Request Reference: 3450

FOI Request dated 09/07/2025 –

1. Standard Firewall (Network)
Firewall services that protect the organisation's network from unauthorised access and other internet security threats.
2. Anti-virus Software Application
Programs designed to prevent, detect, and remove viruses, malware, trojans, adware, and related threats.
3. Microsoft Enterprise Agreement
A volume licensing agreement that may include:

- *Microsoft 365 (Office, Exchange, SharePoint, Teams)*
- *Windows Enterprise*
- *Enterprise Mobility + Security (EMS)*
- *Azure services (committed or pay-as-you-go)*

4. Microsoft Power BI
Or any alternative business intelligence platform used for data connectivity, dashboards, and reporting.

For each of the above areas, I kindly request the following:

1. *Who is the existing supplier for this contract?*
2. *What is the annual spend for each contract?*
3. *What is the description of the services provided?*
4. *Primary brand (where applicable)*
5. *What is the start date of the contract?*
6. *What is the expiry date of the contract?*
7. *What is the total duration of the contract?*
8. *Who is the responsible contract officer?*
   - *Please include **at least their job title**, and where possible, **name, contact number, and direct email address***
9. *How many licences or users are included (where applicable)?*

Response

1. Standard Firewall (Network) - Firewall service protects your corporate Network from unauthorised access and other Internet security threats

The information I require is around the procurement side and we do not require any specifics (serial numbers, models, location) that could bring threat/harm to the organisation.
For each of the different types of cyber security services can you please provide me with:

1. Who is the existing supplier for this contract? Section 31(3) – Law Enforcement (please see below)
2. What does the organisation annually spend for each of the contracts? £181,730.56

3. What is the description of the services provided for each contract? Section 31(3) – Law Enforcement (please see below)
4. Primary Brand (ONLY APPLIES TO CONTRACT 1&2) Section 31(3) – Law Enforcement (please see below)
5. What is the expiry date of each contract? 24/01/2027
6. What is the start date of each contract? 09/07/2023
7. What is the contract duration of contract? 40 months
8. The responsible contract officer for each of the contracts above? Full name, job title, contact number and direct email address. Stuart Craig, Network and Communication Manager, s.craig@hull.ac.uk*

2. Anti-virus Software Application - Anti-virus software is a program or set of programs that are designed to prevent, search for, detect, and remove software viruses, and other malicious software like worms, trojans, adware, and more.

Exempt wholly as per Section 31(3) – Law Enforcement/Section 43(2) – Commercial Interests (please see below reasoning)

1. Who is the existing supplier for this contract?
2. What does the organisation annually spend for each of the contracts?
3. What is the description of the services provided for each contract?
4. Primary Brand (ONLY APPLIES TO CONTRACT 1&2)
5. What is the expiry date of each contract?
6. What is the start date of each contract?
7. What is the contract duration of contract?
8. The responsible contract officer for each of the contracts above? Full name, job title, contact number and direct email address. – This role is currently vacant

3. Microsoft Enterprise Agreement - is a volume licensing package offered by *Microsoft*.

Exempt wholly as per Section 31(3) – Law Enforcement/Section 43(2) – Commercial Interests (please see below reasoning)

1. Who is the existing supplier for this contract?
2. What does the organisation annually spend for each of the contracts?
3. What is the description of the services provided for each contract?
4. Primary Brand (ONLY APPLIES TO CONTRACT 1&2)
5. What is the expiry date of each contract?
6. What is the start date of each contract?
7. What is the contract duration of contract?
8. The responsible contract officer for each of the contracts above? Full name, job title, contact number and direct email address. Kev Sach, Associate Director, IT Services. K.sach@hull.ac.uk*
9. Number of Licenses (ONLY APPLIES TO CONTRACT 3)

Section 1 of the Freedom of Information Act 2000 (FOIA) places two duties on public authorities. Unless exemptions apply, the first duty at Section 1(1)(a) is to confirm or deny whether the information specified in a request is held. The second duty at Section 1(1) (b) is to disclose information that has been confirmed as being held. Where exemptions are relied upon Section 17 of FOIA requires that we provide the applicant with a notice which: a) states that fact b) specifies the exemption(s) in question and c) states (if that would not otherwise be apparent) why the exemption applies.

We have applied the following exemptions to your request – Section 31 (1) (a) – Law Enforcement and Section 43(2) – Commercial Interests. As both are prejudice based, qualified exemptions, evidence of harm and public interest considerations need to be articulated. Please see below -

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 the names of our existing supplier and that of our primary brands, for our Firewall Service, Anti-Virus Software and Microsoft Enterprise Agreement, a motivated individual or group could use this information to target any potential vulnerabilities. Therefore, 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 favouring disclosure

- Increase the public understanding of the University's information technology systems, 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 that 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.

Section 43(2) – Commercial Interests

Factors favouring disclosure

- Disclosing information regarding future IT projects, business plans and ICT strategic plans involved would ensure the University are being open and transparent with the public. The disclosure would encourage public debate and increase public awareness on this subject matter. It would also allow the public to see where the public funds for the University are being spent.

Factors against disclosure

- Disclosing the information requested is likely to damage the relationship between the University and the service provider(s). In turn, this could prejudice the commercial interests of the service provider(s), especially in cases where there may be a limited number of suppliers in the market. Making a disclosure could identify information, which has been specifically obtained through negotiation between the University and the service provider, thus prejudicing the University position in future, negotiations.

Balance test

Despite there being an identifiable public interest in the University, being open and transparent, the interests of the University may be jeopardised if information relating to sensitive commercial information about future IT projects, business plans and ICT strategic plans are disclosed. The community would also be impacted as costs to the University could be driven up by the lack of competition due to companies refusing to do business with University's that disclose commercially sensitive information. If this information were to be disclosed, this could cause harm between the University and its service provider(s). Having weighed up all of the factors outlined above, on balance the argument for disclosing this information is not made out and therefore it is in the public interest to withhold this information from disclosure.

Section 17 of the Freedom of Information Act 2000 requires the University, when refusing to provide information (because the information is exempt) to provide you the applicant with a notice which: (a) states that fact, (b) specifies the exemption in question and (c) states (if that would not otherwise be apparent) why the exemption applies. In accordance with the Freedom of Information Act 2000 this email acts as a Refusal Notice for those aspects of your request

*Please note, the staff named above are exercising their right to object to processing contained in article 21 of the UK General Data Protection Regulation. This right is exercised here with specific reference to not having their contact information used for marketing purposes.