

Data protection policy

This policy is addressed to all staff members. It is valid in any circumstances where it can reasonably be applied.

We also have strict legal obligations to meet in the way we handle data, most particularly sensitive personal data.

This policy is not flexible. If you work for us or with us, you must comply. This policy is part of the contract of employment of every one of our employees.

If you come across any breach of this policy you should immediately report it, preferably in writing to a manager or director.

1. Aim of our data protection principles

- 1.1. The protection of data is of extreme importance. It is important for us as a business, for our customers and suppliers, for you and particularly for every individual, whether or not that person comes into one of those categories.
- 1.2. The aim of this policy is to ensure that everyone handling Personal Data is fully aware of the requirements and acts in accordance with these procedures.
- 1.3. As an employee of Arrol & Snell Ltd, you should be aware of the importance of complying fully with all policies of the company.
- 1.4. The data protection policy exists to:
 - 1.4.1 Comply with the law;
 - 1.4.2 Protect your data;
 - 1.4.3 Protect the data of other staff members;
 - 1.4.4 Protect and manage the data of every third party with whom we deal, in accordance with the law;
 - 1.4.5 Protect the data of the company.
- 1.5. Please remember that data protection is the responsibility of all staff members at all times. It is very easy to disclose information about a colleague to a customer or friend, or about a customer to your spouse or relative. If you do so, you are in breach of this policy and of your contract of employment. To avoid this, you should avoid discussing any aspect of your work outside of work station and discuss issues about which you have strong feelings only with the appropriate person at work.
- 1.6. We are extremely concerned to protect your privacy and confidentiality. We understand that not only all employees, but also customers, suppliers and others with whom we come into contact in our working day are quite rightly concerned to know that your or their data will not be used for any purpose unintended by them, and will not fall into the hands of a third party. Our policy is both specific and strict. If you come across any instance of a failure of our policy, please do let us know.

- 1.7. Information may be unlawfully available to computer hackers and unlawful visitors. We will take reasonable precautions against such events, but we take no responsibility for any unlawful act of any person.
- 1.8. Except as set out below, we do not share, or sell, or disclose to a third party, any personally identifiable information we collect.
- 1.9. To comply with the law, personal information will be collected and used fairly, stored safely and not disclosed to any other person unlawfully.

2. Definitions used in this policy

"Personal Data" means fact or opinion about any human individual processed or recorded electronically, whether or not automatically, whether or not intentionally, and accessible by any one or more human or corporate persons.

"Data Protection Officer" means a person who (either alone or jointly or in common with other persons) determines the purposes for which and the manner in which any Personal Data are, or are to be, processed

3. Data security

- 3.1. Lynn Clarke is the Data Protection Officer in the Company.
- 3.2. Because Personal Data is or may be held on many computers within the office, please use the password system laid down. Do not change any password or insert password access where previously there was none.
- 3.3. The company has a backup procedure for all data. Those involved in any element of it are reminded of the crucial importance of timely compliance with the procedures.
- 3.4. Any unauthorised disclosure of Personal Data to a third party by an employee may result in termination of employment.

4. Data Protection Principles: the Law

Personal Data must be:

- 4.1. processed fairly and lawfully meaning that the individual must give consent to the processing of it. For sensitive Personal Data, the individual must give explicit consent.
- 4.2. obtained only for specified and lawful purposes;
- 4.3. adequate, relevant and no more than is necessary;
- 4.4. accurate and up to date;

- 4.5. not kept for any longer than is necessary;
- 4.6. processed in keeping with the rights of the individual;
- 4.7. protected against unauthorised or unlawful processing, loss, destruction or damage.

5. Sensitive Personal Data

5.1. The Act defines eight categories of sensitive Personal Data.

These are:

- 5.1.1 the racial or ethnic origin of data subjects;
- 5.1.2 their political opinions;
- 5.1.3 their religious beliefs or other beliefs of a similar nature;
- 5.1.4 whether they are a member of a trade union;
- 5.1.5 their physical or mental health or condition;
- 5.1.6 their sexual life;
- 5.1.7 the commission or alleged commission by them of any offence;
- 5.1.8 any proceedings for any offence committed or alleged to have been committed by them, the disposal of such proceedings or the sentence of any court in such proceedings.

5.2. We do not collect sensitive Personal Data.

6. Training

Training and awareness about the Data Protection Act and how it is followed in this organisation will take the following forms:

- 6.1. On induction: Please refer to the Staff Handbook.

7. Employee information

This information is used:

- 7.1. to maintain proper employment records for our own use;
- 7.2. to maintain salary records and to pay staff in accordance with our obligations;
- 7.3. to comply with our legal obligations relating to tax and money;
- 7.4. to comply with legal obligations relating to employment.

8. Customer and client information

This information is used:

- 8.1. to provide customers and clients with the services they have requested;
- 8.2. for billing and accounting purposes;
- 8.3. to enable us to answer their enquiries;
- 8.4. for verifying their identity for security purposes;
- 8.5. for marketing our services and products;
Information which does not identify any individual may be used in a general way by us or third parties, to provide class information, for example relating to demographics or usage of a particular page or service.

9. Domain names and e mail addresses

You are recognised by our servers and the pages visited are recorded. This information is used:

- 9.1. in a collective way not referable to any particular individual, for the purpose of quality control and improvement of our site;
- 9.2. to send out news about the services to which web site visitors have signed up;
- 9.3. to tell customers and clients about other of our services.

10. Financial information, including credit card details

This information is used to obtain payment for goods and services ordered from us. We do not use it for any other purpose. We do not store this information longer than is necessary to process a payment. We are not responsible for such data once it has passed to our merchant service provider /bank.

11. Business associates' information

This is information given to us in the course of business. This information is used:

- 11.1. to maintain our accounts and business records;
- 11.2. to enable us to answer enquiries;
- 11.3. to verify identities.

12. Disclosure to Government and their agencies

We are subject to the law like everyone else. We may be required to give information to legal authorities if they so request or if they have the proper authorisation such as a search warrant or court order.

13. Cookies

The Privacy and Electronic Communications (EC Directive) Regulations 2003, cover the use of cookies and similar technologies for storing information, and accessing information stored. This website complies with that law.

14. Information request

At any time you may review or update the personally identifiable information that we hold about you, by contacting us at the address below. To better safeguard your information, we will also take reasonable steps to verify your identity before granting access or making corrections to your information.

15. Confidentiality before and after termination of the employment

Between us and each employee, the provisions of this agreement shall remain valid and binding not only for the employment period but for a period of ten years after that. Breach of this provision is a breach of the contract of employment.