Cyber and Information Security Policy (Statement)

We (Ramsay Health Care UK) expect the highest standards of information security. Every individual who works for us has a shared responsibility to keep information safe. This policy sets out Ramsay'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 made accessible to those who need to see it.
- Protecting information assets consistently to a high standard to prevent compromise by internal and external threats, both deliberate and accidental.
- Raising and maintaining security awareness to help avoid 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 Ramsay Health Care UK

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.
- We will provide you with regular information security awareness and guidance
- We will provide secure access to appropriate technical and digital services
- We will maintain a secure physical workplace environment
- We require our suppliers and third parties we work with to provide services in compliance with this policy and our security standards.

What we expect from individuals handling/accessing Ramsay's information assets

- To follow this policy and the requirements of other security standards relevant to your role.
- To act with integrity in your use of Ramsay Assets, including data and IT equipment.
  Individuals are reminded they must not disconnect or connect devices to the physical IT infrastructure without appropriate approval from Ramsay D&T colleagues.

- To complete all information security training that applies to you, within the required timeframe (prior to expiry).
- 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 assets in your care.
- To report all security incidents, and inform your manager if you suspect anything which may compromise security or information assets.
- 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.

How we will achieve this

- Every hospital site and function in Ramsay Health Care UK must apply the Cyber & Information Security standards, procedures and guidance.
- They set out the 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
- The Executive Board and Senior Leadership Team are supported by the Information Security Team who provide counsel and challenge on information security matters.
- Applications for exceptions can be submitted and reviewed by the Information Security Team using the 'Security Exception Form'.
- Appropriate governance is in place in the form of the Information Governance Committee (IGC), with representation across the business and chaired by the Senior Information Risk Officer (SIRO) – Ramsay's Chief Digital & Information Officer.
- The IGC provides overall monitoring and scrutiny of all information security related matters and reviews all breaches on a quarterly basis.
- An Information security update report is provided for review by the Risk Committee, attended by the Executive Board on a quarterly basis.

APPROVED BY: NICK COSTA, CEO
DATED: 10 AUGUST 2022

Documentation control

Document Control	Reference Details
Document Title	Cyber & Information Security Policy Statement
Document Reference	POL001
Date of Issue	10th August 2022
Author	Kelly Stather
Owner	Head of Information Security, Risk & Compliance

Version History

Date	Version	Description	Author
8th June 2022	0.1	Draft for consultation	Kelly Stather
8th June 2022	0.2	Removed reference non-compliance and added additional detail re IGC	Kelly Stather
10th June 2022	0.3	Additional clarity added following feedback from SIRO.	Kelly Stather
1st August 2022	0.4	Approval from IGC (July's meeting)	Kelly Stather
10th August 2022	1.0	Published following approval from CEO	Kelly Stather