IT Security: Policy Statement

1. Introduction

1.1 The Trust is committed to protecting the availability, confidentiality and integrity of its IT infrastructure, applications and data against malicious and unauthorised activity.

1.2 The Trust recognises that cyber incidents may impact the Trust's ability to conduct its normal operations – including carrying out its statutory duties – and may incur unplanned costs and negatively affect its reputation.

1.3 The Trust is committed to:

1.3.1. complying with UK data protection legislation and keeping personal data safe and secure.

1.3.2. complying with the Computer Misuse Act 1990 and protecting Trust systems from those who seek to gain unauthorised access to its IT systems.

1.3.3. complying with the Payment Card Industry Data Security Standard (PCI DSS) to allow customers and partners to pay securely for the services they use.

1.3.4. complying with the Cyber Essentials scheme and maintaining certification.

2. Our approach

2.1 We will:

2.1.1. Maintain an IT & Cyber Security Governance Framework which sets out the standards, structure and roles that we have in place to support good cyber security.

2.1.2. Maintain an in-house IT Security function responsible for all security activities and outsource certain security operations to 3rd

parties as appropriate to provide 24/7/365 monitoring and response capabilities.

2.1.3. Use the guidance and standards of good practice set out by the UK's National Cyber Security Centre (NCSC) to inform and judge the maturity of the Trust's IT Security programme.

2.1.4. Operate a risk-based approach to protecting its IT assets, taking into account current and likely threats, vulnerabilities and evolving attacker tools, techniques and procedures.

2.1.5. Manage a set of protective and detective, administrative and technical controls to safeguard its IT assets.

2.1.6. Where possible, operate a least privilege and zero-trust approach to providing access to IT resources.

2.1.7. Seek regular assurance that its IT security controls are effective and appropriate.

2.1.8. Have arrangements in place to manage IT security incidents, facilitate business continuity and disaster recovery.

2.1.9. Ensure that security is designed into all IT projects from the outset.

2.1.10. Provide all colleagues & volunteers with appropriate training and guidance on cyber security.

2.1.11. Embed a culture of good security practices throughout the Trust through advice, training and communications.

2.1.12. Not tolerate being held to ransom by those who seek to exploit any weakness in our IT systems, and use the full force of the law to seek to prosecute those who try.

David Orr CBE

Chair to the Board of Trustees

Campbell Robb

Chief Executive

January 2026