Information and Cyber Security Policy

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.
- Protecting information assets consistently to a high standard to prevent compromise by external and internal threats, both deliberate and unintentional.
- Ensuring data is classified according to its type, sensitivity, and value to Capita and our clients.
- 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 cause financial and reputational damage to Capita.

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 line with this policy, and we expect our suppliers to have implemented appropriate technical and organisational measures to ensure a level of security that aligns with the recognised potential risk.
- We will undertake relevant checks and vetting of personnel as appropriate and proportionate to the identified risk, contractual obligation, and regulatory requirement.

What we expect from you:

- To follow this policy as well as the requirements of other security standards relevant to your role, contract, or business area you operate in.
- To act with the utmost 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 hold all information securely and appropriately when not used.
- To handle and secure information in accordance with contract, regulatory, and legislative requirements.
- To remain vigilant to security threats and always protect the information in your care.
- Report all security incidents and inform if you suspect anything which may compromise security or informational assets.
- Capita encourages you to Speak Up if you face a situation where you are not sure what to do or have a concern with this policy. 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 & Cyber Security policy, standards, procedures, and guidance.
- They set out our baseline requirements and steps which must be followed relating 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 security management.
- Our management teams are supported by 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 include reporting to our Group Risk Committees.