Data Protection Bulletin: March 2019

Update from the Information Compliance Office

The Information Compliance Office has produced new standardised data sharing/data processing agreement templates to be used in the following circumstances

- Where the university is seeking to work jointly with an external organisation and that work requires the sharing of personal between parties (Controller to Controller sharing)
- Where the university has engaged an external organisation to carry out a service on its behalf, where the external organisation would be processing of personal data on the university's behalf (Controller to Processor agreements).

These agreements should be collateral to the main agreements around service/joint working and should be completed before any data is transferred to an external organisation. For further guidance, please contact the Information Compliance Office.

The Information Compliance Office would also like to remind colleagues involved in developing/purchasing new systems or those considering new processing activities that we are required to implement Data Protection by design and default in the scoping and management of such projects. Where newly purchased or developed systems will hold personal data or you are considering new processing activities, please consider the privacy of data subjects as part of those processes. You may need to complete a Data Processing Impact Assessment. Please contact the Information Compliance Office if you would like further information.

Work to produce key policies and procedures has begun and the Information Compliance Office is working collaboratively with colleagues in IS to create concise data breach, IS security and Data protection Policies. It is envisaged that these policies will be shared with Information Custodians for comment during drafting. The Information Compliance Office will be implementing an Awareness and Communications plan during the next few months, with a view to re-build colleagues awareness and reaffirm 'buy-in' around data protection compliance

Summary of the ongoing work of the ICWs

The format of the Information Custodians Workshops has changed, with information custodians divided into smaller workshops, which broadly consist of custodians working in similar operational environments attending the same workshop. The aim of the re-formatting of was to better provide an effective forum in which colleagues felt more able to discuss data protection and compliance issues and in turn share of best practice.

The Head of Data Protection would like to thank all Information Custodians in advance of their work in helping to compile the University's Information Asset Register (IAR). An IAR Template and guidance document will be sent out in due course. To support this work, the Information Compliance Office are looking to provide drop in sessions over the next few months to offer practical advice to those completing the IAR.

The Information Compliance Office are currently making arrangements for the next set of workshops and custodians will be informed of times/date in early March.

Top 5 Risks and Remedies

As part of our efforts to drive best practice in data protection and our continued commitment around addressing information security risks, each bulletin will address 5 compliance risks that have come to the attention of the Information Compliance Office. Many of these risks have been identified through recent Information Custodians Workshop meetings, whilst others have emerged during our office's ongoing compliance monitoring and from 'lessons learnt' analysis of data breaches. We ask that all members of staff and particularly Information Custodians, promote the remedial actions in their operational areas.

- **Removable devices.** The use of removable devices should be avoided where possible. If there is a regular need to access files outside the network, colleagues should consider using VPN access or creating a SharePoint folder. If there is an established need to use a removable device, then that device should be encrypted and password protected. Removable devices should not be sent through the post or by courier without first seeking the advice of the Information Compliance Office. Much the same as any IT equipment, when a damaged device is irreparable or the device has reached the end of its lifespan, attempts should be made to overwrite or erase any files that remain on the device and devices should be disposed of securely, by contacting Estates.

- **Transferring data.** Staff should consider the most effective way to securely transfer personal data to other colleagues/external contacts. If you are working collaboratively with colleagues, it may be more appropriate to use SharePoint (more information can be found here). If you are sending large files containing personal data to colleagues, then you should make use of password protected 'Goesend' (more information can be found here). If you are making an ad hoc transfer of personal data by email, you should 'zip' the file and password protect that file. Whenever using passwords, send the password separately from the file, ideally through a different medium- if the file is sent by email, share the password by phone. Please avoid cloud based sharing platforms as their use has implications around third party processing and data security.

- **Securely storing data.** Whether in an electronic or paper based format, ensuring the continued security of data and any associated processing is of paramount importance in safeguarding against potential breaches. Electronic data should be stored in a university network drive that is subject to appropriate access controls. If leaving your computer unattended, the screen should be locked. Apart from ensuring that data is held within a secure network environment, saving to a drive also means that the data can be located, retained and deleted in accordance with best practice. If the data is paper based, it should be stored in a locked cabinet and the key kept securely. Colleagues should also be aware of the need to maintain the security of buildings and offices; they should be actively making sure that doors are locked, windows closed etc when leaving offices unattended.

- **Reporting of Breaches.** Staff should be reminded of the need to report potential data breaches to the Information Compliance Office as soon as the breach has been discovered. In certain circumstances, the Information Compliance Office may need to forward the breach notification to the ICO and we would be required to do so within 72 hours of the organisation becoming aware of the breach. Late reporting to the ICO of reportable breaches may result in the ICO considering enforcement action.

- **Training.** The completion rates around GDPR training are still low. It is imperative that colleagues complete the mandatory training around GDPR. Information Custodians will be provided with lists of those who have competed the training and the Information Compliance Office would be grateful if the Information Custodians assisted in re-enforcing the need for colleagues to co-operate on this issue. Any future non-compliance will be reported to EG. The Information Compliance Office are currently looking at finding a more effective training platform for on boarding and refresher training that more suits a higher education environment.

News from the Information Commissioner's Office

When trying to promote good Information Governance, Information Custodians may find it useful to remind colleagues of the serious consequences of non-compliance. Please see below for a summary of pertinent cases recently enforced by the ICO.

Heathrow Airport Limited (HAL) fined for loss of USB stick

In October 2018, the ICO fined HAL £120,000 over the loss of an unencrypted USB memory stick. Despite holding over 1000 files, the stick held a relatively small amount of personal and sensitive personal data relating to around 50 HAL employees. The stick was found by a member of the public, who passed it to a national newspaper, which in turn took copies of the data before returning the stick to HAL. The ICO investigated and found that only 2% of HAL employees had completed information security and Data Protection training. The ICO noted that a number of employees were disregarding HAL's own polices and guidance around the use of removable media and that HAL did not maintain adequate levels of controls to monitor and prevent such behaviour from occurring.