



GDPR Policy

In the course of our work we will come into contact with or use confidential information about employees, clients, customers and suppliers, for example their names and home addresses. The Data Protection Act 1998 contains principles affecting employees' and other personal records. Information protected by the Act includes not only personal data held on computer but also certain manual records containing personal data, for example employee personnel files that form part of a structured filing system. The purpose of this policy is to ensure South East Solar & Electrical and its representatives do not breach the Act.

South East Solar & Electrical and its representatives are aware that we are personally accountable for our actions and that we can be held criminally liable if we knowingly or recklessly disclose personal data in breach of the Act. A serious breach of data protection is also a disciplinary offence and will be dealt with under the Company's disciplinary procedure. If South East Solar & Electrical or its representatives access another person's personnel records without authority, this constitutes a gross misconduct offence and could lead to disciplinary action being taken.

This policy does not form part of any contract of employment, but it is a condition of employment that representatives of South East Solar & Electrical abide by this policy and therefore any failure to follow it can result in disciplinary proceedings.

The data protection principles

There are eight data protection principles that are central to the Act. South East Solar & Electrical and its representatives shall always comply with these principles in their information-handling practices. In brief, the principles say that personal data must be:

1. Processed fairly and lawfully and must not be processed unless certain conditions are met in relation to personal data and additional conditions are met in relation to sensitive personal data. The conditions are either that the employee has given his consent to the processing, or the processing is necessary for the various purposes set out in the Act. Sensitive personal data may only be processed with the explicit consent of the person and consists of information relating to:
 - Race or ethnic origin.
 - Political opinions and trade union membership.
 - Religious or other beliefs.
 - Physical or mental health or condition.
 - Sexual life.
 - Criminal offences, both committed and alleged.
2. Obtained only for one or more specified and lawful purposes, and must not be processed in any manner incompatible with those purposes.
3. Adequate, relevant and not excessive in relation to the purposes for which it is processed. South East Solar & Electrical will review a person's personnel files on a regular basis to ensure they do not contain a backlog of out-of-date or irrelevant information and to check there is a sound business reason requiring information to continue to be held.
4. Accurate and, where necessary, kept up-to-date. If your personal information changes, for example you change address or you get married and change your surname, you must inform your line manager as soon as practicable so that the Company's records can be updated. The Company cannot be responsible for any such errors unless the employee has notified the Company of the relevant change.
5. Not kept for longer than is necessary. South East Solar & Electrical will keep personnel files for no longer than six years after. Different categories of data will be retained for different periods of time, depending on legal, operational and financial requirements. Any data which the Company decides it does not need to hold for a particular period of time will be destroyed after approximately one year. Data relating to unsuccessful job applicants will only be retained for a period of one year.



GDPR Policy

6. Processed in accordance with the rights of employees under the Act.

7. Secure. Appropriate technical and organisational measures must be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, data. Personnel files are confidential and are stored as such in locked filing cabinets. Only authorised persons have access to these files. For a list of authorised persons, please contact Tom Mitchinson. Files will not be removed from their normal place of storage without good reason. Data stored on memory sticks, discs, portable hard drives or other removable storage media is kept in locked filing cabinets. Data held on computer is also stored confidentially by means of password protection, encryption or coding and again only the above employees have access to that data. The Company has network back-up procedures to ensure that data on computer cannot be accidentally lost or destroyed.

8. Not transferred to a country or territory outside the European Economic Area unless that country or territory ensures adequate level of protection relation to the processing of personal data.

Persons consent to personal information being held

South East Solar & Electrical shall inform any person or its representatives about the type of personal data the Company shall hold. At no time shall South East Solar & Electrical share your personal information or seek your consent to do so.

Rights to access personal information

Under the Act, persons have the right on request to receive a copy of the personal data that the Company holds about them, including personal data held on personnel files that form part of a relevant filing system, and to demand that any inaccurate data held be corrected or removed. They also have the right to seek compensation where damage and distress have been caused to them as a result of any breach of the Act by the Company.

Persons have the right, on request:

- To be told by the Company whether and for what purpose personal data about them is being processed.
- To be given a description of the personal data concerned and the recipients to whom it is or may be disclosed.
- To have communicated in an intelligible form the personal data concerned, and any information available to the Company as to the source of the data.
- To be informed in certain circumstances of the logic involved in computerised decision-making.

Upon request, the Company will provide you with a statement regarding the personal data held about you. This will state all the types of personal data the Company holds and processes about you and the reasons for which they are processed.

If you wish to access a copy of any personal data being held about you, you must make a written request for this and the Company reserves the right to charge you a fee of £10.00 for the supply of the information requested. If you wish to make a request, please complete a Personal Data Request Form, which can be obtained from Tom Mitchinson. Once completed, it should be returned to Tom Mitchinson. The Company will respond promptly and in any case within 40 calendar days of receiving the request. Note that the Company will always check the identity of the person making the request before processing it.

If you wish to make a complaint that this policy has not been followed in respect of personal data the Company holds about you, you should raise the matter with Tom Mitchinson.

Exemptions

There are a number of exemptions from the data protection regime set out in the Act, for example:



GDPR Policy

- Confidential references that are given, but not those received by the Company from third parties. Only designated persons can give Company references. Confidential references will not be provided unless the Company is sure this is the persons wish.
- Management forecasts and management planning (including documents setting out management plans for a person's future development and progress).
- Data which is required by law to be publicly available.
- Documents subject to legal professional privilege.

Representatives and persons obligations in relation to personal information

If, as part of your job duties and responsibilities, you collect personal information about employees or other people such as clients or customers, you must comply with this policy. This includes ensuring the information is processed in accordance with the Act, is only processed for the purposes for which it is held, is kept secure and is not kept for longer than necessary. You must also ensure you comply with the following guidelines at all times:

- Do not give out confidential personal information except to the data subject. In particular, it should not be given to someone, either accidentally or otherwise, from the same family or to any other unauthorised third party unless the data subject has given their explicit prior consent to this.
- Be aware that those seeking information sometimes use deception in order to gain access to it. Always verify the identity of the data subject and the legitimacy of the request, particularly before releasing personal information by telephone.
- Where the Company provides you with code words or passwords to be used before releasing personal information, for example by telephone, you must strictly follow the Company's requirements in this regard.
- Only transmit personal information between locations by fax or e-mail if a secure network is in place, for example, a confidential fax machine or encryption is used for e-mail.
- If you receive a request for personal information about another person, you should forward this to the HSQE Manager, who will be responsible for dealing with such requests.
- Ensure that any personal data which you hold is kept securely, either in a locked filing cabinet or, if it is computerised, it is password protected so that it is protected from unintended destruction or change and is not seen by unauthorised persons.
- Do not access another person's records without authority as this will be treated as gross misconduct and it is a criminal offence.
- Do not write down (in electronic or hard copy form) opinions or facts concerning a data subject which it would be inappropriate to share with that data subject.
- Do not remove personal information from the workplace with the intention of processing it elsewhere unless this is necessary to enable you to carry out your job duties and has been authorised by the HSQE Manager
- Ensure that, when working on personal information as part of your job duties when away from your workplace and with the authorisation of Tom Mitchinson, you continue to observe the terms of this policy and the Act, in particular in matters of data security.
- Ensure that hard copy personal information is disposed of securely, for example cross-shredded.

Compliance with the Act is the responsibility of all persons and representatives of South East Solar & Electrical. Any questions or concerns about the interpretation of this policy should be raised with Tom Mitchinson.

Oliver Lloyd – Managing Director

03/11/2023

Next Review Date (on or by): November 2024 or within Legislation changes