Freedom of Information Act 2000 – Request Reference FoI/24/246
IT Infrastructure

Q1. Can you please list the number of devices deployed by your organisation for the following?	
Device Type	**Number of Devices**
Desktop PCs	9,451
Laptops	5,498
Mobile Phones	138+ and 5,000 mobile handsets
Printers	322 including MFDs
Multi Functional Devices (MFDs)	406
Tablets	700
Physical Servers	Section 31(1)(a)
Storage Devices (for example: NAS, SAN)	Section 31(1)(a)
Networking Infrastructure (for example: Switches, Routers, Interfaces, Wireless Access Points)	Section 31(1)(a)
Security Infrastructure (for example: Firewalls, Intrusion Detection Systems (IDS), Virus Monitoring Tools)	Section 31(1)(a)

Cardiff and Vale University Health Board (the UHB) is withholding certain information requested above, relying on section 31(1)(a) of the Freedom of Information Act 2000 ('the prevention or detection of crime'). Specifically, the UHB believes that disclosing details regarding its ICT infrastructure, or support of that infrastructure, would be likely to prejudice the prevention or detection of crime, particularly cybercrime.

As this is a qualified exemption, the UHB is required to complete a public interest test in deciding whether it is in the public's interest to withhold or disclose the information.

In favour of disclosure

The UHB recognises there is a public interest in transparency and in public authorities demonstrating that their systems effectively protect personal data.

Against disclosure

There is a very strong public interest in protecting the extremely sensitive data held by the UHB. Cybersecurity and the associated risk of cyberattacks represent a rapidly evolving arena that becomes more complex and dangerous with time. Releasing details of the UHB's ICT infrastructure into the public domain significantly reduces its capacity to manage this threat to the stated public interest by exposing potential vulnerabilities.

Decision

The UHB considers that the public interest in withholding the information is significantly greater than any interest there may be in disclosing it and potentially exposing sensitive personal data to an increased level

of risk. The UHB strongly believes that posing additional unnecessary risk to the UHB, and consequently patient care and safety, would be viewed as an unacceptable risk by the public.

Whilst the UHB acknowledges a public interest in providing assurances of effective protection of personal data, it believes the most effective means of increasing public confidence in data protection is to successfully protect the data itself. As such, disclosure of the information sought would be likely to allow interested parties to create a detailed picture of the UHB's IT infrastructure, rendering it vulnerable to exploitation through perceived weaknesses.

The UHB considers its responsibility to protect the personal data of patients and staff to be of the highest importance. It was therefore decided that it is not in the public's interest to disclose this information.

Q2. Does your organisation plan to procure any of the below enterprise applications or software, if yes, please provide information in the below format. **Please note, if the applications you're planning to procure are not listed below then do mention them separately.**	**2024/25 Spend/Budget (£000)**	**2025/26 Spend/Budget (£000)**
Content Management System	No	No
Supply Chain Management (SCM)	No	No
Inventory Management Software	No	No
Enterprise Asset Management (EAM) Software	No	No
Business Intelligence Systems	No	No
Other software/apps (mention the name of the software)	Section 12	Section 12

In completing a search for certain information requested, the UHB has confirmed that this information is not centrally recorded or collated. To retrieve the information requested would require a manual search through individual records and the UHB considers that this would exceed the limit set within Regulations for responding to a request. The UHB has therefore relied upon the section 12 exemption of the Freedom of Information Act 2000 ('Exemption where cost of compliance exceeds appropriate limit') and is refusing your request.

The UHB has estimated that to complete the work needed to respond to this request would exceed the time limit as set within Regulations to respond to a Freedom of Information Act request. Under the Act there is an allowance of two and a half days, or 18 hours, to comply with a request and the cost limit set within the Fees Regulations for this amount of work (18 hours) is £450 for the UHB. The Fees Regulations specify that the cost of complying with a request must be calculated at the rate of £25 per hour.

Q3. Do you have any plans to procure End user devices (desktop/laptop/tablet/mobile phones etc)? if yes, please provide information in the below format.	**2024/25 Spend/Budget (£000)**	**2025/26 Spend/Budget (£000)**
Desktop	Approx. 300k	Approx. 300k
Laptop	Approx. 150k	Approx. 150k
Mobile Phones	No	No
Tablets and Others (Please specify, if Others)	No budget set	No budget set

Q4. Do you have any plans to procure below services/softwares? if yes, please provide information in the below format.	2024/25 Spend/Budget (£000)	2025/26 Spend/Budget (£000)
Artificial Intelligence (AI)	No	No
Cyber Security	Section 31(3)	Section 31(3)

For the information requested on cyber security solutions in Q4, the UHB can neither confirm nor deny that it holds this information by virtue of section 31(3) of the Freedom of Information Act 2000, in particular, relying on the section 31(1)(a) exemption ('the prevention or detection of crime'). The UHB believes that disclosing details regarding its ICT infrastructure, or support of that infrastructure, would be likely to prejudice the prevention of crime, particularly cybercrime. As this is a qualified exemption, the UHB is required to complete a public interest test in deciding whether it is in the public's interest to maintain the exemption from the duty to confirm or deny holding the information sought.

Against maintaining the exemption

The UHB recognises there is a public interest in transparency and in public authorities demonstrating that their systems effectively protect personal data.

In favour of maintaining the exemption

There is a very strong public interest in protecting the extremely sensitive data held by the UHB. Cybersecurity and the associated risk of cyberattacks represent a rapidly evolving arena that becomes more complex and dangerous with time. Releasing details of the UHB's ICT infrastructure into the public domain significantly reduces its capacity to manage this threat to the stated public interest by exposing potential vulnerabilities.

To confirm or deny whether this information is held could identify to a cybercriminal if a specific attack was successful. The UHB strongly believes that posing additional unnecessary risk to the UHB, and consequently patient care and safety, would be viewed as an unacceptable risk by the public. Whilst the UHB acknowledges a public interest in providing assurances of effective protection of personal data, it believes the most effective means of increasing public confidence in data protection is to successfully protect the data itself.

Decision

The UHB considers that the public interest in maintaining the exemption from the duty to confirm or deny is significantly greater than not maintaining the exemption. The UHB considers its responsibility to protect the personal data of patients and staff to be of the highest importance. It was therefore decided that it is in the public's interest to maintain the exemption from the duty to confirm or deny holding the information sought.