NHS
Solent
NHS Trust

FOI_1222_2023-24 – FOI Request Concerning – Cybersecurity and DSPT Strategy

1. **What software/tools/products do you currently have in place to securely: manage privileged user access/administrator accounts/manage endpoints**

   3rd Party suppliers provide the platforms to manage those as follows:
   Privileged User accounts: AD/Azure AD
   Admin Accounts: Azure Privileged Identity Management (PIM) | Endpoints: Intune/SCCM

2. **How do you comply with the DSPT requirements surrounding privileged access/managing administrator accounts?**

   The Trust is compliant

3. **How many data breaches/data security incidents have you suffered as a result of accidental or deliberate misuse of access credentials in the last 3 years? Please break these down year by year. (*A data breach is a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data).**

   The following were reported to the ICO
   2020/21 – 0
   2021/22 – 0
   2022/23 – 1

4. **When carrying out and completing DSPT assessments, do you have a dedicated employee/s for this, and can you specify the job title/s of those responsible, how long does it take, and how many staff are involved?**

   Head of Information Governance & Digital Security

5. **How beneficial and efficient do you think DSPT assessments are as a means of assessing data security best practice?**

   Please be advised that FOI Act 2000 does not cover the collation of opinion, but rather information held. Therefore, this question is exempt.

6. **What actions are you taking to ensure your organisation complies with the new NHS Cyber Strategy?**

   The Trust has recently appointed a new Cyber Security Manager, who will undertake an assessment of this.

7. **What security tech/software/tools does your organisation use to help you comply with DSPT and cyber resilience in general? For example, MFA, email filtering, Privileged Access Management, Anti-Virus, back-up protection, endpoint management**

   All of the above

8. **Do you keep an accurate log of who has privileged user access to each, IT system, device, application and database – including third party suppliers - and how do you manage this?**

   Yes, which is managed through our starter’s leavers process