UNIVERSITY OF HULL

University of Hull
Hull, HU6 7RX
United Kingdom
E: dataprotection@hull.ac.uk
w: www.hull.ac.uk

Request Ref: 2707

FOI Request dated **05/09/2022** as follows –

Q1. Please list the number of devices deployed by your organisation for the below list?
Q2. Does your organisation have any plans of refreshing or replacing any of the ICT devices from the below list. If yes, please provide the indicative or projected expenditure in the given format?
Q3. Does your organisation have any plans for developing, refreshing, or replacing any software applications, if so, can you please provide the information in the below format?

Response

Please find attached.

We have added a partial s31(1)(a) exemption to your response as follows -

We are unable to provide the requested information regarding security infrastructure on this occasion, in line with Section 17 of the Act, this response acts as a Refusal Notice. The Act contains a number of exemptions that allow public authorities to withhold certain information from release.

We have applied the following exemption to your request – Section 31 (1)(a) – Law Enforcement.

As with other large organisations; universities are reliant on the smooth running of their IT Networks. Maintaining the security of these networks is a significant challenge for all universities, who are increasingly subject to both general cyber security threats and targeted attempts to obtain information from students/staff. Release of any information under the Act represents a disclosure to the word, and it is our belief that if information was disclosed about security infrastructure devices the university has deployed, a motivated individual or group could use this information to target any potential vulnerabilities, exposing the University's IT systems to various types of unlawful attack, and consequently prejudicing the prevention of criminal activity.

Having determined the aforementioned in that disclosure of this information would expose the University to a real and significant risk of crime, application of S31 (1) Law Enforcement also requires us to consider the public interest in withholding/disclosing the information.

Factors in favour of disclosure –
• Increase public understanding of the University's information technology systems and processes, and how it manages its business.
• Enhancing the transparency and accountability of our cyber security system and about our ability to protect our systems and assets.

Factors against disclosure –
• Protecting the ability of public authorities to protect valuable public assets acquired with public funds.
• There is a strong public interest in not publishing information which might expose the University to cyber-attacks and in preventing criminal activity that could damage the running of the University and the security aspect of the information held.

After considering the above factors, we believe the factors against disclosure outweigh those in favour, and therefore applying Section 31 on this basis.

For future requests you may find it more purposeful to apply outside of the FOI Act and directly to our procurement services, please see following link for relevant details – https://www.hull.ac.uk/work-with-us/more/supplying-our-university/procurement and https://www.hull.ac.uk/work-with-us/more/supplying-our-university/buyer-profile.

S.No
1
2
3
4
5

Q1. Please list the number of devices deployed by your organisation for the below list?

DEVICE TYPE
Desktop PCs
Laptops
Mobile Phones
Personal Digital Assistants (PDAs)
Printers
Multi-Functional Devices (MFDs)
Tablets
Servers (Physical)
Storage Devices (E.g., NAS, SAN, etc.)
Networking Infrastructure (E.g., Switches, Routers, Interfaces, Wireless Access Points, etc.)
Security Infrastructure (E.g., Firewalls, Intrusion Detection Systems (IDS), Virus Monitoring Tools, etc.)

Q2. Does your organisation have any plans of refreshing or replacing any of the ICT devices from the below list. If y

	REPLACE/
IT OR ICT HARDWARE	
Desktop PCs	
Laptops	
Mobile Phones	
Personal Digital Assistants (PDAs)	
Printers	
Multi-Functional Devices (MFDs)	
Tablets	
Servers	
Storage Devices (E.g., NAS, SAN, etc.)	
Networking Infrastructure (E.g., Switches, Routers, Interfaces, Wireless Access Points)	
Security Infrastructure (E.g., Firewalls, Intrusion Detection Systems (IDS), Virus Monitoring Tools)	

Note: If the projected expenditure is not available, list the years when the refresh/replacement is due or planned

Q3. Does your organisation have any plans for developing, refreshing, or replacing any software applications, if so

APPLICATION NAME
Apprenticeship Management System
CRM
ERP
ESM

NUMBER OF DEVICES
4211 Centrall Managed
1860 centrally managed
366
0
70
233
196
85
7
4 core switches, 41 distribution switches, 572 access switches and 1222 APs.
Exempt from disclosure - please see response letter

es, please provide the indicative or projected expenditure in the given format?

'REFRESH PROGRAMME:

EXPENDITURE
2022/23
350k
150k
0
0
0
150k
Tablets are ad-hoc purchases, and tend to be unplanned
30k
Network fully refreshed this year, so no spend predicted in medium term
As above

' for the above devices.

, can you please provide the information in the below format?

MONTH/YEAR
Sep-22
next 18-24 months
next 18-24 months
next 18-24 months

2023/24	2024/25
350k	150k
150k	350k
0	0
450k	