By e-mail: Barry Salmon <request-377118-78bcc0b8@whatdotheyknow.com>

Office of the University Secretary
4 West
University of Bath
Claverton Down
Bath
BA2 7AY

16 January 2017

Dear Mr Salmon

Request for information under the Freedom of Information Act (FOIA), 2000 – 2016/246

Your request for information was received on 14 December 2016 and handled under the provisions of the Freedom of Information Act, 2000. It is reproduced below for your reference:

"1. What is your policy for using personally owned devices accessing IT applications?
- *We allow access to both student and staff with personal and corporate devices*
- *We allow access to staff with personal and corporate devices*
- *We only allow access to corporate devices*

2. Do you have visibility into devices that are used to access University applications?
- *Yes*
- *No*

3. Do you use multi-factor authentication (such as a hardware token, software code generated by a mobile phone app, or an SMS code) to access IT applications? Please select one answer only.

- *Yes, we use multi-factor authentication for all access by students, faculty and staff onto the devices, apps, intranet or IT network*
- *Yes, we only use it for access to all sensitive data such as financial payments, grades and personally identifiable data (PII) data held on the network*
- *No, we just use single factor authentication today*
- *We just use single factor authentication today but we are planning on implementing multi-factor authentication in the next 12 months.*

4. What security risks in personal devices are you most worried about when accessing University applications?
- *Out of date software. Ex: Operating systems, browsers*
- *Physical security of devices. Ex: passcode lock*
- *Jailbroken / Rooted devices*
- *Others (Please specify)*

5. What is your policy regarding patching and updating digital devices, operating systems and apps which access your corporate network? Please select one answer only.

- *We implement all patches/upgrades within 48 hours from notification*
- *We implement all patches/upgrades within 7 days of notification*
- *We implement all patches/upgrades within 30 days of notification*
- *It is impossible for us to maintain all devices, operating systems and apps at the latest version and patches/upgrades typically take longer than 30 days to implement.*
- *We outsource the patching and upgrade of all our devices and systems to a third party*

6. Has your university ever been the victim of a phishing attack (where an individual is duped into disclosing their login, password or credit card details via an email purporting to be from a trusted source)? Please select one answer

- *Yes*
- *No*
- *Don't know*

6a. If yes, how often have you experienced a phishing attack in the last 12 months? Please select one answer.

- *0-5 times*
- *6-10 times*
- *11-50 times*
- *51+ times*
- *Don't know*

6b. If yes, which is the most common target of the phishing campaigns? (please select one)

- *Students*
- *Lecturers/faculty staff*
- *Employees*
- *Other (please specify)*

6c. What type of data was being targeted? (select all that apply)

- *Student personally identifiable information (PII) e.g. date of birth. National Insurance Nos.*
- *Employee PII*
- *Financial/payroll data*
- *Research/patents*
- *Other (please specify)*

6d. Did you identify the attackers and, if so, are they? (select all that apply).

- *Organised cyber-criminals*
- *Opportunistic hackers (non-organised)*
- *Political hacktivists*
- *Disgruntled employees/former employees*
- *Disgruntled students/former students*
- *State sponsored hackers*
- *Other (please specify)*

Section 1(1) usually entitles you to be told whether the requested information is held and have that information provided to you unless it is judged to be exempt from disclosure. The University is able to provide you with the following information.

Q1. We allow access to both student and staff with personal and corporate devices.

Q2-5. Exempt pursuant to s.31(1)(a) and s.43(2).

6. Yes

6a-c. Exempt pursuant to s.31(1)(a) and s.43(2)

6d. Exempt pursuant to s.31(1)(a) , s.31(1)(b) and s.43(2)

Exempt information

Some information is exempt from disclosure under section 31(1)(a) of the FOIA, which applies when disclosure would or would be likely to prejudice the prevention or detection of crime.

In this instance the University considers that disclosure of this information into the public domain would be likely to prejudice the prevention and/or detection of crime by providing suitably motivated perpetrators with knowledge that could be used to compromise the security of the University's IT infrastructure. Disclosure of this information concerning cybersecurity arrangements and perceived risks to these arrangements would provide these perpetrators with valuable intelligence and thus increase the University's subsequent vulnerability to attack. For example disclosure of patching policies and authentication arrangements would be valuable to individuals with an intent to circumvent these security measures. Similarly, disclosure of perceived risks would create an obvious increased threat of attempted attacks. In relation to question 6d the University also considers that section 31(1)(b) would be engaged, which applies when disclosure would or would be likely to prejudice the apprehension or prosecution of offenders. Disclosure would enable attackers and/or potential attackers to identify whether their activities had thus far been detected. Section 31 is a qualified exemption subject to the application of a public interest test. The University acknowledges a general public interest in favour of transparency. However it has concluded that there is an overriding public interest in not prejudicing the prevention/detection of crime and maintaining the security of the University's business-critical IT infrastructure (for example protecting the personal data of thousands of staff and students), which therefore weighs strongly in favour of maintaining the exemption in this instance.

The University has also concluded that the exempt material engages section 43(2) of the FOIA which applies when disclosure would or would be likely to prejudice the commercial interests of any organisation (including the University itself). In this instance disclosure would be likely to prejudice the University's own commercial interests. Disclosure of details of IT security arrangements that could be used to undermine those arrangements would have a detrimental impact upon the University's commercial interests (for example the financial and reputational impact of potential data loss). Section 43(2) is a qualified exemption subject to the consideration of the public interest. The University acknowledges a general public interest in favour of transparency concerning how it is managed. However it considers that this public interest is met by information it places in the public domain such as relevant IT Security Policies. Moreover, it has concluded that in this instance the public interest weighs in favour of maintaining the exemption. The likely prejudice to the commercial interests of the University, its staff and students would not be in the public interest in the context of an institution that conducts teaching and research for the public benefit.

If you are dissatisfied with any aspect of how your request was handled you may ask the University to conduct an internal review. A request for an internal review must be submitted within 40 working days of receipt by you of this response. Requests received outside this period will only be considered at the University's discretion and where there is a valid reason to do so. Applications for internal review should be addressed in writing to:

University Secretary
University of Bath
Claverton Down
Bath, BA2 7AY or e-mail M.G.W.Humphriss@bath.ac.uk.

If you still feel dissatisfied following the outcome of the internal review you may appeal to the Information Commissioner's Office (ICO):

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

Further details of this process are available via the following link:

https://ico.org.uk/concerns/getting/

Please note that the Information Commissioner will only consider appeals once the internal review process has been completed.

Yours sincerely

James Button
Freedom of Information Officer