Davy Engineering Ltd
GDPR Policy Document

DAVY ENGINEERING LTD

Stirling Road, Shirley,
Solihull, West Midlands,
B90 4NE
Tel: 0121 711 4060 Fax: 0121 711 4994
E-mail: sales@davyeng.co.uk

Our Privacy Policy

Our written Privacy Policy is provided and made available to all our customers.

Who are we?

Davy Engineering Ltd. is a "data controller" which means that we are responsible for deciding how we hold and use personal information about you. We are registered with the Information Commissioner's Office.

We are required under Data Protection legislation to notify you of the information contained within this Privacy Policy.

Davy Engineering Ltd. has its registered office at Stirling Road, Shirley, West Midlands, B90 4NE and can be contacted on 0121 711 4060.

We collect the following personal customer information:

- ☐ Full Name
- ☐ Delivery Address and Invoice Address
- ☐ Telephone Number
- ☐ Mobile Number
- ☐ Fax Number
- ☐ Email Address
- ☐ Bank and Payment Card Details
- ☐ Transactions (products bought)

How do we collect this information?

We receive information about you when we provide you with goods or services. This includes making enquiries or placing orders via telephone, email, fax or online. Information can also be gathered from the public domain e.g. from your own website.

Purpose of collecting customer information details

Here at Davy Engineering we take your privacy very seriously and will only use your personal information to administer your account and to provide the products and services you have requested from us.

Personal information is used in ways our customers would reasonably expect and which have a minimal privacy impact. If we plan to use the personal data collected for a new purpose, we update this policy and communicate the changes to individuals before starting any new processing.

Here is a list of the ways we may use your personal information:

Lawful Basis	Our Reasons / Explanation
Consent: the individual has given clear consent for you to process their personal data for a specific purpose.	Non Contractual Customer information is processed to administer accounts e.g. credit card details. Processing of orders using contact information etc. Where possible, we avoid making consent a precondition of service.
Contract: the processing is necessary for a contract you have with the individual, or because they have asked you to take specific steps before entering into a contract.	To process and deliver goods and services you have purchases from us. I.e. fulfilling a contract. To manage payments, fees and charges. To register you as a new customer.
Legal obligation: the processing is necessary for you to comply with the law (not including contractual obligations).	Managing customer accounts / providing services. Keeping our records up to date. Detect, investigate and report financial crime (e.g. fraud) Complying with Health and Safety Obligations
Vital interests: the processing is necessary to protect someone's life.	Not applicable
Public task: the processing is necessary for you to perform a task in the public interest or for your official functions, and the task or function has a clear basis in law.	We may be asked to complete confidential Government questionnaires – e.g. National Office of Statistics
Legitimate interests: the processing is necessary for your legitimate interests or the legitimate interests of a third party unless there is a good reason to protect the individual's personal data which overrides those legitimate interests. (This cannot apply if you are a public authority processing data to perform your official tasks.)	Data is used in ways our customers, suppliers and employees would reasonably expect and which have a minimal privacy impact. For example, using delivery addresses when dispatching goods. Demand forecasting – we use information about sales figures to help us respond to demand, ensuring we have the correct stock in place for our customers. Notifying customers about additional products that they are likely to use. This is done with legitimate interests in mind and is normally the result of customer relationships being developed. Setting up an account. Maintaining network and data security helps us to maintain the safety and confidentiality of your data. To collect and recover sums of money owed to us.

We also process your personal data on the basis that we have a legitimate interest in preventing fraud and money laundering, and to verify identity, in order to protect our business and to comply with laws that apply to us.

Sharing Customer Data with Third Parties

We may provide some information to third parties but only if it is necessary to provide our product / service or to deal with your request. For example:

- Third Party couriers require our customer's name, address and contact details in order for you to receive your goods.

- IT Companies – we work with an external company who supports our business systems.

- Payment Processing – we work with a trusted third party payment processing provider in order to securely take and manage payments.

- We do not directly transfer personal customer data outside of the European Union.

- We do not share or sell information with Third Parties for any other reason.

Anyone we share your data with may only use it in accordance with this privacy notice and is required to take appropriate security and organisational measures to protect your data

How long do we keep customer data?

We only retain your data as long as is necessary for the purpose which we collected it for. To determine the appropriate retention period for personal data, we consider the amount, nature, and sensitivity of the personal data, the potential risk of harm from unauthorised use or disclosure of your personal data, the purposes for which we process your personal data and whether we can achieve those purposes through other means, and the applicable legal requirements.

Customer and Employee Rights

Personal data is protected by legal rights, which include your rights to object to our processing of your personal data; request that your personal data is erased or corrected; request access to your personal data.

Right of access – to request access to your personal information and information about how we process it
Information held on customers and employees can be made available within two working days. It will be delivered by a secure encrypted email unless otherwise stated by the customer.

Right to rectification – to have your personal information corrected if it is inaccurate and to have incomplete personal information completed
If any information we hold is inaccurate our customers or employees can make a request for rectification verbally or in writing. We will respond to any request without delay and at least within one month of receipt.

As a business we also conduct regular data quality reviews of systems and manual records, to ensure the information continues to be adequate for the purposes we are processing for.

Right to erasure – to have your personal information erased
If we are requested to destroy data held on our system we will delete this information whereby it cannot be recovered (a certificate of destruction can be provided). We use a third party who are BSIA accredited.

Right to restriction of processing – to restrict processing of your personal information
Customers and employees can make a request verbally or in writing. We then verify the identity of the person making the request, using "reasonable means" and then respond to the request without delay and at least within one month of receipt.

Right to data portability – to electronically move, copy or transfer your personal information in a standard form
Customers and employees can obtain and reuse their personal data for their own purposes across different services by making a verbal or written request.

Right to object – to object to processing of your personal data
Customers and employees can object to the processing of their personal data in certain circumstances. Customers can make a request verbally or in writing and we will respond to the request without delay and at least within one month of receipt

Rights with regards to automated individual decision making, including profiling – rights relating to automated decision makings, including profiling
We safeguard against the risk that potentially damaging decisions is taken without human intervention during all of our processes.
Customers and employees can request that they are not subject to an automated decision verbally and in writing. We will then respond to the request without delay and at least within one month of receipt

Retention and Disposal of Data

We have a process to dispose of hardware, backup tapes, removable media, hard drives, waste paper and any other types of media that hold data. We use a third party they can provide a certificate of destruction.

Data is not held for any time period longer than necessary and individuals can request for erasure verbally or in writing. We respond to any request without delay and at least one month of receipt.

Our full 'Retention Policy' is available upon request.

Other Confidential Data and Assurances

- By the nature of our business we do collate confidential data such as bank account / credit card details and credit checks. This information is never divulged to third parties unless permission is explicitly requested or granted by the customer in writing.

- Confidential Data is stored securely at all times and we do not hold the data for any period longer than is required to carry out the purpose it was initially collated for. E.g. we do not keep credit card details on record after the transaction has been completed.

- We do not actively copy or clone any data unless required to do so in order to offer our products and services in full. For example, we may be required to clone an order or copy a delivery note to resolve queries.

- Our full ICT Security is detailed within our GDPR Policy Document which is available on request.

- We do not process any children's personal data and do not offer any kind of online service directly to children.

Personal Data Held

Employees

- Full Name
- Full Address
- Telephone Numbers
- Email Address
- National Insurance Number
- Bank Account Details
- Next of Kin Contact Details
- Qualifications

Sharing
This information is only shared with our Accountant and the Pension PAYE Company.

Location
This data is held in a private locked filing cabinet.

Customers

- Full Name
- Delivery Address and Invoice Address
- Full Name
- Telephone Number
- Mobile Number
- Fax Number
- Email Address
- Bank and Payment Card Details
- Credit Terms / any Credit Checks
- Transactions (products bought)

Sharing
Limited details may be shared with our Third Party couriers for example, customer's name, address and contact details. We do not share or sell information with Third Parties for any other reason.

Location
This information is held on our secure computer system and occasionally in private filing cabinets.

Method of Communication
Where personal data needs to be sent out externally we use secure encrypted emails.

Access Request

Employees

All employees are able to view the information we hold on them by simply asking.

Customers

Information held on customers is made available within two working days. It will be delivered by a secure encrypted email unless otherwise stated by the customer.

Please see ‘Customer and Employee Rights’ in previous section for additional information.

ICT Security

Data Breach Prevention

Third Party Subcontractors

- We use an external ICT company who look after our system.

- All third parties used adhere to our strict ICT Policy and respect our obligations to our customers by performing as if they were signatories.

Firewall Defense System

Our internal networks are protected with an industrial grade WatchGuard Firewall product. The Firewall enables us to detect and monitor for any security breaches.

Anti-Spam / Anti-Virus

Our internal systems all have anti-spam / anti-virus protection in place that is updated on a daily basis. Our staff are all fully trained to be vigilant when dealing with emails. We adopt a strict 'in doubt, delete' policy.

Threat Detection

In addition to our outer perimeter firewall security features, we make use of Windows security log files to monitor individual computers.

Credentials / Password Policy

- Each employee has their own unique username.
- Password must be unique within the organization.
- No password should ever be written down.

System Maintenance

Where required our computer systems are patched and updated.

Removable Media

- Removable media may be used internally for the internal transfer of data.
- A secure password must be entered to transfer data from the system onto removable media.
- Movement of small amounts of confidential data outside the office is only allowed on encrypted protected devices.
- Copying of any data is only permitted to complete the job in hand.
- Where we backup large amounts of data, care is taken to safeguard the encrypted media.
- We do not transfer personal data outside of the European Union.

Data Backup

- Relevant computer systems are fully backed up daily (no fewer than once every 24 hours)
- Backup drives are stored in a secure place and are clearly and correctly labelled.
- At least three generations of the backup are retained at any time.
- Periodically backups are checked to ensure the data can be restored successfully.
- The backup log files are checked on a daily basis.
- To protect against ransomware attacks we:
    - Use daily disk rotation
    - Use a proprietary backup software that offers protection against tampering.
- Media used for back up purposes is disposed of in a secure manner when no longer required.

Disaster Recovery

- We have a system in place that allows recovery of any critical system within one working day. To achieve this we also have a spare machine available.
- For each critical system we hold the necessary drives, software tools etc. to ensure rapid rebuilds. Our backups are easily identified.
- Recovery tests are carried out no less than twice per annum.

Security Testing

- At least once a quarter we conduct testing of our ICT systems.
- Results of such testing can be made available to our Customer's upon request.

Asset Register

- Our Asset Register is maintained and updated as required (when an asset is added, removed or changed).

Breach Notification

We have a duty to report certain types of personal data breaches to the ICO and, in some cases, to the individuals affected.

The ICO will be notified of a breach unless it is unlikely to result in a risk to the rights and freedoms of individuals. Where a breach is likely to result in a high risk to the rights and freedoms of individuals, we will notify those concerned directly and without undue delay. Any notifiable breach will be reported to the ICO without undue delay, no later than 72 hours after becoming aware of it. All staff are fully aware of what constitutes a breach.

We maintain records of personal data breaches, whether or not they are notifiable to the ICO.

We have an internal breach reporting procedure in place.

Staff Training and Responsibility

All of our staff have signed a confidentiality agreement as part of their employment contract. Any new members of staff also adhere to this policy.

It is the policy to regularly review with the staff the company policy of the GDPR regulations.

Handling Telephone Calls

- We make any caller aware that we may record the call.

External Cold Calls

- Every caller must clearly identify who they are i.e. the name and number they are calling from and the nature of the call.
- Staff must satisfy themselves that the caller is who they say they are. If they are unsure the call is to be transferred to the office manager or the most senior person available.
- They will be asked for the source from where they acquired our details.
- Staff names will not be given out, only an email address for them to send additional information for further consideration.

Customer Calls

- The caller is asked for the nature of the call, which is then put through to the relevant person.

Emails

- The sending or receiving of personal emails is forbidden on the business' computer system.
- Each person is responsible for not releasing emails held by the anti-spam software unless they are absolutely sure of the genuineness. If unsure the office manager or most senior person in the office should be consulted. This policy also applies to opening any 'email links'.
- Any confidential emails, including any emails with personal data, must be sent securely.

Internet

- The internet can only be used for company business during working hours.
- It is forbidden to access any social media sites at any time.

Clean Desk Policy

- We operate a clean desk policy whereby all sensitive information is placed in secure filing cabinets.