Data Protection Policy

CONTENTS

Overall and final responsibility for the implementation of this policy lies with the:

Managing Director

JBW undertakes to abide by the Data Protection Information Commissioner's Code of Practise and Good Practice Notes and to follow all appropriate legislative requirements and guidelines issued by the Commissioner and relevant enforcement industry associations.

1.0 PRIMARY LEGISLATION

The Data Protection Act 1998 replaces the 1984 Act and places legal obligations on persons who process or record personal information in any format including data obtained by CCTV systems. These obligations relate to the manner in which they are obtained, maintained and utilised.

Related legislation is summarised as follows:

- Data Protection Act 1998
- Freedom of Information Act 2000
- Privacy and Electronic Communications Regulations 2003
- Telecommunications (Lawful Business Practice) Interception of Communications Regulations 2000
- Computer Misuse Act 1990
- Human Rights Act 1998
- Environmental Information Regulations
- Data Protection (Processing of Sensitive Personal Data)(Elected Representatives) Order 2002
- Radio Frequency Identification Guidance (RFID)

2.0 PROCEDURES

JBW collects and uses information about Customers, Clients and others and it is our policy to ALWAYS adhere to the above policies when doing so. This information is obtained from a variety of sources in the public domain or alternatively from sources whilst acting as an agent for our clients – e.g. DVLA.

JBW will store any information obtained in a secure manner regardless of format, e.g. electronic data will be stored and protected by firewalls and passwords, and hard data will be stored in secure filing cabinets.

JBW will maintain the relevant data registration relating to its commercial activities.

JBW will ensure that all staff are kept fully informed concerning their responsibilities under the legislation by means of their training and regular updates as appropriate.

2.1 Policy

JBW will at all times make sure that:

- Personal data is obtained only for lawful purposes
- Personal data is processed lawfully
- Personal data is kept confidential
- Personal data is only released to authorised individuals
- All relevant external codes and guidelines are followed

2.2 JBW Organisational Guidelines

The Managing Director will ensure that:

- All policies are published and available
- All staff are familiar with the requirements of the legislation
- The policy is kept under constant review and updated as necessary
- That reference documentation is available for access at all times – in hard copy and/or via the web
- That any Trade Association guidance will be followed
- That the terms of the company's data registration will be accurate and regularly reviewed

3.0 INTERNET AND EMAIL STAFF GUIDELINES

JBW do not allow staff or visitors to use the internet for personal use during office hours. Staff and visitors are authorised to use the internet and email facilities before and after office hours but are well-informed as to the seriousness of misuse, as this may be a disciplinary matter. No JBW email addresses (i.e. test@jbw.co.uk) are to be used as personal addresses, JBW reserves the right at all time to quarantine and delete any messages that are received via any company email account.

Attachments that are received by any email account must NOT be opened if the sender is not recognised. If emails are received with attachments from an unknown source please notify the IT manager and your direct manager ASAP and DO NOT delete the message as this may not remove the problem but just make it more difficult to find.

JBW staff will not send or store confidential, sensitive, inappropriate or illegal material, any evidence of misuse of these facilities may result in disciplinary procedures in line with the Employee Handbook.

4.0 ELECTRONIC DATA SECURITY

As part of the control over the protection of data JBW maintains up to date security programs covering its servers and PCs in the following areas:

- Anti Virus
- Anti Spyware
- Back-ups in the event of temporary crashes
- Constant Voltage Supply mechanisms
- Firewalls

Passwords are regularly amended and password protected screensavers are used so that PCs cannot be left logged on for inappropriate usage by staff.

There are established, secure arrangements for the backing up of data and systems software. Back-up data is stored in fire and theft resistant safes.

We have business continuity plans in place as well as appropriate levels of insurance cover.

JBW has gained ISO27001 accreditation for its Information Security Management Systems.

Our Enforcement Agents are issued with PDAs and all their vehicles are fitted with tracking devices. These devices are all covered within the data protection requirements and the RFID guidelines.

5.0 ON LINE CLIENT ACCESS

JBW, at all times, keep up to date software firewalls as well as hardware firewalls. We monitor user logs and regularly contact client users with new passwords and detailed user activities.

Users with access to the JBW Debt Recovery System only have access to the data and information held about their customers.

6.0 ON LINE PAYMENTS

JBW offers the facility of On Line Payments and to protect data we use the services of Protex Payment Services and SQL for encrypted data.

The JBW website is subject to the international standard for secure transactions under which all payments are subject to the relevant levels of encryption.

7.0 AUTOMATIC NUMBER PLATE RECOGNITION (ANPR)

All ANPR computer equipment is protected by a software firewall as well as anti virus software. All data sent and received via ANPR vehicles is encrypted using SQL, users each have unique usernames and passwords and user logs are checked and monitored by the IT manager on a regular basis.

8.0 SUBJECT ACCESS REQUESTS

JBW will respond to subject order requests in detail and without delay. JBW will ALWAYS obtain the permission from the data subject unless not required to by law.

JBW are registered under the Data Protection Act.