Freedom of Information Request: 0699

1. **Does the organisation have training that covers:**
    1. **Recognising and reporting Phishing emails** Yes.
    2. **Recognising Tailgating and how to respond (challenging strangers, checking for ID etc)** Yes.
    3. **Disposal of confidential information** Yes.
    4. **Dangers of using USB sticks being given away or finding one that looks like it has been dropped** Yes.

2. **Does the organisation allow the use of USB sticks?**

    Yes.

3. **Does the organisation deliver specialised training to key staff (those staff that could be targeted as part of a phishing email campaign, ie finance, execs etc)?**

    No.

4. **Does the organisation perform confidentiality audits as per the Data Security & Protection Toolkit?**

    Yes.

    Can you also answer relating to the audits:

    1. **Where the audits are undertaken would these be organised with the local team manager or the head of department ie the director etc?**

        No, audits are normally undertaken as unannounced audits. Occasionally departments would be informed prior to the audit.

    2. **Would an audit ever be carried out unannounced?**

        Yes.

    3. **Do you have a policy / procedure of how to conduct the audit? – if so can you supply a copy.**

        We do not have a policy/procedure. However, audits are normally unannounced, with two auditors from the Information Governance team. The audits tend to focus on environmental aspects such as the following:

        - Locked/unlocked computers
        - Tailgating into areas
        - Accessibility of paper records
        - Were auditors approached or challenged by staff
        - Is confidential information displayed on noticeboards

The audits are then reported back to the relevant area using the report below.

4. **Do you record the results on a checklist / report and return the key contact? – if so can you supply a blank copy.**

   Yes – see attached documents.

5. **Does the organisation have confidential waste receptacles placed through the entire organisation and are they regularly emptied?**

   Yes

6. **Does the organisations Exec board receive board level training relating to Cyber Awareness?**

   The Executive team receive Information Governance training on an annual basis.

7. **How does the organisation provide Data Security & Protection Training to staff, does the organisation use (please select all the options that are applicable):**

a. Third party application package	☐
b. Third party Trainer / class room	☐
c. eLearning for Health Data Security Awareness	X☐
d. In house developed package	X☐
e. Combination of any of the above	X☐