DATA PROTECTION POLICY

Cardiff Consultancy Services aims to fulfil its obligations under the Data Protection Act 1998 and the General Data Protection Regulation to the fullest extent. The Partners have been allocated responsibility for compliance with the Data Protection Act & the General Data Protection Regulation.

In order to operate efficiently, Cardiff Consultancy Services has to collect and use information about people with whom it works. This may include clients, customers and suppliers. This personal information must be handled and dealt with properly, however it is collected, recorded and used, and whether it be on paper, in computer records or recorded by any other means, and there are safeguards within the Act & Regulation to ensure this.

Cardiff Consultancy Services regards the lawful and correct treatment of personal information as very important to its successful operations and to maintaining confidence between the company and those with whom it carries out business.

Personal information applies to both manual and computerised personal data held in a relevant filing system. This information must be accurate and up-dated as necessary and clients have the right to see records kept about them.

- Information held on individuals will only be held as long as it is necessary and the company will not hold any information that is unnecessary.
- Data will only be disclosed when legally required to do so or if explicit consent is given by the person on whom the data is held
- The company will identify the relevant filing systems that will be covered by the provisions of the Data Protection Act & the General Data protection Regulation.
- Unauthorised access to personal data (manual or computerised) will not be permitted

Reviewed: May 2020
Next Review: May 2022

Computer Security

- Cardiff Consultancy Services regards the integrity of its computer system as central to the success of the organisation. Its policy is to take any measures it considers necessary to ensure that all aspects of the system are fully protected.
- Laptop computers should not be left unattended and should be stored out of sight in a secure and locked cabinet.
- Databases should not be stored on disks, keydrives or other such mobile data storage devices.

Procedure

- Overall computer security is the responsibility of the partners.
- Information held on record should not be used for a different purpose from the one it was gathered for.
- All incoming emails may be monitored and scanned for viruses before being released to the recipient.
- Passwords must be used at all times and changed regularly. All passwords must be kept confidential

Reviewed: May 2020
Next Review: May 2022