ALBION
LEGAL
integrity ◆ commitment ◆ trust

Online Security

We understand that we store employee information on our website which is highly sensitive, and we take protecting that very seriously. We believe that the sensitive data that we store is more secure on our website than it is in the traditional physical filing cabinets in which we have all stored this data historically.

We have never had a data breach, and we review our data security regularly. We consult three independent companies, including Symantec and the specialist data security arm of a blue-chip global IT company, to review and test our security measures and make recommendations for improvement.

Our focus is both on maintaining continuous client access to their information and on preventing theft of that information by unauthorised parties (both criminals and “nosy staff” seeking information about their colleagues).

Data Backup

We back up our client data every day to a server at a separate physical location from our core web host. This provides assurance that in the event of a problem at one location, for example fire or flood, we will not only be able to restore the data but also provide continuous service to clients.

We comply with EU regulations for storing personal information, and ensure that both the main server and the backup are located within the UK. This also has the advantage of making it faster to serve information to client requests.

Prevention of Data Theft

Data can be stolen from a location where it resides or from the journey from our server to a client computer. We therefore take steps to secure both.

Physical security

Both the main and the backup server are located in highly secure locations with 24x365 security equipment and staff. We do not disclose the location of either of these servers.

Risk of theft through hacking

The main risk that many people worry about is “hacking.” Hackers could attempt to break into our servers and steal files without logging into our software, or log in and steal files once inside, or steal files while they are travelling between our clients’ computers and our servers.

We deal with each threat separately:

Server protection

Our hosting company provide both hardware and software firewalls to protect our servers. These are scanned permanently by automated tools to ensure they are running securely. Our host reviews its procedures regularly in order to keep up with the latest security measures. Its other hosting clients include both large private organisations and security departments with highly sensitive data; some of these clients regularly test our hosting company's procedures to ensure they remain robust. Our data benefits from the same levels of security as the hosting company's other clients.

Software protection:

Our software requires users to log in using their username and password. We use industry standard authentication software developed by Microsoft for this.

We recommend that users change their passwords frequently and keep them confidential.

Our software automatically logs users out after 20 minutes of inaction to minimise the risk that a passer-by can jump on to a device logged onto our software and make unauthorised use of it.

We have written the software to minimise the risk that someone will be able to detect a pattern of web addresses and guess at potential usernames to try.

We use a digital security company which counts major banks among its customers to review the vulnerability of our software and make recommendations. This testing reviews the risks that an authorised user can access data they are not authorised to see as well as the risks of an unauthorised user gaining access through the software itself.

Risk of theft during data transmission

We use Norton's Secure Website services to encrypt data transmitted from our server to a client computer. Clients need to log onto a secure website using the https letters rather than the simpler, unencrypted http.

We have contracted with Symantec to regularly scan our site for potential vulnerabilities.