Information Security Policy

Picker is fully committed to delivering high quality surveys, research and service improvement in a way that ensures the confidentiality, availability and integrity of data, including personally identifiable data, and protects the reputation of our clients. To assist in meeting this commitment, we maintain the following accreditations:

- ISO 20252:2019 Market, opinion and social research
- ISO 27001:2013 (transition to ISO 27001:2022 due in 2025) Information security, cybersecurity and privacy protection – Information security management systems
- Cyber Essentials
- NHS Data Security and Protection Toolkit
- Registration with the Information Commissioner's Office

By maintaining these accreditations, Picker is providing a guarantee that all information is handled securely and that compliance with data protection legislation and the Market Research Society's (MRS) Code of Conduct is upheld.

Picker's Information Security Objectives are:

- To avoid any data breaches during normal working practice
- To not incur any data theft or loss
- To prevent any concerns arising which would require reporting to the Information Commissioner's Office
- To maintain our external accreditations
- All staff and freelancers receive an Information Security and Quality Assurance induction

Picker has a quality assurance and information security management system (QA&ISMS) in place which details the processes, policies and procedures to ensure we comply with the above accreditations. In addition, Picker has a Data Processing and Protection Policy, which is available on our website www.picker.org, which fully supports and complies with current data protection legislation. Our Data Processing and Protection Policy has a clear scope, defines roles and responsibilities and has a comprehensive distribution and training plan.

Our systems and processes include a thorough approach to assessing and mitigating risk, and ensuring business continuity through a prescribed plan.

We have procedures in place to ensure that any sub-contractors we use conform to our QA&ISMS.

We are committed to the continuous improvement of our QA&ISMS: we routinely monitor and act on opportunities to improve systems and processes. In addition to the regular surveillance visits carried out by external bodies we have our own auditing and quality assurance and information security management team. With the help of feedback from our clients, the team continuously monitors and improves the quality of service we provide.

Executive Team
September 2024