FOI Request Response information

FOI request reference:	2016/223
Date request received:	22/08/2016
Date request responded to:	15/09/2016
Category:	IM&T
Tags:	IT, security, IG, Information, Governance

Request Detail:

1. How many staff do you currently have?

2. How many IT network accounts do you have for logging on to the network currently?

3. How many Full Time Equivalent (FTE) staff (including vacancies) do you have that are responsible for Information Governance (IG)?

4. How many FTE staff (including vacancies) do you have that are responsible for information/IT security? (If they are the same FTE as those responsible for IG just say that)?

5. Please state the make/model version number (as applicable) for the following IT security controls on your IT network;

    a. Desktop firewall
    b. Anti-Malware
    c. Device Control (e.g. endpoint protection to prevent exfiltration of data)
    d. Network Vulnerability
    e. Web Proxy
    f. Network Access Control
    g. Intruder Prevention System (IPS)
    h. Intruder Detection system (IDS)
    i. Firewall activity logging/monitoring
    j. Active Directory activity logging/monitoring
    k. Security Incident and Event Management (SIEM)

6. Date (month/year) of last penetration test carried out on any part of your organisation's IT infrastructure (whether that is hosted infrastructure or not)?

Response Detail:

The Trust response to your recent FOI request is as follows:

1. How many staff do you currently have?

6697

2. How many IT network accounts do you have for logging on to the network currently?

~7000

3. How many Full Time Equivalent (FTE) staff (including vacancies) do you have that are responsible for Information Governance (IG)?

2 FTE

4. How many FTE staff (including vacancies) do you have that are responsible for information/IT security? (If they are the same FTE as those responsible for IG just say that)?

1 FTE

5. Please state the make/model version number (as applicable) for the following IT security controls on your IT network;

a. Desktop firewall
b. Anti-Malware
c. Device Control (e.g. endpoint protection to prevent exfiltration of data)
d. Network Vulnerability
e. Web Proxy
f. Network Access Control
g. Intruder Prevention System (IPS)
h. Intruder Detection system (IDS)
i. Firewall activity logging/monitoring
j. Active Directory activity logging/monitoring
k. Security Incident and Event Management (SIEM)

In the interests of IT security, we are not at liberty to discuss the above other than to say we have these measures in place.

6. Date (month/year) of last penetration test carried out on any part of your organisation's IT infrastructure (whether that is hosted infrastructure or not)?

Testing carried out August 2016 for all systems hosted by LCFT