UNAPPROVED
CIRCULATED

Edinburgh Napier
UNIVERSITY

UIGG(16/17)10

EDINBURGH NAPIER UNIVERSITY
DIGITAL STRATEGY & INVESTMENT COMMITTEE

UNIVERSITY INFORMATION GOVERNANCE GROUP

Minutes of the meeting held on Tuesday 21 February 2017
at 2.00pm in the Siegfried Room, Craiglockhart Campus

Present

D Watt (Information Governance Manager)[Convenor]; J Baillie (Campus Support Assistant/Technician); A Deegan Wood (Planning Officer); M Henderson (School Support Coordinator); N Kivlichan (Head of Market Intelligence and Evaluation); B Merchant (Portfolio & Services Engagement Manager); D Munro (International Marketing Manager); A Richmond (Governance Adviser (Records Management)); L Smith (Operations Support Manager); D Spiers (Lecturer)

Apologies

P Barron (Professor of Hospitality & Tourism Management); R Bews (Appeals, Complaints & Conduct Officer); C Biggar (PA to Principal); E Clark (Governance Advisor (Freedom of Information)); D Cloy (Assistant Secretary); L Conlan (Head of HR Services); O Dellal (School Operations Officer); J Dickson (Faculty Quality Advisor); S Duncan (Head of Campus Services); L Fraser (HR Adviser); G Hamilton (Information Security Manager); L Mabberley (Assistant Director Marketing Brand and Communications); L McElhone (Head of Student Administration); J Martin (Systems Officer); S Simeone (Assistant Faculty Operations Manager); N Turner (Head of Research and Innovation Office)

In Attendance

M Mackay (Administrative Assistant)[Clerk]

Opening Remarks

The Information Governance Manager welcomed members to the meeting, and extended a specific welcome to the new members: A Richmond, who had joined Governance & Compliance in the post of Governance Adviser (Records Management) (GA(RM)), and M Henderson, who was deputising for O Dellal.

The apologies were **noted**.

01 Minutes of the Meeting held on 06 October 2016 UIGG(16/17)03

Members **approved** the minutes of the meeting on 06 October 2016 as an accurate record.

02 Matters Arising from the Minutes

a) Information Governance Co-ordinators' Network

The Information Governance Manager reported that she had been liaising with departments across the University to establish the Information Governance Co-ordinators' Network, but required more volunteers for the role of IG Co-ordinators.

Actions: The IGM to circulate the remit for the Information Governance Co-ordinators Network. Members to notify the IGM of nominees for Information Governance Co-ordinators by **17th May 2017**

b) Communication of Information Governance Matters

The IGM requested feedback on the effectiveness of the IG newsletter that had been sent to members. It was reported that while members did forward the newsletters to colleagues, it was difficult to be sure these were read.

The IGM had been attending team meetings to provide briefings for staff on the new requirements and responsibilities due to the General Data Protection Regulation. It was suggested that a briefing sheet on the GDPR might be a potential alternative, although the IGM stated that, given the scope and importance of the GDPR, attending meetings was a worthwhile commitment.

Action: Members to contact the IGM if they wish a GDPR briefing at their team meeting.

03	**Policy Updates**	**UIGG(16/17)04 - 07**

The IGM informed members that the following policy documents had been reviewed: Access to Information Policy, Data Protection Policy Statement, Manual and Physical Data Security Policy, and Records Management Policy.

Functional amendments had been made to ensure the policies contained up to date contact information and referred to the current structure of the University. The Data Protection Statement had also been further amended due to the General Data Protection Regulation, in advance of the major update this would require to the University's Data Protection policies and Code of Practice.

The revised versions of all the policies were **approved**.

04	**Data Protection Audit and General Data Protection Regulation Update**	**Oral Report**

The information Governance Manager reported on the most recent developments on the GDPR.

The intranet page on the GDPR had been updated with actions, which would be circulated to Senior Leadership Group to cascade to staff. Some specific points highlighted were:

1. Penalties – with the increase in maximum fine increased to €20M or 4% of annual turnover, the risk to the University had substantially increased, and was included on the main Risk Register for the University.

2. Definition of Personal Data – the expanded definition of what constituted person data would require a review of the University's systems and process to ensure compliance.

3. Conditions for Processing – changes to the number of conditions available to provide a valid legal basis for processing personal data mean that staff need to carefully consider the data they process, and be able demonstrate compliance, e.g. by documenting processes.

System user access forms would be required for anyone using University systems to process personal data, and new templates were being rolled out.

Staff contracts were updated recently to specifically include data protection along with information security and records management. The university's policies covering the use of cloud computing services would be reviewed.

4. Privacy Notices – these would need to contain more information to cover the changes of rights of data subjects and responsibilities of staff, and ensure compliance with the GDPR.

5. Contracts – These present a potentially major challenge, as any contract for services involving data processing would require review to ensure a data sharing agreement was included for compliance with the GDPR.

6. Contracts with organisations outwith the European Economic Area would also require review to ensure compliance.

7. The University was already carrying out Privacy Impact Assessments for systems being procured or rolled out, as required by the GDPR.

8. Consent – requirements for demonstrating consent from data subjects were being tightened, and the rights of data subjects to withdraw their consent as well as exercise the 'right to be forgotten' would need to be balanced with the University's requirements to retain data, e.g. for proof of qualifications.

9. Data Portability – data processing systems would require review to ensure data could be extracted in a machine-readable format.

10. Profiling – individuals' rights to not be subject to automated decision making have been highlighted by recent ICO action and any such systems would need to be reviewed to ensure compliance.

11. Data Subject Access Requests – the time allowed for the response for a DSAR would be reduced and there would no longer be a fee charged.

Action: Members to circulate the link to the GDPR web page to colleagues and promote awareness of the issues arising from it.

05 Freedom of Information Report to January 2017 UIGG(16/17)08

The Information Governance Manager spoke to the paper and highlighted some key points:

- The number of Freedom of Information requests had risen slightly over the previous year, and the complexity of questions from individual requests had also increased
- The majority of requests continued to be received from the media
- The University's drive to proactive publication of information had led to the application of more Section 25 exemptions to requests where the information was already available
- There were no requests for the review of a decision on a requests during the reporting period

In response to a query regarding the sometimes burdensome requests for commercial information from companies seeking to do business with the University, the IGM informed the Group that the Scottish Information Commissioner had been clear that these were considered valid FOI requests and this was unlikely to change. This could be an area that pro-active publication of frequently requested information could be used to reduce the workload involved.

06 Data Protection and Records Management Report to January 2017 UIGG(16/17)09

The Information Governance Manager spoke to the paper and highlighted some key points:

Data Protection

- There had been no data security breaches during the reporting period.
- However, there had been a number of data security incidents, including:
  - Misdirected emails
  - Personal data being sent via unencrypted email
  - Insecure electronic storage of sensitive personal data
  - Personal data left on an MFD
  - Personal data sent to the incorrect office via internal mail
- A new contractor had taken over running the confidential waste consoles. Confidential waste sacks were no longer in use, and Property and Facilities were liaising with the new contractors to explore potential alternative measures, such as mobile consoles.
- The fines levied by the Information Commissioner's Office for data security breaches had been increasing, bring these into line with the GDPR.
- ICO had highlighted a 40% increase in data security incidents in the educational sector. This is likely to mean that the education sector will be under increased scrutiny.
- High level guidance on the GDPR had been produced by the European Data Protection Board and ICO.
- The Scottish Higher Education Information Practitioners' Group had formed a working group, allowing Universities to spread the workload of preparing guidance and best practice for the implementation of the GDPR across the sector.
- Enforcement action taken by the ICO in relation to data security breaches by two Universities in recent years had placed a focus on staff training.
- New template forms for access to University systems had been developed.
- New checklists for staff dealing with data protection requests, e.g. police requests had been developed.
- New template data sharing agreements had been developed.

Records Management

- Work on retention schedules was continuing across the University.
- Governance Services were liaising with colleagues to promote the use of SharePoint, with a generally positive reception.
- Guidance for electronic records management was being developed.
- The GA(RM) was liaising with Information Services to develop guidance for staff using unsupported/insecure data storage systems. Alternative secure systems with similar functionality which are recommended for use by the IS would be investigated and included in the guidance.
- The GA(RM) was liaising with colleagues dealing with events to ensure a consistent approach to records management.

Action: The IGM requested that members continue to promote Information Governance training.

07 Review of Car Park Safety Oral Report

The information Governance Manager passed a request from Dougie Dack, Campus Manager to members of the group. As part of a project to improve safety in the University's car parks, a review of CCTV was being conducted, with a view to installing new cameras. The CM was canvassing for feedback from staff on safety in the car parks.

Action: Members to pass any feedback on car park safety to D Dack.

08 Information Security / Network and Security Services Report Oral Report

The Portfolio & Services Engagement Manager reported on current information security issues:

The project to remove local administrator rights from staff PCs had been put on hold. Useful work to determine the extent to which these rights are currently granted had been completed, but it was felt that any changes to existing arrangements would be difficult to enforce without corresponding changes to Information Security Policies. A decision by the University to adopt Cyber Essentials would assist this change and a proposal to do so had been taken to Digital Strategy and Investment Committee. A separate project to develop a Windows 10 desktop image had been started and it was hoped that this would enforce no local administrator rights as part of its specification.

A number of administrative credential management products had been investigated and it was intended that a course of action would be recommended in the coming weeks. A communications campaign was underway to encourage staff and students to enrol for the Password Manager service, to allow self-service password resets.

The mobile device management service had been soft-launched, allowing staff to enrol University-owned mobile devices in order to ensure that proper security controls were being applied, as well as providing app delivery and automatic configuration of account settings. It is hoped that MDM enrolment would be made mandatory for all University-owned mobile devices in due course.

A revised Information Security Awareness Training course was expected to be made available within the coming weeks. Discussions between Information Services and Human Resources were taking place to make this mandatory for all staff, with the course being run through Moodle, allowing tracking of compliance. The work to review Information Security Policies was ongoing.

Recent information security incidents have shown that some members of staff were unaware of the intended purpose of certain University data storage areas and in particular, who had access to documents placed there. There may be a need for additional documentation and/or training to be provided, to ensure that University information is being stored appropriately.

09 Information Services Project Updates Oral Report

The Portfolio & Services Engagement Manager reported on two major projects currently being undertaken by Information Services:

Office 365 for Staff:
The technical constraints on the migrations process had been either resolved or mitigated, with the first batch of test accounts moved to the cloud at the end of January. Testing of these accounts had identified some issues with how Office 365 licences were being assigned. This was proving to be a complex issue to resolve that would involve unpicking some staff licence assignments and reapplying them to the correct licence plans. If not implemented correctly this had the potential to remove access to features currently in use by staff (and potentially also students) or in the worst case scenario decommission mailboxes after 30 days, hence great caution was being taken to ensure this is resolved before any live mailboxes were migrated.

The Office 365 project was planned as a phased release of features to staff, however recommendations would be going to the Project Board about how to progress with the management of these features (existing and emerging) when the project was complete. Some features of O365 (although already released to students) may pose a greater risk to the University if made available to staff, especially those that involve tools for collaboration. Other examples included Yammer, which has its data hosted in the US, and the use of Group email accounts that could allow the potential for impersonation.

Remote Access To Data:
Following extensive market research and a formal Request for Information exercise at the end of 2016, Information Services were working with a third party supplier to implement a month-long Proof of Concept (POC) of a product called Syncplicity. IS were negotiating with the supplier to install the product in such a way that would allow continued use of the existing mapped drives in synchronisation with the new product to give a true picture of the functionality. A deliverable of the project is a clear definition of the various data areas made available by the University for staff and students. This would allow two-way mapping with the Information Classification Scheme to make it clearer which storage area was suitable/unsuitable for various types of data.

Further details would be announced on the Staff Intranet closer to the launch of the POC, when it will be vital for all interested areas of the University to take part in the testing and feedback on whether the product meets their needs. Members were therefore encouraged to participate in the Proof of Concept of the system.

Next meeting date

Currently scheduled for **Thursday 01 June 2017**, at **10.00am**, in the **Tower Boardroom, Merchiston Campus**.