Our Ref: **005781/15**

Freedom of Information Section
Nottinghamshire Police HQ
Sherwood Lodge, Arnold
Nottingham NG5 8PP

Tel: 101
Ext 800 2507
Fax: 0115 967 2896

02 November 2015

Request under the Freedom of Information Act 2000 (FOIA)

I write in connection with your request for information, which was received by Nottinghamshire Police on 27/08/2015.

Following receipt of your request searches were conducted within Nottinghamshire Police to locate the information you require.

Please find below answers to your questions:-

RESPONSE

Under S 1 (1) (a) of the Freedom of Information Act 2000 (FOIA), I can confirm that Nottinghamshire Police does hold the information you have requested.

I am writing to you to request information about the cyber security practices across your corporate network, and other networks that you may use. This request is applicable under the Freedom of Information Act 2000.

If you please, I would initially like you to establish contextualising information about the corporate network(s) that you use.

1a. May you confirm who deployed these networks and their names (i.e. in the instance of Sunderland City Council's corporate network, it has been reported that the network was deployed by BT: http://www.telecompaper.com/news/bt-delivers-corporate-network-for-sunderland-city-council--819112)

Nottinghamshire Police do not currently have a single contract for its IT network. All our links are on single contracts on a per link basis which per purchased of the old government framework.

We have three suppliers of infrastructure, BT, Virgin Media and MLL Telecom. These suppliers were all on the old framework, along with 9 others suppliers, all of which were invited to reply.

The requirement for each circuit was submitted to the framework and Nottinghamshire Police awarded based purely on price.

1b. May you provide me with copies of the tender award documents (these may be 1b.1 ¿ the invitation to tender, and 1b.2 ¿ the final contract, and 1b.3 etcetera, wherein they display an evaluation of the tender process) relating to the deployment of your corporate network.

The requested information above is exempt from disclosure under Section 43(2) of the Act: Commercial Interests.

43. *– (2) Information is exempt information if its disclosure under this Act would, or would be likely to, prejudice the commercial interests of any person (including the public authority holding it).*

Section 43 is a class based qualified exemption which requires a public interest test to be conducted to consider whether the public interest lies in favour of disclosing the information or in maintaining the exemption. Please see below.

Section 43(2) of the FOIA provides a qualified exemption on the disclosure of information where the information would be likely to prejudice the commercial interests of any person. The information Commissioners guidance indicates that commercial interests for the purpose of applying Section 43(2) includes information held by public authorities in the context of procuring goods and services which include information regarding the budget made available by the public authority for obtaining goods or services.

Factors Favouring Disclosure
The public have an interest in knowing how public funds are spent in respect of procurement/provision of services. This would demonstrate an openness and transparency and would give the public the opportunity to judge whether the force was using public funds appropriately and would allow them to debate any issues.

Factors Favouring Non-Disclosure
Companies compete by offering something different from their rivals. The difference will often be reflected in their price and may also relate to the quality or specification of the product or service they offer. Disclosure of the requested information would allow other companies to use this knowledge to undercut rivals which, could then impact on the future quality and service the force receives.

Information identifying this unique element is commercially sensitive as it may reveal information regarding forward spending plans which would be likely to prejudice future contract negotiations with suppliers.

Balance Test

Giving due consideration to all the points above, whilst I feel that the public have a right to know how public monies are spent, there is potential harm to both the companies that supply this service to the force and the Force itself as well as potential breaches of confidentiality also being a significant consideration. Therefore, on balance I feel that non-disclosure of the information outweighs disclosure and it is therefore in the public interest to withhold this information under Section 43(2).

This letter constitutes a refusal notice under Section 17 (1) of the Freedom of Information Act 2000 with Section 43(2) of the act being applied.

1c. I would like to be able to contextualise the successful bid by understanding how many bids you received and how they were evaluated. If you may, I would like you to provide this as a table in a spread sheet format, the rows of which would list those tendering and the columns of which would list the evaluation criteria. If such a document does not exist, please provide me with a facsimile which might only include the financial range of the bids, in a spread sheet format.

No information held. Such a table is not held by Nottinghamshire Police. As above, the successful bid was awarded purely on price.

This information is of obvious value in understanding the deployment of your corporate network which is necessary information to complement the following questions regarding your security practices.

2a. I would like to know what anti-virus and anti-malware solutions you use, this information would be the names of the solutions, the locations at which they are installed, and the names of the companies who have provided them.

We currently use McAfee and Microsoft Endpoint Protection. The solutions are deployed force wide. We obtain the software through our normal software reseller and deploy them using our internal IS staff. We follow the standard government procurement frameworks when purchasing these solutions.

2b. May you provide me with copies of the tender award documents for these solutions, as per 1b. Here I would like to understand the procurement process for these solutions and the degrees to which they are expected to provide security. I ask for these as I am aware the solutions may be purchased alone, while also an AV solution is often provided as part of a Microsoft Enterprise Agreement, for instance.

The requested information above is exempt from disclosure under Section 43(2) of the Act: Commercial Interests.

43. *– (2) Information is exempt information if its disclosure under this Act would, or would be likely to, prejudice the commercial interests of any person (including the public authority holding it).*

Section 43 is a class based qualified exemption which requires a public interest test to be conducted to consider whether the public interest lies in favour of disclosing the information or in maintaining the exemption. Please see below.

Section 43(2) of the FOIA provides a qualified exemption on the disclosure of information where the information would be likely to prejudice the commercial interests of any person. The information Commissioners guidance indicates that commercial interests for the purpose of applying Section 43(2) includes information held by public authorities in the context of procuring goods and services which include information regarding the budget made available by the public authority for obtaining goods or services.

Factors Favouring Disclosure
The public have an interest in knowing how public funds are spent in respect of procurement/provision of services. This would demonstrate an openness and transparency and would give the public the opportunity to judge whether the force was using public funds appropriately and would allow them to debate any issues.

Factors Favouring Non-Disclosure
Companies compete by offering something different from their rivals. The difference will often be reflected in their price and may also relate to the quality or specification of the product or service they offer. Disclosure of the requested information would allow other companies to use this knowledge to undercut rivals which, could then impact on the future quality and service the force receives.

Information identifying this unique element is commercially sensitive as it may reveal information regarding forward spending plans which would be likely to prejudice future contract negotiations with suppliers.

Balance Test

Giving due consideration to all the points above, whilst I feel that the public have a right to know how public monies are spent, there is potential harm to both the companies that supply this service to the force and the Force itself as well as potential breaches of confidentiality also being a significant consideration. Therefore, on balance I feel that non-disclosure of the information outweighs disclosure and it is therefore in the public interest to withhold this information under Section 43(2).

This letter constitutes a refusal notice under Section 17 (1) of the Freedom of Information Act 2000 with Section 43(2) of the act being applied.

2c. May you confirm the date these solutions have been running for.

McAfee has been deployed for 8 years. The Microsoft solution has been running for approximately 2 years

2d. May you confirm the number and type of machines across which these solutions are installed.

Microsoft is deployed across our end user devices (approx. 4000). McAfee is deployed on our server estate (approx. 300)

2e. May you inform of whether there is an employee responsible for maintaining these solutions, and whether this employee does so exclusively. If you may also explain to me their title and pay range in pounds sterling.

The maintenance of these systems does not fall under any one person's responsibility. It is maintained by the IS department operations team.

I am also interested in the threats that you are facing.

3a. May you inform me of the number of malware alerts that your AV solutions detected in the past twelve months.

3b. Most solutions will provide alerts when it comes to malware detections, may you inform me of the number of alerts your solutions have provided, by solution.
These alerts should be held on a database which provides a high degree of granularity in recording the causes of the alerts.

3b.2 May you provide me with a copy of this granular information (preferably in spread sheet format) for the period covering the last twelve months, or shorter if not applicable.
number of infections

3c. I also wish to receive information about the number of infections that have occurred in the last twelve months, and in what areas, and on what machines these occurred.

3d. I would like to know at what account level these infections occurred.

3e. I would like to know how many instances were there in which these infections were not contained, but spread to another part of the network.

3f. I would like to know what the entry-point of these infections was, in each case.

3g. I would like a list of the number and type of unauthorised accesses within your networks.

3h. I would like to know how many of these were classified as personal data incidents, and how many were reported to the Information Commissioner's Office.

Nottinghamshire Police can neither confirm nor deny that information is held relevant to your request as the duty in Section 1(1)(a) of the Freedom of Information Act 2000 does not apply by virtue of the following exemptions:

Section 23(5) Information supplied by or concerning certain Security Bodies
Section 24(2) National Security
Section 31(3) Law Enforcement

Section 23 is a class based absolute exemption and there is no requirement to evidence the harm or articulate public interest considerations to the applicant.

With Sections 24 and 31 being prejudice based qualified exemptions there is a requirement to articulate the harm that would be caused in confirming or not whether information is held as well as considering the public interest.

Harm in Confirming or Denying that Information is held
To confirm or deny whether any other information is held regarding your request would identify vulnerable computer systems and provide a confirmation of whether such attacks have or have not taken place.
In order to counter criminal and terrorist behaviour it is vital that the police and other agencies have the ability to work together, where necessary covertly, in order to obtain intelligence within current legislative frameworks to ensure the arrest and prosecution of offenders who commit or plan to commit acts of terrorism, whereby their modus operandi may involve 'hacking' into secure databases.
In order to achieve this goal, it is vitally important that information sharing takes place with other police forces and security bodies within the United Kingdom in order to support counter-terrorism measures in the fight to deprive terrorist networks of their ability to commit crime.
To confirm or deny specific details of any breaches of information technology and security would be extremely useful to those involved in terrorist activity as it would enable them to map vulnerable information security databases.

Public Interest Considerations

<u>Section 24(2) National Security</u>
Factors favour complying with Section 1(1)(a) confirming that information is held
The public are entitled to know how public funds are spent and how resources are distributed within an area of policing. To confirm where information security breaches have occurred would enable the general public to hold Nottinghamshire Police to account ensuring all such breaches are recorded and investigated appropriately. In the current financial climate of cuts and with the call for transparency of public spending this would enable improved public debate.

Factors against complying with Section 1(1)(a) confirming or denying that any other information is held

Security measures are put in place to protect the community that we serve. As evidenced within the harm to confirm where specific breaches have occurred would highlight to terrorists and individuals intent on carrying out criminal activity vulnerabilities within Nottinghamshire Police.
Taking into account the current security climate within the United Kingdom, no information (such as the citing of an exemption which confirms information pertinent to this request is held, or conversely, stating 'no information is held') which may aid a terrorist should be disclosed. To what extent this information may aid a terrorist is unknown, but it is clear that it will have an impact on a force's ability to monitor terrorist activity.
Irrespective of what information is or isn't held, the public entrust the Police Service to make appropriate decisions with regard to their safety and protection and the only way of reducing risk is to be cautious with what is placed into the public domain.
The cumulative effect of terrorists gathering information from various sources would be even more impactive when linked to other information gathered from various sources about terrorism. The more information disclosed over time will give a more detailed account of the tactical infrastructure of not only a force area but also the country as a whole.
Any incident that results from such a disclosure would by default affect National Security.

Section 31 – Law Enforcement
Factors favouring complying with Section 1(1)(a) confirming that information is held

Confirmation that information exists relevant to this request would lead to a better informed public which may encourage individuals to provide intelligence in order to reduce such security breaches.

Factors against complying with Section 1(1)(a) neither confirming nor denying that information is held

Confirmation or denial that information is held in this case would suggest Nottinghamshire Police take their responsibility to protect information and information systems from unauthorised access, destruction, etc., dismissively and inappropriately.

Balancing Test
The points above highlight the merits of confirming or denying the requested information exists. The Police Service is charged with enforcing the law, preventing and detecting crime and protecting the communities we serve. As part of that policing purpose, information is gathered which can be highly sensitive relating to high profile investigative activity.

Weakening the mechanisms used to monitor any type of criminal activity, and specifically terrorist activity would place the security of the country at an increased level of danger.

In order to comply with statutory requirements and to meet the NPCC's expectations of the Police Service with regard to the management of information security a national policy created by the College of Policing titled Information Assurance has been put in place. This policy has been constructed to ensure the delivery of core operational policing by providing appropriate and consistent protection for the information assets of member organisations. A copy of this can be found at the below link:

https://www.app.college.police.uk/app-content/information-management/information-assurance/

This is linked to the old ACPO Information Systems Community Security Policy:

http://library.college.police.uk/docs/APPref/ACPO-ACPOS-2009-Information-Systems.pdf

In addition anything that places that confidence at risk, no matter how generic, would undermine any trust or confidence individuals have in the Police Service.
Therefore, at this moment in time, it is our opinion that for these issues the balance test favours neither confirming nor denying that information is held. No inference can be drawn from this refusal that information is or isn't held

Finally, I would like to ask about your security maintenance policies.

4a. If one exists, may you explain your password policy and its enforcement.
As below

4b. If one exists, may you explain your log-on policy and its enforcement.

All log on attempts are logged, successful logons are stored against the users paycode which record the Date, Time and Workstation.
These logs are used as part of our identity and authentication process if a customer contacts us for a LAN password reset.

4c. If one exists, may you explain your email policy and its enforcement.

Our Email policy limits the amount of receipts per email to a set number, it limits the size of each email to a set size, our mailboxes are quoted to a set size, all emails go through scanning and filtering software including a different antivirus supplier to what is on workstations before being received or sent by our mail servers.

4d. If one exists, may you explain your device policy (i.e. nothing from home) and its enforcement.

We follow Home Office Guidelines and acceptable use policies

4e. May you clarify whether you store and or process bank card data?

No

4f. May you clarify whether you are PCI compliant?

NA

Complaints Rights
Your attention is drawn to the enclosed review procedure, which details your right of complaint.

Copyright
Nottinghamshire Police in complying with their statutory duty under Sections 1 and 11 of the Freedom of Information Act 2000 (FOIA) to release the enclosed information will not breach the Copyright, Designs and Patents Act 1988. However, the rights of the copyright owner of the enclosed information will continue to be protected by law. Applications for the copyright owner's written permission to reproduce any part of the attached information should be addressed to the Force Solicitor, Nottinghamshire Police, Force Headquarters, Sherwood Lodge, Arnold, Nottinghamshire, NG5 8PP.

I would like to take this opportunity to thank you for your interest in Nottinghamshire Police.

Should you have any further enquiries concerning this matter, please write or contact the Freedom of Information Officer on telephone number 0115 9672507 or e-mail freedomofinformation@Nottinghamshire.pnn.police.uk quoting the above reference number.

Yours sincerely

Disclosure Officer

Are you dissatisfied with your response?

Nottinghamshire Police has a duty to implement a complaints process in relation to Freedom of Information Act requests. If you are not content with our response, you may appeal, this process is known as an 'Internal Review'

Internal reviews are intended to be a fair and impartial means of reviewing the original request process.

You can appeal about your request if you:-

- Disagree with the Forces interpretation of your request;
- Believe the Force hold more information than has been disclosed to you;
- Disagree with the application of exemptions;

How do I appeal?

All appeals should be made in writing and sent to:-

Information Management
Nottinghamshire Police
Force Headquarters
Sherwood Lodge
Arnold
Notts
NG5 8PP

or alternatively freedomofinformation@nottinghamshire.pnn.police.uk

To deal with your appeal as quickly as possible please provide the unique identification number provided with your response and the reasons for your appeal.

Once we have received your request for appeal, your FOI response will be reviewed in full to identify any problems in the disclosure.

The review will be undertaken by someone different from, and preferably senior to, the original decision maker and this should be completed within 20 working days from receipt, in exceptional circumstances it may be extended by a further 20 working days.

What if I'm still not satisfied?

You can appeal to the Information Commissioner. You can contact the Information Commissioner Office at the following:-

Information Commissioner's Office
Wycliffe House
Water Lane
Wilmslow
Cheshire
SK9 5AF

Tel: 0303 123 1113 (local rate) or 01625 545 745 (national rate)

E-mail: casework@ico.org.uk