GRANT'S
ELECTRICAL SOLUTIONS

DATA PROTECTION AND UK GDPR POLICY

Corporate Policy Document

Document reference	GES-POL-DP-001
Version	1.0
Classification	Internal. Available to data subjects on request
Policy owner	Shaye Grant, Managing Director
Approved by	Shaye Grant, Managing Director
Effective date	22nd July 2026
Next review	22nd July 2027

DOCUMENT CONTROL

Version History

Version	Date	Description of change	Author
1.0	22nd July 2026	First issue	S. Grant

Approval

Name	Position	Signature and date
Shaye Grant	Managing Director	Shaye Grant 22nd July 2026

Distribution

This policy is issued to all directors, employees, workers and sub-contractors of Grants Electrical Solutions Ltd, forms part of induction, and is available to customers and other data subjects on request.

CONTENTS

GRANT'S
ELECTRICAL SOLUTIONS

1 INTRODUCTION

1.1 Grants Electrical Solutions Ltd (the “Company”) is an electrical contracting business providing domestic, commercial and industrial electrical installation, inspection, testing, certification, EV charging and renewable energy services across Devon, Cornwall and Somerset.

1.2 In the course of the business the Company collects and uses personal data relating to customers, commercial clients, employees, workers, job applicants, suppliers, sub-contractors and website users. The Company is committed to handling all personal data lawfully, securely and transparently.

1.3 The Company is the data controller of the personal data it processes. Company details: Grants Electrical Solutions Ltd, Company No. 16071674, VAT No. 504 327 521, registered office Unit 24 Cavalier Road, Heathfield Industrial Estate, Newton Abbot, Devon, TQ12 6TZ. Telephone 01626 374 059. Email info@grantselectricalsolutions.co.uk. Website www.grantselectricalsolutions.co.uk.

2 PURPOSE

2.1 This policy sets out the standards the Company applies to the processing of personal data in order to comply with the UK General Data Protection Regulation (UK GDPR) and the Data Protection Act 2018 (together “Data Protection Legislation”).

2.2 It defines the responsibilities of the Company and of every person working for it, the rights of the individuals whose data the Company holds, and the procedures for handling requests, breaches and complaints.

3 SCOPE

3.1 This policy applies to all personal data processed by the Company in any format, whether electronic or paper, and on any system or device used for the business.

3.2 It applies to all directors, employees, workers, consultants and sub-contractors of the Company (“staff”), all of whom are required to read and comply with it. Compliance is a condition of employment or engagement.

4 DEFINITIONS

Term	Meaning
Personal data	Any information relating to an identified or identifiable living individual.
Processing	Any operation performed on personal data, including collection, recording, storage, use, disclosure, alteration and deletion.
Data controller	The organisation that determines the purposes and means of processing. The Company is the controller of the data it holds.
Data processor	A third party that processes personal data on the Company's behalf and on its instructions, such as a software provider.
Data subject	The individual to whom personal data relates.

Special category data	Data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, genetic or biometric data, health data, or data concerning sex life or sexual orientation.
Personal data breach	A breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data.
ICO	The Information Commissioner's Office, the UK supervisory authority for data protection.

5 ROLES AND RESPONSIBILITIES

5.1 **Data Protection Lead.** The Managing Director, Shaye Grant, has overall accountability for data protection and acts as the Company's Data Protection Lead. The Data Protection Lead is responsible for:

(a) maintaining, reviewing and enforcing this policy;

(b) responding to requests from data subjects and to correspondence from the ICO;

(c) maintaining the personal data breach log and managing breach response under Appendix B;

(d) approving new systems, processors and data sharing arrangements; and

(e) ensuring staff receive data protection training.

5.2 **All staff.** Every member of staff must:

(a) process personal data only as needed for their role and in accordance with this policy;

(b) keep personal data secure and confidential, and never disclose it to any unauthorised person;

(c) pass any request from an individual about their data to the Data Protection Lead on the day it is received; and

(d) report any actual or suspected personal data breach immediately under Section 17.

6 DATA PROTECTION PRINCIPLES

6.1 The Company processes all personal data in accordance with the principles in Article 5 UK GDPR. Personal data shall be:

(a) processed lawfully, fairly and in a transparent manner (lawfulness, fairness and transparency);

(b) collected for specified, explicit and legitimate purposes and not further processed incompatibly with those purposes (purpose limitation);

(c) adequate, relevant and limited to what is necessary (data minimisation);

(d) accurate and, where necessary, kept up to date (accuracy);

(e) kept in identifiable form no longer than necessary (storage limitation); and

(f) processed with appropriate security (integrity and confidentiality).

6.2 The Company is responsible for, and must be able to demonstrate, compliance with these principles (accountability).

7 PERSONAL DATA PROCESSED BY THE COMPANY

Category of data subject	Personal data processed
Customers and clients	Name, address, telephone, email; property and installation details including photographs, drawings, test results, certificates and reports issued under BS 7671 (EICs, EICRs, Minor Works Certificates); quotations, contracts, invoices and payment records; correspondence; temporary access information such as key safe or alarm codes, held only for the duration of the works.
Employees, workers and applicants	Identity, contact and right to work documentation; employment records, qualifications, training and competency records; payroll, pension, tax and bank details; health information where required for health and safety or statutory purposes (see Section 9).
Suppliers and sub-contractors	Contact details; qualification, registration and insurance records; RAMS; bank and payment records.
Website users and enquirers	Information submitted through contact and quotation forms on www.grantselectricalsolutions.co.uk; technical data such as IP address arising from operation of the website.

8 LAWFUL BASES FOR PROCESSING

8.1 The Company identifies a lawful basis under Article 6 UK GDPR before processing personal data, as follows:

Processing activity	Examples	Lawful basis
Delivery of services	Quoting, carrying out, testing and certifying electrical works and EV charger installations	Contract (Art 6(1)(b))
Certification and statutory notification	Notification of works to building control and registration bodies (NICEIC, NAPIT); OZEV grant administration	Legal obligation (Art 6(1)(c)); legitimate interests (Art 6(1)(f))
Finance, tax and payroll	Invoicing, accounting, VAT returns, PAYE	Legal obligation (Art 6(1)(c))
Employment administration	Recruitment, managing engagement, training, health and safety	Contract; legal obligation
Business administration	Scheduling, records of works, insurance, complaints, debt recovery	Legitimate interests (Art 6(1)(f))
Direct marketing	Service reminders and offers to existing and past customers	Legitimate interests or consent; opt out always available (Section 18)

8.2 Where legitimate interests are relied on, the Company balances its interests against the rights and reasonable expectations of the individual. The Company does not carry out automated decision making or profiling.

9 SPECIAL CATEGORY DATA

9.1 The Company does not seek special category data from customers. Where such data is volunteered, for example a health condition relevant to safe access arrangements, only what is necessary is recorded.

9.2 Health data relating to staff is processed only where necessary to comply with employment, health and safety or social security obligations, in reliance on Article 9(2)(b) UK GDPR, and is held with restricted access. Special category data is never used for marketing.

10 DATA SHARING AND DISCLOSURES

10.1 The Company does not sell personal data. Personal data is disclosed only where necessary, to:

(a) registration and certification bodies (NICEIC and NAPIT) and building control, for notification and certification of works;

(b) scheme and grant administrators applicable to the works, including OZEV, Pod Point and Ohme programmes;

(c) distribution network operators and utility companies where an application or notification concerning the supply is required;

(d) the Company's accountants, payroll provider, insurers, legal advisers and, where necessary, debt recovery agents;

(e) sub-contractors engaged on the relevant works, limited to what they need to carry out those works; and

(f) HMRC, the Health and Safety Executive, the ICO, the courts and other authorities where disclosure is required by law.

10.2 Every disclosure is limited to the minimum personal data necessary for the purpose.

11 DATA PROCESSORS

11.1 The Company uses third party software providers as processors, including its accounting, job management, certification, email and storage systems. Each processor is engaged under terms which require it to process personal data only on the Company's instructions, to keep it secure and confidential, and to assist the Company with its obligations under Data Protection Legislation.

11.2 New processors and systems must be approved by the Data Protection Lead before personal data is placed in them.

12 INTERNATIONAL TRANSFERS

12.1 Personal data is stored in the United Kingdom or, where a provider hosts data outside the UK, only under safeguards recognised by UK GDPR, being an adequacy decision or the International Data Transfer Agreement or Addendum. The Company makes no other transfers of personal data outside the UK.

13 DATA RETENTION

13.1 Personal data is retained only as long as necessary for the purpose for which it was collected, for legal and regulatory requirements, and for the establishment or defence of legal claims. The Company's retention periods are set out in Appendix A.

13.2 At the end of the applicable retention period, personal data is securely deleted, destroyed by shredding, or irreversibly anonymised.

14 DATA SECURITY

14.1 The Company applies technical and organisational measures appropriate to the risk, including:

(a) password protected, access controlled systems, with multi factor authentication enabled where available;

(b) access to personal data restricted to staff who need it for their role;

(c) Company devices secured, kept updated and not shared outside the business;

(d) paper records held securely at the registered office and destroyed by shredding;

(e) contractual confidentiality and data protection obligations on all processors and sub-contractors; and

(f) back up of business systems through the Company's software providers.

15 RIGHTS OF INDIVIDUALS

15.1 Every data subject has the following rights under UK GDPR, each of which the Company gives effect to without charge and within one calendar month of a valid request:

Right	What it means
To be informed	To know how their data is used. This policy and the Company's privacy information deliver this right.
Of access	To obtain a copy of their personal data and supporting information (a subject access request, Section 16).
To rectification	To have inaccurate or incomplete data corrected.
To erasure	To have data deleted where there is no continuing lawful reason to hold it. Data the Company must retain by law, such as issued certificates and accounting records, cannot be erased during the statutory period, and this will be explained in the response.
To restrict processing	To limit how data is used in defined circumstances, for example while accuracy is contested.
To data portability	To receive data they provided in a structured, commonly used, machine readable format where processing is by automated means under contract or consent.
To object	To object to processing based on legitimate interests, and to object absolutely to direct marketing.
Automated decisions	Not to be subject to solely automated decisions with legal or

	similarly significant effects. The Company makes no such decisions.

15.2 Requests may be made to the Data Protection Lead by email to info@grantselectricalsolutions.co.uk, by telephone on 01626 374 059, or in writing to the registered office.

16 SUBJECT ACCESS REQUESTS

16.1 A subject access request may be made in any form and to any member of staff, and need not mention the UK GDPR. Any member of staff who receives one must pass it to the Data Protection Lead on the day of receipt.

16.2 Requests are handled under the procedure in Appendix C. The statutory deadline of one calendar month runs from receipt, extendable by two further months only for complex or numerous requests, with the individual informed within the first month.

16.3 No fee is charged unless the request is manifestly unfounded or excessive, in which case a reasonable fee may be charged or the request refused, with reasons and the right to complain to the ICO explained.

17 PERSONAL DATA BREACH MANAGEMENT

17.1 Any member of staff who becomes aware of an actual or suspected personal data breach must report it to the Data Protection Lead immediately, and in any event within 12 hours of becoming aware.

17.2 Breaches are managed under the procedure in Appendix B. Every breach, however minor, is recorded in the Company's breach log with its facts, effects and remedial action.

17.3 Where a breach is likely to result in a risk to the rights and freedoms of individuals, the Company will notify the ICO without undue delay and within 72 hours of becoming aware. Where the risk is high, the affected individuals will also be informed without undue delay.

18 DIRECT MARKETING

18.1 The Company may send existing and past customers information about its own similar services, including reminders that periodic inspection and testing is due, in reliance on the soft opt in under the Privacy and Electronic Communications Regulations 2003.

18.2 Every marketing communication identifies the Company and contains a simple means to opt out. An opt out is actioned immediately and permanently. The Company does not purchase marketing lists and does not share personal data with third parties for their marketing.

19 WEBSITE AND COOKIES

19.1 Data submitted through forms on www.grantselectricalsolutions.co.uk is used only to respond to the enquiry and provide the Company's services, and is handled in accordance with this policy.

19.2 The website may use cookies and similar technologies for its operation and analytics. Where consent is required it is obtained through the website, and cookie information is published on the site.

20 TRAINING AND AWARENESS

20.1 Data protection forms part of induction for all staff and is refreshed periodically and whenever this policy materially changes. Records of training are retained.

21 NON-COMPLIANCE

21.1 Breach of this policy by an employee is a disciplinary matter which may amount to gross misconduct. Breach by a sub-contractor is a breach of their terms of engagement. Deliberate unauthorised access to or disclosure of personal data may also be a criminal offence under the Data Protection Act 2018.

22 COMPLAINTS AND THE ICO

22.1 Concerns about the Company's handling of personal data should be raised with the Data Protection Lead at info@grantselectricalsolutions.co.uk, and will be investigated and answered in writing.

22.2 Every individual also has the right to complain at any time to the Information Commissioner's Office: ico.org.uk, telephone 0303 123 1113, or Information Commissioner's Office, Wycliffe House, Water Lane, Wilmslow, Cheshire, SK9 5AF.

23 POLICY REVIEW

23.1 This policy is reviewed at least annually by the Data Protection Lead, and additionally on any material change in Data Protection Legislation, the Company's systems, or the business. Changes are recorded in the version history and reissued to all staff.

A APPENDIX A: DATA RETENTION SCHEDULE

Record type	Retention period
Electrical certificates, test results and records of works (EICs, EICRs, Minor Works Certificates)	Minimum 6 years from completion, and for the expected life of the installation where required for future inspection, insurance or conveyancing
Contracts, quotations, invoices and accounting records	6 years from the end of the financial year to which they relate
Warranty and guarantee records	Warranty period plus 12 months
Employment records	Duration of employment plus 6 years; payroll and tax records for the periods required by HMRC
Health and safety records, accident book	As required by health and safety legislation, and no less than 3 years from the date of the record or incident
Unsuccessful job applicant records	6 months from the recruitment decision
Enquiries that do not result in works	12 months from last contact
Temporary property access information (key safe and alarm codes)	Deleted on completion of the works
CCTV or site imagery containing identifiable individuals, where captured	31 days unless required for an incident or claim

B APPENDIX B: PERSONAL DATA BREACH RESPONSE PROCEDURE

Step	Timescale	Action
1. Report	Immediately, within 12 hours of awareness	Staff member reports the actual or suspected breach to the Data Protection Lead with all known facts.
2. Contain	Immediately	Stop the breach and secure the data: recall emails, disable accounts, recover devices or documents, change credentials.
3. Assess	Within 24 hours	Establish what data, whose, how many individuals, cause, and the likelihood and severity of risk to those individuals.
4. Record	Within 24 hours	Record the breach in the breach log with facts, effects and remedial action, whether or not it is reportable.
5. Notify ICO	Within 72 hours of awareness	If the breach is likely to result in a risk to individuals, notify the ICO with the required information. Record reasons if the decision is not to notify.
6. Notify individuals	Without undue delay	If the risk is high, inform affected individuals of the nature of the breach, likely consequences, measures taken, and the contact point.
7. Review	Within 10 Business Days	Identify the root cause, implement corrective measures, and update security, training or this policy as needed.

C APPENDIX C: SUBJECT ACCESS REQUEST PROCEDURE

C.1 Log the request and the date of receipt on the day it arrives. The one month statutory deadline runs from receipt.

C.2 Verify the identity of the requester using proportionate means before disclosing any data. If verification is needed, request it promptly; the deadline pauses until identity is confirmed.

C.3 Clarify scope with the requester where the request is very broad, without treating clarification as a condition of responding.

C.4 Search every system and location holding personal data, including email, job management, certification and accounting systems, mobile devices and paper files.

C.5 Review and redact third party personal data and any material subject to legal privilege or a statutory exemption, recording what was withheld and why.

C.6 Respond in writing within one month with a copy of the data and the supporting information required by Article 15 UK GDPR: purposes, categories, recipients, retention, rights, and the right to complain to the ICO.

C.7 Retain a record of the request, the search, the response and any redactions.

Adopted for and on behalf of Grants Electrical Solutions Ltd

Signed: Shaye Grant

Shaye Grant, Managing Director Date: 22nd July 2026