

Date: 21/04/2016

FREEDOM OF INFORMATION REQUEST 012708 – Ransomware

1. Has any of the Trust's IT equipment been infected by so-called "ransomware" (malicious software that encrypts files and then demands payment in order for the files to be decrypted; examples include Cryptolocker, Cryptowall, CryptoDefense, Locky)
2. If so, how many infections have been detected?
3. If so, what information was affected?
4. If so, has the Trust paid money in order to have the files decrypted?
5. If so, how much money was paid and via what means?
Information required for the last 3 years

The Trust is using Exemption 43 (2) applied given the Trust would consider information relating to potential information security vulnerabilities commercially sensitive. The public interest test set out in section 2(2)(b) supports application of exemption 43 (2) given there is a greater public interest in maintaining the exemption 43 (2) outweighing the public interest in disclosure to ensure the Trust is not targeted by cyber criminals through social engineering emails to target Trust staff.