MERCERS

SOLICITORS

Information and Data Security

The Firm's measures

Cyber security

We give utmost priority to the security of our IT systems and data held to ensure it is protected and remains confidential. We have numerous measures in place to protect our systems and data, implemented using a range of experts to ensure there are no gaps and that work is independent and audited.

Proactive and preventative measures include

- investment in robust, quality hardware and software designed to protect our systems from vulnerability and attack. We have a programme of review for upgrading this

- accreditation to Cyber Essentials and Cyber Essential Plus, the latter ensuring rigorous independent checks on standards of compliance and security

- accreditation to ISO 9001;2015, (equivalent to Lexcel) which sets expected standards of compliance across all areas of the Business and our management systems. There is regular scrutiny of our compliance via independent auditing twice a year

- regular programme of independent testing of our systems by cyber experts including vulnerability scans and cyber penetration testing to ascertain that systems are up-to-date and there is no vulnerability

- a full programme of training ensuring staff awareness of law, regulation and policy around confidentiality, data management and cyber risks – this includes social engineering testing and risk awareness training programmes to enhance practical skills in detecting and avoiding fraud

- regular notifications to staff regarding current scams, stats and trends

- regular internal tests and audits to review areas of risk and identify any weak areas

Arrangements for retention/deletion of data and information

We are required by law and our Regulator to retain documentation and data concerning our cases for specific periods of time. This prevents us from destroying documentation clients and contacts send us in connection with a case even after completion of a matter, as we have a duty to retain the file. The timeframes for destruction are quite complex and vary according to the nature of the case and the data held. We have a formal Retention and Disposal Policy which the Firm follows regarding retention of data. That Policy will be applied to the work we are doing in the matter in which you are involved.

Obtaining ID and Source of Funds information

We are required by law to obtain information on client identify, the purpose of the instructions and the source of funds or wealth being used to fund a transaction or matter. We are prevented by law from continuing to act where the information provided is inadequate or unsatisfactory. We use third parties to assist us in meeting our duties. One such third party is Thirdfort, who are an identification verification service. We only use third parties after a rigorous process of due diligence checks to ensure they are safe, reputable, accredited to certain standards and have necessary security and data protection measures in place. Thirdfort are a respected company with whom we have had dealings for a number of years and who have achieved Law Society-Partner status and meet HMLR "digital standard" compliance requirements. They provide verification reports using a range of sophisticated techniques and data-sources to provide full information and counteract fraud. For more information about Thirdfort and their credentials, refer to their website www.thirdfort.com

Our recommended action for your own protection

There are some steps that you can take which will reduce risks of fraud and add protection. Recommended action is:-

For all communications with us, ensure you use a secure e-mail account which is protected with multi-factor authentication.

We recommend you avoid all forms of public or less secure WiFi when accessing your e-mails.

Take care with any incoming communications that you are on the alert for scams, phishing attempts and any suspect links or attachments in incoming e-mails. These open you up to vulnerability and potential e-mail interception/fraud.

Ensure you do not post on social media any information about circumstances around your legal matter, especially an impending property transaction, as it will make you a target for fraud.

Ensure your social media and other on-line accounts have restricted permissions, safe password protection and no shared access in order to restrict information that fraudsters can access about you and your contacts.