Emily Quick
request-372xxxxxxxxxxx@xxxxxxxxxxxxxx.xxx

30 November 2016

Our Ref: FOI 2016/379 – F0759559

Dear Ms Quick,

Re: Freedom of Information (Scotland) Act 2002 – Request for Information

Thank you for your email which was received by the University on 22 November 2016 timed 11:18 hours, requesting the following information:

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- **Out of date software.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)**

DATA PROTECTION AND FREEDOM OF INFORMATION OFFICE
University of Glasgow, Tay House, Glasgow G12 8QQ
Data Protection: Telephone: 0141-330-3111 *E-Mail: x@xx*
Freedom of Information: Telephone: 0141-330-2523 *E-Mail: foi@gla*.ac.uk
The University of Glasgow, charity number SC004401

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)**

University's Response

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**

The University allows access to both students and staff with personal and corporate devices.

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

The University has visibility into some devices, but not all.

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)**

The University considers that the disclosure of the information requested for questions 3 and 4 would, or would be likely to, prejudice substantially the effective conduct of public affairs. It is imperative that the University's IT infrastructure is secure and to release details of the specific measures in place used to maintain that security could seriously adversely affect the

University's effective operation as a provider of higher education in Scotland. The University therefore considers that the "harm test", as required by Section 30(c), is met.

Section 30 of FOISA does not provide an absolute exemption to the general entitlement to information. The University has therefore considered whether, notwithstanding the exemption, it is in the public interest to release the information.

The University has considered the public interest by applying the "public interest test". That is, the University has balanced whether the release of the information is in the public interest against whether disclosure would otherwise prejudice substantially, or be likely to prejudice substantially the effective conduct of public affairs. The view of the Office of the Scottish Information Commissioner (OSIC), in its advice on the application of the "public interest test", is that the public interest should not be interpreted as "of interest to the public". That is, the potential release of the information must be in the interests of the public and not merely of individual interest. The public interest in the disclosure of the information in the manner requested is slight. The University of Glasgow operates in a highly competitive environment and the public interest is in ensuring the continuing success and operational effectiveness of the University. The University is understandably concerned that the release of the requested information could endanger the security of the University's IT infrastructure, systems and information. Knowledge of the security measures in use and of the attending security risk concerns could allow hackers to target attacks at the University's systems and security measures. Such attacks on the University's computing infrastructure would cause major disruption, possibly resulting in an effective shutdown of the University's networked systems and consequently a real and significant burden in terms of expense and distraction to the University and its staff. Additionally, the University could suffer, both in reputation and monetarily, if such an attack resulted in a breach in terms of the Data Protection Act 1998. The University considers that the disclosure of the requested information would therefore prejudice substantially, or be likely to prejudice substantially, the University's ability to effectively conduct its affairs.

The University therefore concludes that the "public interest test", as required when applying Section 30(c) of FOISA, is met. The public interest in withholding the information is greater than the public interest in its release.

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**

Operating system and application security patches are applied in a timely manner. However, different systems and devices have different patch schedules, so there is no single "time in days" patch interval figure for everything.

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)**

The University considers that the disclosure of the information requested in question 6 and its sub-questions would, or would be likely to, prejudice substantially the effective conduct of public affairs. It is imperative that the University's IT infrastructure is secure and to release details of attacks on that infrastructure could aid future attack attempts and therefore seriously adversely affect the University's effective operation as a provider of higher education in Scotland. The University therefore considers that the "harm test", as required by Section 30(c), is met.

Section 30 of FOISA does not provide an absolute exemption to the general entitlement to information. The University has therefore considered whether, notwithstanding the exemption, it is in the public interest to release the information.

The University has considered the public interest by applying the "public interest test". That is, the University has balanced whether the release of the information is in the public interest against whether disclosure would otherwise prejudice substantially, or be likely to prejudice substantially the effective conduct of public affairs. The view of the Office of the Scottish Information Commissioner (OSIC), in its advice on the application of the "public interest test", is that the public interest should not be interpreted as "of interest to the public". That is, the potential release of the information must be in the interests of the public and not merely of individual interest. The public interest in the disclosure of the information in the manner requested is slight. The University of Glasgow operates in a highly competitive environment and the public interest is in ensuring the continuing success and operational effectiveness of the University. The University is understandably concerned that the release of the requested information could endanger the security of the University's IT infrastructure, systems and information. Knowledge of whether and how often certain attacks may have occurred at the University, and against which classes of victim, could allow hackers to formulate additional attacks based on these details. Such attacks on the University's computing infrastructure would cause major disruption, possibly resulting in an effective shutdown of the University's networked systems and consequently a real and significant burden in terms of expense and distraction to the University and its staff. Additionally, the University could suffer, both in reputation and monetarily, if such an attack resulted in a breach in terms of the Data Protection Act 1998. The University therefore considers that the disclosure of the requested information would therefore prejudice substantially, or be likely to prejudice substantially, the University's ability to effectively conduct its affairs.

The University therefore concludes that the "public interest test", as required when applying Section 30(c) of FOISA, is met. The public interest in withholding the information is greater than the public interest in its release.

The supply of documents under the terms of the Freedom of Information (Scotland) Act 2002 does not give the applicant or whoever receives the information any right to re-use it in such a way that might infringe the Copyright, Designs and Patents Act 1988 (for example, by making multiple copies, publishing or otherwise distributing the information to other individuals and the public). The Freedom of Information (Scotland) Act 2002 (Consequential Modifications) Order 2004 ensured that Section 50 of the Copyright, Designs and Patents Act 1988 ("CDPA") applies to the Freedom of Information (Scotland) Act 2002 ("FOISA").

Breach of copyright law is an actionable offence and the University expressly reserves its rights and remedies available to it pursuant to the CDPA and common law. Further information on copyright is available at the following website:

http://www.ipo.gov.uk/copy.htm

Your right to seek a review

Should you be dissatisfied with the way in which the University has dealt with your request, you have the right to require us to review our actions and decisions. If you wish to request a review, please contact the University Secretary, University Court Office, Gilbert Scott Building, University of Glasgow, Glasgow, Scotland G12 8QQ or e-mail: xxx@xxx.xx.uk within 40 working days. Your request must be in a recordable format (letter, email, audio tape, etc). You will receive a full response to your request for review within 20 working days of its receipt.

If you are dissatisfied with the way in which we have handled your request for review you may ask the Scottish Information Commissioner to review our decision. You must submit your complaint in writing to the Commissioner within 6 months of receiving the response to review letter. The Commissioner may be contacted as follows:

The Scottish Information Commissioner
Kinburn Castle
Doubledykes Road
St Andrews
Fife
KY16 9DS
Telephone: 01334 464610
Fax: 01334 464611
Website www.itspublicknowledge.info
E-mail: enquiries@itspublicknowledge.info

An appeal, on a point of law, to the Court of Session may be made against a decision by the Commissioner.

For further information on the review procedure please refer to (http://www.gla.ac.uk/services/dpfoioffice/policiesandprocedures/foisa-complaintsandreview/) All complaints regarding requests for information will be handled in accordance with this procedure.

Yours sincerely,

Data Protection and Freedom of Information Office