Your request read:

“I would be most grateful if you would provide me, under the Freedom of Information Act, details in respect to the following questions;

1. How many instances of the Microsoft Windows 7 Operating System are currently in operation across your entire network? How many devices such as kiosks, lap tops etc are still running Windows 7?

2. How many instances of the Microsoft Windows XP Operating System are currently in operation across your entire network? How many devices such as kiosks, lap tops etc are still running Windows XP?

3. Who is the officer responsible for maintaining and delivering legacy applications to all your users?”

The University of Leeds holds this information. However, we are withholding this information under sections 31(1)(a) of the Freedom of Information Act.

Section 31(1)(a) sets out that information is exempt if its disclosure would or would be likely to prejudice the prevention or detection of crime.

We consider that the release of this information would be likely to make the University of Leeds more vulnerable to cyber-attacks. It is public knowledge that Microsoft have stopped supporting the Windows XP and Windows 7 operating systems. This means that Microsoft no longer provide security updates or technical support to users of those systems. This makes machines running Windows XP or Windows 7 vulnerable to cyber criminals, because they are not equipped with the latest security measures designed to protect users from attacks.

To reveal the number of systems we currently operate which are running those systems (if any), would provide would-be attackers with valuable information which could be used to assist in the planning of a cyber-attack. If the University of Leeds is running a large number of machines on Windows XP and/or Windows 7, a broad-scale attack may be successful. If we are only running a small number of machines with those systems, a more targeted attack is likely to have increased success. By
revealing the name of the individual who is responsible for legacy applications, we
would provide those with nefarious objectives with a specific target for their actions.

We also consider that if we were to release this information, it is possible (or even
likely) that it could be combined with other information to provide attackers with
further, useful information. For instance, if information on departmental spent on
computers were to be made available (e.g. as the result of an FOI request) over the
last five or ten years, this would give would-be attackers clues as to where the
machines running the older operating systems may be based; if the Department of X
and Y have not spent any money on the purchase of computers in the last 10 years,
it is more likely that the machines in that department are running older operating
systems, and are therefore prime targets for an attack.

In combination with the contact information we publish online, we believe this would
provide would-be attackers with sufficient information to attempt a targeted attack,
which would be likely to have a higher chance of success than a speculative attempt.
This clearly demonstrates the prejudice which would be likely to occur as a result of
the release of this information.

Section 31(1)(a) is a qualified exemption, and as such we are required to consider
whether the public interest is in favour of maintaining the exemption or disclosing the
information. We recognise a public interest in the release of information which
contributes to public understanding of our approach to cyber-security. However, we
consider that these interests are vastly outweighed by the public interest in
protecting our ability to shield our staff and students from cyber-attacks and their
potential outcomes.

We therefore consider that the public interest is strongly in favour of withholding this
information.

We hope this information is helpful. If you have any questions about this email,
however, please do not hesitate to contact us on foi@leeds.ac.uk

If you are unhappy with the service you have received in relation to your request and
wish to make a complaint or request a review of our decision, you can request an
Internal Review. Requests for Internal Review should be made in writing using the
following contact information:

Post: Mr D Wardle
Deputy Secretary
The University of Leeds
Leeds
LS2 9JT

Email: foi@leeds.ac.uk

Requests for Internal Review should be submitted within 40 working days of
receiving the University’s response to your request. Further information about how
the University manages Freedom of Information requests and about our complaints
procedure is also available on our website (www.leeds.ac.uk).
If you are not content with the outcome of the internal review, you have the right to apply directly to the Information Commissioner for a decision. Generally, the ICO cannot make a decision unless you have exhausted the review/complaints procedure provided by the University. The Information Commissioner can be contacted at: Information Commissioner’s Office, Wycliffe House, Water Lane, Wilmslow, Cheshire, SK9 5AF.

Yours sincerely

Chloe Wilkins
Freedom of Information Officer

Secretariat
University of Leeds