FOI 0154/2021 Response

Request

1. Does the Trust have appointed Information Asset Owner's (IAO's)

2. If the answer to Q1 is yes, how often are they trained, when was the training last delivered and who is responsible for organising the training? (as in, the person)

3. Are you or have you considered becoming ISO 27001 compliant or certified? If so whom is responsible for the project? (as in, the person)

4. How is 3rd Party supplier risk assurance managed, in particular the risk in the areas of data protection and information security and who is responsible for this, if relevant (as in, the person)

5. When did you last conduct a Physical Security risk assessment of the Trust's Estate(s) and Building(s), and who is responsible for managing risk in this area? (as in, the person)

*****Clarification has been sought from the Requester to confirm what information they are seeking for question4.

The Requester has confirmed that they would like to know when engaging with a third party suppliers, how does the Trust ensure that we safely, correctly and securely handle information shared between each party, and how is any identified risk in these areas managed'.

For example, Data Privacy Impact Assessments and Data Sharing Agreements.

Response

1. Does the Trust have appointed Information Asset Owner's (IAO's)

Yes

2. If the answer to Q1 is yes, how often are they trained, when was the training last delivered and who is responsible for organising the training? (as in, the person)

Please note the following:

- An Asset owner (AO) is trained once they become the owner of an asset.

- The AO training and ongoing support is delivered and available from the Trust's Information Governance Team and the Trust's ICT Team on an ad hoc basis, or when there is a new AO/ new asset.

3. Are you or have you considered becoming ISO 27001 compliant or certified? If so, who is responsible for the project? (as in, the person)

Not Recorded.

4. How is 3rd Party supplier risk assurance managed, in particular the risk in the areas of data protection and information security and who is responsible for this, if relevant (as in, the person)

The Trust have the following suite of documents completed by AO's that address the areas of data protection, information security, and ensures robust information governance when sharing information with third parties:

- Data Protection Impact Assessments (DPIA) Screening questions
- Data Protection Impact Assessments (DPIA)
- Business Continuity Plan (BCP)
- System Level Security Plan (SLSP)
- Information Risk Assessments
- Information Flow Mapping
- Confidentiality audit and summary report
- Information Sharing Protocol (ISP)

5. When did you last conduct a Physical Security risk assessment of the Trust's Estate(s) and Building(s), and who is responsible for managing risk in this area? (as in, the person).

The Trust is unable to disclose the name of the staff member responsible for managing Physical Security risk assessments of Trust sites. This is because the Trust does not routinely release staff members information for those under a band 8c role.

The Trust therefore, rely on exemption Section 40 of the Freedom of Information Act 2000 to deny this aspect of your request.

However, the Trust can confirm that the Local Security Management Specialist is responsible for managing Physical Security risk assessments.

The Trust is also unable to provide a specific date of when the last Physical Security risk assessment was conducted. This is because there is a rolling annual programme of security audits that is carried

out for each Trust site, and therefore some Physical Security risk assessments would have been completed at various times within the last 12 months or longer