



Request Reference: 3513

FOI Request dated 15/10/2025 –

- *As below*

Response

Q1. Can you please list the number of devices deployed by your organisation for the following?	
Device Type	Number of Devices
Desktop PCs	3532
Laptops	1801
Mobile Phones	260
Printers	149
Multi Functional Devices (MFDs)	See printers above
Tablets	151
Physical Servers	74
Storage Devices (for example: NAS, SAN)	6
Networking Infrastructure (for example: Switches, Routers, Interfaces, Wireless Access Points)	1900
Security Infrastructure (for example: Firewalls, Intrusion Detection Systems (IDS), Virus Monitoring Tools)	Section 31*

Q2 – No plans to all

Q3 – No plans to all

*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 world, 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.

Please be aware that Freedom of Information (FOI) requests made with the intention of furthering commercial interests, such as selling goods or services or gaining a competitive advantage over potential suppliers, are outside the intended scope of FOI. Using FOI for gaining a commercial advantage over others is not in line with the purpose of the Act and provides minimal or no benefit to the public. ICO guidance sets out that: "The public interest here means the public good, not what is of interest to the public, and not the private interests of the requester.