UNIVERSITY OF HULL

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

Request Ref: 2820

FOI Request dated **22/02/2023** as follows –

1. Telephony and UC/ Collaboration
a. Please confirm the manufacturer of your telephony system(s) that are currently in place
b. When is your contract renewal date?
c. Who maintains your telephony system(s)?
d. Do you use Unified Communications or Collaboration tools, if so which ones?
2. Microsoft
a) What Microsoft 365 licence do you have across the business e.g. E3, E5
b) Which partner looks after your Microsoft tenant?
c) Where do you host your applications? Do you have on-premise infrastructure or do you host your applications in public or private cloud? Which?
3. Storage
a. Does your organisation use on-premise or cloud storage or both?
b. Please confirm the on-premise hardware manufacturer
c. Please confirm your cloud storage provider
d. What is your annual spend on cloud storage?
e. How do you back up your data and with who e.g. Backup as a Service

Response

1. Telephony and UC/ Collaboration
a. Avaya
b. November 2025
c. BT
d. Microsoft Teams

2. Microsoft
a. A5
b. Phoenix
c. Applications are hosted on premise, private and public cloud.

3. Storage
a. Both
b. Dell and Tintri.
c. Box, Azure and OneDrive
d. £100K

e. 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 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, 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 storage systems and processes, and how it manages its business.

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.