Ref No: 4073
Date: 14/01/2020
Subject: Information Governance and Environmental Impact

REQUEST

1) please can you send me a copy of the current subject access request acknowledgment AND response letter that you use

2) a copy of the last 5 dpias completed

3) a copy of any internal mandatory information governance training that you give to staff which was written in the last 2 years including presentation slides and videos and any other media

4) a copy of any instructions given to staff members to reduce data security breaches, for example double checking work which was written in the last 5 years

5) a list of any policies implemented in the last 2 years within the organisation to help reduce the environmental impact that the organisation has?

RESPONSE

1) Please see attached. Please note, that these are automatically created through the Information Governance Portal.
Redactions have been applied to the personal information within the templates. This information is exempt from release under section 40(2) of the Freedom of Information Act 2000 as the release of this information would breach one or more of the data protection principles. This acts as our refusal notice.

2) Please see the attached documents for the last 5 DPIAs completed at the University. Please note, we have removed certain information from the completed DPIAs.

Personal information of staff members, mostly names, have been removed as this information is exempt from release under section 40(2) of the Freedom of Information Act 2000 as the release of this information would breach one or more of the data protection principles. This acts as our refusal notice.

Risk assessment information has been removed from the DPIAs as this contains information about where the University and/or its systems may be vulnerable to cyber-crime. This information is exempt from release under section 32(1)(a) of the Freedom of Information Act 2000, as its release would make the University more vulnerable to crime. This acts as our refusal notice.

Section 31 is a qualified exemption and therefore we are required to conduct a public interest test before engaging the exemption.

Whilst we recognise the public interest in openness and transparency we do not believe that this supersedes the need to protect the University itself, but also its students and staff, from crime and its consequences. Releasing the detailed risk assessment information would be likely to increase the likelihood that University systems would be targeted for criminal activity and therefore the public interest in protecting the University, its students and staff is greater than the public interest in releasing the requested information.

3) The requested information is also exempt from release under section 31(1)(a) of the Freedom of Information Act, as its release would make the University or its staff more vulnerable to crime. Releasing information on how we train our staff on information security issues could lead a potential attacker to exploit any holes or flaws in the training and allow them to predict how members of staff will respond to different attack vectors. This would be likely to make the University more vulnerable to being targeted by criminals.

Section 31 is a qualified exemption and therefore we are required to conduct a public interest test before engaging the exemption.

We recognise the public interest in openness and transparency however, we do not believe that this should come at the expense of the security of the information that the University holds and which it has legal responsibilities to protect. By releasing the training, we would be making it more likely that the University could be targeted by criminals. We do not believe this to be in the public interest to release this information.

In line with our section 16 duty to provide aid and assistance to requesters, we have listed below the broad topics that which the training covers:

- Understanding information security
- Legislation, policies and procedures
- Data Protection
- Information classifications
- Freedom of Information
- Physical security
- Password protection
- Cloud computing
- Email and phishing
- Threats

All staff are required to complete the mandatory induction training within 1 week of their employment commencing. As of 2018, staff are also required to complete a 'refresher' module every 24 months.

4) There have been no instructions to staff on double checking work for the purposes of reducing data security breaches.

The University has an Information Security Policy and a Data Protection Policy that give staff advice on how to reduce the likelihood of data security breaches.

5) Please find attached the Environmental Policy for the University. This was approved in August 2017 has been implemented over the last two years.

Your request i.d. is: 4073. Please quote this in all enquiries.

The University aims to comply fully with its obligations under the Freedom of Information Act 2000 and to ensure that the service it provides for those wishing to gain access to information is helpful and effective.

The personal information you have supplied will be used only to process your request; some details will be retained for our records after the request has been answered. This information will not be passed on to other parties unrelated to the University unless we are required to do so by law, or where it would be necessary to answer the request in full (in which case we would seek your consent for any transfer).

Process for Making a Complaint

If you feel the service you have received does not meet our aims or your expectations, please write to:

Claire Geddes
Head of Governance Services
University House
Lancaster University
Bailrigg
Lancaster
LA1 4YW

Email: c.burston@lancaster.ac.uk

If, following our internal review, you are dissatisfied with the response provided, you may write to the Information Commissioner's Office, for details visit www.ico.org.uk.