Capita

Information and Cyber Security

We expect the highest standards of information security, regardless of whether information belongs to Capita, our people, our clients, or their customers. Every person who works for us has a responsibility to keep information safe. This policy sets out Capita's commitments to information security and what we expect of you.

We are committed to

- Maintaining the confidentiality, integrity, and availability of information, while ensuring information is only accessible by those who are entitled to access it.
- Protecting information assets consistently to a high standard to prevent compromise by external and internal threats, both deliberate and unintentional.
- Raising and maintaining security awareness to help avoid the unintentional or malicious disclosure of confidential information, which could cause inconvenience and distress to others, be unlawful, and to avoid causing financial and reputational damage to Capita.

In line with our:

- Cyber and Information Security Standards.

What you should expect from us

- We will conduct our business in a way that detects, prevents, and disrupts the deliberate or unintended misuse of information.
- We will act in accordance with all relevant and applicable data protection laws that apply in the countries we operate in as well as industry good practice and our client obligations.
- We will provide you with regular information security awareness and guidance.
- We will provide secure devices and a secure IT working environment.
- We will maintain a secure physical workplace environment.
- We require our suppliers, agents and other third parties we work with to provide services in compliance with this policy and our Security Standards.

What we expect from you

- To follow this policy and acceptable use standard as well as the requirements of other security standards relevant to your role and the business area you operate in.
- To act with the upmost integrity in your use of any Capita assets, including data and IT equipment. This includes only connecting authorised devices to Capita IT systems.
- To complete all information security training that applies to you.
- To keep company assets safe and return them to us for secure disposal or reuse when required.
- To remain vigilant to security threats and always protect information in your care.
- To report all security incidents and inform your manager if you suspect anything which may compromise security or informational assets.
- We expect the highest standards of information security, regardless of whether information belongs to Capita, our people, our clients, or their customers. Every person who works for us has a shared responsibility to keep information safe. This policy sets out Capita's commitments to information security and what we expect of you.
- To Speak Up if you face a situation where you are not sure what to do or have a concern in relation to this policy.
- Our **Speak Up Policy** sets out the channels available to you to do so and no action will be taken against you if you report a genuine concern. Whether proven or not.

How we will achieve this

- Every division and function in Capita must apply our Information Security & Cyber standards, procedures, and guidance.
- They set out our baseline requirements and steps which must be followed in relation to:
  - Data security and handling / classification of information.
  - Identifying and dealing with information security incidents and threats.
  - Physical security of information and systems.
  - IT system, cloud computing and network requirements.
  - Supply chain management.
- Our management teams are supported by our Group and Divisional Information Security Officers who provide counsel and challenge on information security matters.
- We take policy non-compliance very seriously. Information security is reported and managed through our governance mechanisms, which ultimately includes reporting to our Group Risk Committees.

Paul Key
Group Chief Information Security Officer
May 2021