



Cyber Psychological Safety Policy

In today's fast-moving digital world, cybersecurity is as much about people as it is about technology. At Capita, we're committed to creating a culture where psychological safety empowers colleagues to speak up, ask questions, and learn from mistakes without fear of blame. This policy ensures that internal cybersecurity assessments are used to support growth and learning, so everyone feels confident to engage openly. It also protects those who raise concerns, reinforcing our shared responsibility for a secure and accountable workplace. Together, we build resilience by putting people at the heart of our cyber strategy.

We are committed to:

- **Valuing Everyone** by fostering a culture of psychological safety in our cybersecurity practices, where every colleague feels safe to speak up, learn, and grow without fear of blame or retribution.
- **Achieving Together** by using internal assessments - like phishing exercises, penetration tests, and incident reviews - as opportunities for shared learning and continuous improvement, not punishment.
- Putting **Customers First** by maintaining a non-punitive environment that strengthens our collective resilience, ensuring that any errors or vulnerabilities lead to smarter, more secure outcomes for those we serve.
- Encouraging **Fearless Innovation** through open communication and collaboration, empowering all team members to contribute confidently to Capita's cybersecurity defences.

In line with our:

- Information & Cyber Security Strategy & Policy.

What you should expect from us:

- A safe and inclusive environment where every contribution to cybersecurity is valued, and colleagues can engage without fear of blame or reprisal.
- Clear and transparent internal assessments that are used solely to identify opportunities for improvement.
- Fair, non-punitive responses to security vulnerabilities or incidents, with a focus on learning and strengthening our collective knowledge.
- Open, honest communication that encourages collaboration and innovation, empowering teams to challenge norms and explore new ideas.
- A dedicated focus on improving the security culture across the business, ensuring that everyone feels part of the journey towards a safer, more secure Capita.

What we expect from you:

- Engage openly and honestly in all cybersecurity assessments, sharing relevant information to help identify areas for improvement.
- Embrace a culture of learning and growth, recognising that assessments are designed to strengthen our security, not assign blame.
- Actively contribute with constructive feedback and collaboration.
- Follow cybersecurity protocols and best practices, supporting Capita's ongoing efforts to enhance security.
- Reach out to your line manager for help and guidance when you don't understand something.
- Remain proactive and vigilant, reporting any security concerns or vulnerabilities promptly to help protect Capita.

How we will achieve this:

- Communicate clearly and transparently about how cybersecurity assessments are conducted and how their findings will be used to support learning and improvement.
- Create space for ongoing collaboration and feedback by involving teams in discussions around assessment outcomes, encouraging shared responsibility for strengthening our security.
- Provide regular learning opportunities to help all colleagues and managers understand the purpose of assessments and how they contribute to a safer working environment.
- Keep security culture front and center by continuously reinforcing behaviours, mindsets, and practices that make cybersecurity a shared, everyday responsibility.

What we expect from our managers:

- Lead by example, encouraging open communication and treating cybersecurity assessments as opportunities, engaging fully with our security culture initiatives.
- Provide constructive feedback and support their teams in addressing vulnerabilities and implementing necessary improvement.
- Ensure that internal assessments are conducted fairly and transparently, with a clear focus on strengthening Capita's security, not assigning fault.
- Recognise and promote a growth mindset, helping their teams view assessments as chances for development and reinforcing the importance of collaboration and continuous improvement.

Luke Beeson
Chief Information Security Officer
October 2026