4c Engineering Information, Data Protection & Privacy Policy

At 4c Engineering, we recognize the importance of protecting personal data and are committed to complying with the General Data Protection Regulation (GDPR) requirements. As a Controller of personal data, we only collect and process basic personal data about individuals in a business context. This includes name, address, email, and phone number, which is necessary to provide information about our services and for carrying out the contracted work.

All personal data is processed by us in the UK, and any data located on servers outside of the UK is through a company signed up to an appropriate GDPR compatible agreement. We have a Data Protection regime in place to oversee the effective and secure processing of personal data. Personal data is not shared with any third parties unless data subjects explicitly agree to engage in publicity with them, or if the law allows them to do so.

We collect web statistics concerning visits to our website, which are stored in a log file, and employ cookie technology to enable certain features (e.g. embedded videos, map, social media links). Cookies do not contain any personal information and cannot be used to identify an individual user. Users can set their browser not to accept cookies, but this may affect some of the enhanced features on our website.

Data is collected when a client or supplier contacts 4c Engineering. Data will be used to generate a contract, communicate with the client or supplier, and for the purpose of carrying out the contracted work, along with all associated processes. The data may be seen by members of 4c Engineering and subcontractors. When the contracted work is complete, the information may be used to stay in touch and for any associated follow-up.

We keep personal data for as long as it is necessary for the purposes for which it was collected, and in accordance with this Information, Data Protection & Privacy Policy. If individuals believe that the information we process about them is incorrect, they may request to see this information and have it corrected or deleted. If they wish to raise a complaint about how we handle their personal data, they can contact directors (Andy Hall, Peter MacDonald or Jo Wilson), who will investigate the matter. If data subjects are not satisfied with our response or believe that we are processing their personal data not in accordance with the law, they can complain to the Information Commissioner's Office (ICO).

This privacy policy applies to all personal data processed by 4c Engineering, regardless of the source of the personal data. We may update this policy from time to time to reflect changes in the law or our privacy practices. Any updates will be posted on our website, and we encourage data subjects to review this policy regularly to stay informed about our data privacy practices.

4c Engineering takes Data Protection seriously. Any breach of the Information, Data Protection & Privacy Policy should be investigated, and may lead to disciplinary action.

1. **Data Protection responsibilities**
    a. The company does not require a Data Protection Officer. The Directors of the company are responsible for Data Protection.

2. **Authorised users & access to information**
    a. Only authorised personnel can access the 4cE premises.
    b. Only authorised personnel can login to the computing system or associated programmes holding personal data (e.g. Quickbooks). Approval from one of the Directors must be obtained for authorising new users.
    c. When a user leaves the company then their accounts are de-activated.
    d. All passwords must be at least 8 characters long. Users are responsible for keeping PIN/passwords secure.

e. Data that is of the categories in the personal data mapping audit (section 6) should only be accessed and handled by users with authorisation.
f. All authorised users receive appropriate training in the company Information & Data Protection policies as part of the induction process, and during their employment.
g. Directors should undertake appropriate monitoring of the data and systems usage by users. This includes reviewing audit trail of system access and data use as required.

3. Asset management and security

a. New software & hardware should only be installed with the approval of one of the Directors, and should be recorded in the asset register if appropriate.
b. Any new or modified information system, application or network (include security provisions) should be correctly sized, comply with security requirements, and be compatible with existing systems.
c. Personal data should only be recorded on to removable media with the approval of one of the Directors, and should be deleted as soon as possible. Any removable media with personal data on which is lost, stolen or misplaced should be treated as a security incident.
d. Firewalls and anti-malware should be installed and kept up to date on all machines.
e. Time settings should be correct on all machines so that audit trails can be checked.
f. New assets should have default passwords reset.
g. On disposal of assets, all data should be securely wiped from them or alternatively the assets should be securely destroyed.

4. Incident reporting & management

a. Any information security incident or suspected weaknesses should be reported to one of the Directors.
b. Any information security incident or suspected weaknesses should be investigated within an appropriate timeframe, and a full report made to the Directors. The investigation should be recorded and reviewed. All staff should be informed of any learning points or changes of procedure.
c. If required as a result of an incident, data should be isolated to facilitate forensic examination. This would be carried out by an external company.
d. Incidents must be reported to external bodies if required (e.g. law enforcement if criminal activity is detected).

5. System reviews & incident testing

a. Directors should ensure that business impact assessments, business continuity and disaster recovery plans are produced for critical information, applications, systems and networks.
b. Directors should review the company Data and Information Policies (including the business continuity and disaster recovery plans), and test the incident response process annually. A simulation exercise should be run as appropriate.

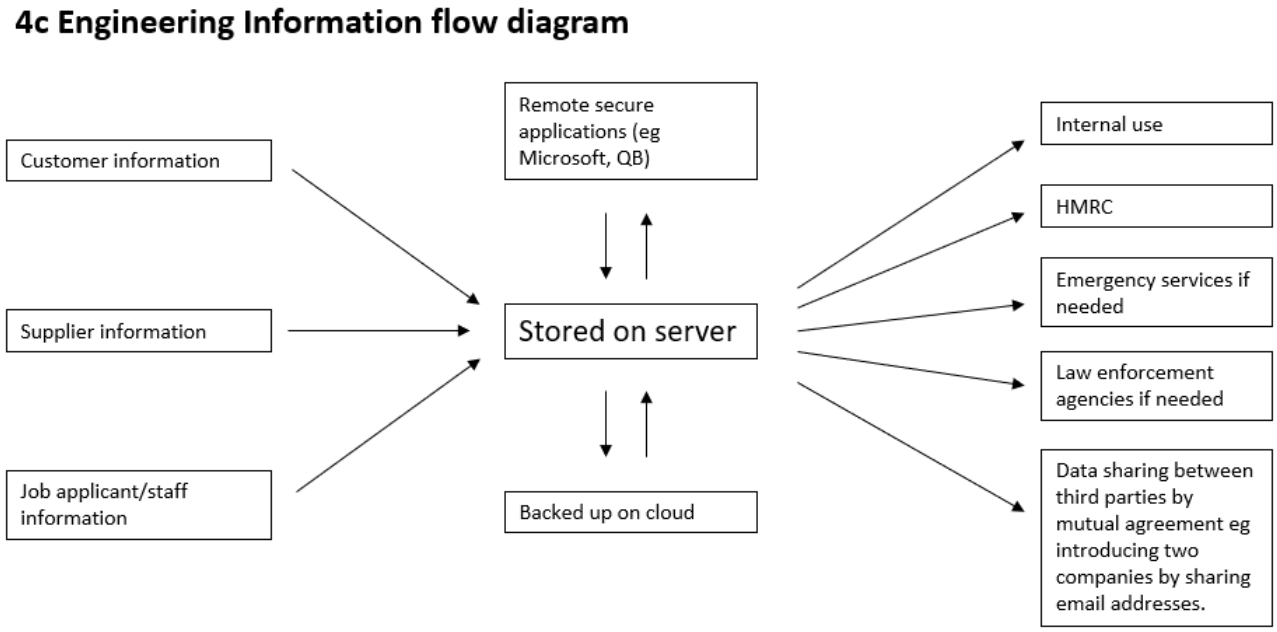
6. Personal Data Mapping Audit

The personal data mapping table is a tool that helps us to identify the personal data we hold and process for different types of data subjects, including prospective and actual clients, suppliers, partners, and employees. As a B2B engineering consultancy, our GDPR requirements are primarily focused on the personal data we hold and process for business purposes, rather than for the general public. This data mapping exercise helps us to ensure that we are processing personal data lawfully and in accordance with GDPR requirements.

Data Subject	Type of Personal Data	Location	Purpose	Lawful Basis	Retention Period
Prospective Clients	Name, email address, phone number, NDAs	Email client, SharePoint	To contact potential clients and provide them with information about our services	Legitimate Interest	Indefinite, unless requested otherwise
Actual Clients	Name, email address, phone number, address, payment information, NDAs	Email client, SharePoint, Accounting software	To manage client accounts and provide services, including future marketing	Contractual Obligation & Legitimate Interest.	Indefinite, unless requested otherwise
Suppliers	Name, email address, phone number, payment information	Email client, Accounting software, SharePoint	To manage supplier accounts and process payments	Contractual Obligation	Indefinite, unless requested otherwise
Project Partners	Name, email address, phone number, NDAs	Email client, SharePoint, Accounting software	To maintain communication with partners and collaborate on projects	Contractual Obligation	Indefinite, unless requested otherwise
Employees	Name, contact information, employment details, bank account information, CVs, Confidentiality agreements	HR system, Payroll system, SharePoint	To manage employment and payroll	Contractual Obligation	7 years after employment termination

7. Information flow diagram

The below information flow diagram gives a visual representation of how information flows through 4c Engineering.



Andy Hall, Jo Wilson & Peter MacDonald - Directors