



Joint Policy for Cumbria Partnership Foundation Trust & North Cumbria University Hospital NHS Trust

Policy Title: Joint Cyber Security Encryption Policy

Reference	POL/IG/013
Version	V1.0
Date Ratified	19/03/2019
Next Review Date	31/03/2022
Accountable Director	Executive Director of Finance & Strategy (Joint Director of IM&T and Estates)
Policy Author	Trust Information and Cyber Security Officer

THIS POLICY IS EXEMPT FROM PUBLICATION ON THE TRUSTS' PUBLIC WEBSITES

Cyber-attacks, which may amount to criminal offences for example under the Computer Misuse Act 1990 or the Data Protection Act 1998 (GDPR from 25th May 2018), are rated as a Tier 1 threat by the UK Government. The Trust like any organisation may be subject to cyber-attacks, and since it holds large amounts of sensitive, personal and confidential information, and is classed as an Operator of Essential Services (OES) by the electronic communications, the Network and Information Systems Regulations 2018, maintaining the security of this information is extremely important. In this context, the Trust considers that disclosure would provide information about the Trust's information security systems and its resilience to cyber-attacks. There is a very strong public interest in preventing the Trust's information systems from being subject to cyber-attacks. Confirming or denying the type of information requested would be likely to prejudice the prevention of cyber-crime and effective conduct of public affairs, and this is not in the public interest. In conclusion this is the rationale and reasoning as to why this policy is exempt from publication on the Trusts' websites.