Information Management and Security - Is Your Data Secure?

At The Safeguarding Company many members of our team have extensive experience of investigating safeguarding concerns and giving evidence in courts, tribunals and at other formal hearings. Consequently, all of our systems, processes and behaviours are designed to achieve the best possible levels of information security. The security of information held within our Products and Services is of paramount importance, both to us and to our customers, not least because of the impact that this has on the lives of the children, young people and adults at risk whose welfare you are responsible for.

Accountability

Our Chief Technology Officer (CTO), Darryl Morton, has Board-level responsibility for all of our security and data protection arrangements. He is supported by a full-time Systems Administrator and Data Protection Officer who is responsible for all aspects of security on a day-to-day basis.

The biggest risk to information security in any organisation can be the way that information is handled by staff. All The Safeguarding Company staff are background checked and are subject to a relevant Disclosure and Barring Service (DBS) check , which guarantees that they are fit and proper to work with confidential data or in a restricted environment. Additionally, our staff are regularly trained and updated on information security to maintain an active awareness of their responsibilities.

Our Safeguarding Team are all recruited with a relevant background in fields such as social work, policing or the teaching profession. In addition to receiving regular information security training, each Safeguarding Team member undertakes an annual refresher on safeguarding; in fact, many of our Safeguarding Team also provide accredited safeguarding training to our customers.

Information security also forms an integral part of the training and staff briefing materials that we provide to establishments adopting our Products and Services.

Secure Access to MyConcern

Access to the data in MyConcern is secured using two-factor authentication. Every transaction within the software is captured in an unalterable audit log to guarantee the integrity of the data, such that it can be relied upon in court as evidence. Establishments allocate locally controlled role-based access to MyConcern, so their trusted users will only ever see the information that they 'need to know' and are entitled to access.

Quality Systems

The processes we follow as a business are accredited to the ISO9001:2015 standard. By adhering to a quality-managed process, we can demonstrate that we follow correct procedures to meet our customers' expectations. Our ISO9001 system is audited annually by an independent, UKAS-accredited auditor.

Security: Independently Audited and Accredited

We hold two specific accreditations for information security, the first of which is ISO27001:2013, the latest version of this internationally recognised information security standard. ISO27001 (sometimes referred to as '27K') requires us to comply with 114 individual controls covering every aspect of information security. As part of ISO27001, we employ security practices such as 'least privilege' access, asset management and tracking, rotation of certificates, regular resetting of administrator passwords, encryption, secure disposal of old equipment, secure shredding of paper waste, and many more, practices which some software vendors neglect to follow. The ISO27001 certification is audited annually by an independent, UKAS-accredited auditor.

We also hold the Cyber Essentials Plus certification, against which we are independently audited on an annual basis. Part of this audit involves external penetration testing of our own network and systems to prove that our internal systems are secure. (Cyber Essentials is a Government-backed, industry-supported scheme to help organisations protect themselves against the most common threats found on the internet. However, the basic Cyber Essentials certification is based on self-assessment. Cyber Essentials Plus offers a greater level of assurance that the controls are in place by using a wider range of tools and techniques to test the controls including an audit of our security arrangements by expert external assessors).

Many software vendors claim to hold certifications for information security, but upon closer inspection, you will find that it is only the data centre they are using that has the necessary accreditations in place to keep your data secure.

Penetration Testing

We also conduct regular Penetration Testing against our Products to ensure that the applications and data centres that hold your sensitive data are subject to independent scrutiny by security consultants, Purecyber Security. Any issues or recommendations found during testing are acted upon to ensure that all systems outside of our office are secure. We ensure that our supply chain also holds these same accreditations.

Registered with Information Commissioner's Office

The Safeguarding Company is registered with the Information Commissioner's Office both as a Data Processor for our customers' data and as a Data Controller for our own company data. Our systems and operations are fully compliant with both the Data Protection Act 2018 and the General Data Protection Regulation (GDPR). Our statement on GDPR sets out how we ensure we are fully compliant.

Secure Hosting

All data centres used by The Safeguarding Company are secure, resilient Microsoft Azure data centres located in the UK. Data is not transferred outside of the EEA. Microsoft holds many accreditations and certifications relating to information security which can be accessed from the Trust Center pages of the Microsoft Azure web site.

Resilient Architecture

We operate our Products from multiple data centres, in the event of a service-affecting incident in one location, we can continue to provide services to our customers from another data centre. The architecture of our data centres means that data is stored on multiple, redundant servers in each location mitigating the need to restore from a backup. In the event that we do need to roll back, data is backed up to yet another data centre and kept for 30 days.

Disaster Recovery and Business Continuity

We have robust disaster recovery and business continuity plans in place, so that, should the worst happen, we can continue to provide a quality service to our customers and maintain high standards.

Data at rest is protected by Azure's Transparent Data Encryption (TDE). The cipher used is 256-bit AES and encryption keys are rotated every 90 days. Data in transit is protected using a TLS 1.2 certificate that are regularly renewed (and updated, if relevant).

Our applications run on 2 UK based Azure Data Centres which provides excellent redundancy options. If our services were adversely affected we are also able to quickly redeploy our Products temporarily to an EU based Azure data centre which provides even greater resiliency for our customers' data and availability.

Registration/Certificate Numbers

Companies House	Company Registration Number: 09075059
ISO9001:2015	Certificate number: 63990/A/0001/UK/En
ISO27001:2013	Certificate number: 63990/B/0002/UK/En
Cyber Essentials Plus	Audited by Predatech | Cyber Security Specialists
Information Commissioner's Office	Registration reference: ZA102991
Penetration Testing Services	Audited by PureCyber | Award-winning Cyber Security
Microsoft Azure Trust Centre	https://azure.microsoft.com/en-gb/overview/trusted-cloud