officer must ensure that all affected data subjects are informed of the breach directly and without undue delay. Data breach notifications shall include the following information:

- The categories and approximate number of data subjects concerned.
- The categories and approximate number of personal data records concerned.
- The name and contact details of the Company's data protection officer (or other contact point where more information can be obtained)
- The likely consequences of the breach.
- Details of the measures taken, or proposed to be taken, by the Company to address the breach including, where appropriate, measures to mitigate its possible adverse effects.

Implementation of Policy

This Policy shall be deemed effective immediately. No part of this Policy shall have retroactive effect and shall thus apply only to matters occurring on or after this date.

Signed
Mark Parry

Mark Parry
Managing Director
mjpelectricalgroup.com

MJP
ELECTRICAL GROUP LTD
www.mjpelectricalgroup.com