Surrey and Sussex Healthcare
NHS Trust

Trust Headquarters
East Surrey Hospital
Canada Avenue
Redhill
RH1 5RH

Tel: 01737 768511
www.sash.nhs.uk

Our ref: 4570

1 March 2018

Freedom of information request

1. Does your organisation adhere to the Network Security guidance outlined by the National Cyber Security Centre, within its' 10 Steps to Cyber Security'? *See below
   - o Yes
   - o No

2. Do you ensure that security patches for critical vulnerabilities are routinely patched within 14 days, as recommended by the National Cyber Security Centre? *See below
   - o Yes
   - o No

3. Have you suffered from any service outages on your network in the last two years, however small? *See below
   - o Yes
   - o No

4. Did any of these outages cause a loss, reduction or impairment to your organisation's delivery of essential services? *See below
   - o Yes
   - o No

5. Was the root cause of the service outage identified and confirmed – at the time or afterwards? *See below
   - o Yes
   - o No

6. Is it possible that any service outages you have suffered in the last two years was caused by a cyber attack – such as ransomware, DDoS attack, or malware? *See below
   - o Yes
   - o No

7. Are you aware that Distributed Denial of Service (DDoS) attacks are a significant contribution to service interruptions, outages and downtime? *See below
   - o Yes
   - o No

*We are withholding this information under Section 24 (1) (National Security) of the Freedom of Information Act and Section 31(1) (a) of the Act (law enforcement) which covers all aspects of the prevention and detection of crime. Both section 24 and 31 are qualified exemptions, which means they are subject to a public interest test. Under Section 24 (1) we consider that disclosure would not be in the interest of the Trusts' security. Disclosing details about security, could allow individuals to assess the strength of our defences. The public interest arguments against disclosure under Section 31 (1) (a) are similar. Any attempt to hack into an IT system is a criminal offence. Disclosing this information could aid a criminal who was intent on launching an attack on the Department's ICT systems and could expose the Trust to potential threats such as targeted e-crime. We acknowledge the public interest in openness and transparency.

We also appreciate that disclosure of this information would provide assurance that we are appropriately protecting our IT infrastructure while ensuring value for money. However, for the reasons outlined we have concluded that the balance of public interest favours withholding this information.