APPROVED
CIRCULATED

UIGG(16/17)03

EDINBURGH NAPIER UNIVERSITY
DIGITAL STRATEGY & INVESTMENT COMMITTEE

UNIVERSITY INFORMATION GOVERNANCE GROUP

Minutes of the meeting held on Thursday 06 October 2016
at 10.00am in Room 6.B.30, Sighthill Campus

Present
D Watt (Senior Governance Officer, Records Manager)[Convenor]; P Barron (Professor of Hospitality & Tourism Management); C Biggar (PA to Principal); E Clark (Governance Assistant); A Deegan Wood (Planning Officer); S Duncan (Head of Campus Services); L Fraser (HR Adviser); G Hamilton (Information Security Manager); N Kivlichan (Head of Market Intelligence and Evaluation); L Mabberley (Assistant Director Marketing Brand and Communications); L McElhone (Head of Student Administration); J Martin (Systems Officer); B Merchant (Portfolio & Services Engagement Manager); S Simeone (Assistant Faculty Operations Manager); N Turner (Head of Research and Innovation Office)
Apologies
J Baillie (Campus Support Assistant/Technician); R Bews (Appeals, Complaints & Conduct Officer); D Cloy (Assistant Secretary); L Conlan (Head of HR Services); O Dellal (School Operations Officer); J Dickson (Faculty Quality Advisor); D Munro (International Marketing Manager); L Smith (Operations Support Manager); D Spiers (Lecturer)
In Attendance
M Mackay (Administrative Assistant)[Clerk]
Opening Remarks
The Senior Governance Officer (Records Manager) welcomed members to the first UIGG meeting of 2016/17, and extended a specific welcome to the new members: P Barron, L Fraser and J Martin, as well as returning member L Mabberley. The apologies were **noted**.
01 Minutes of the Meeting held on 31 May 2016 UIGG(15/16)25
Members **approved** the minutes of the meeting on 31 May 2016 as an accurate record.
02 Matters Arising from the Minutes
a) Minute 7 – CCTV Code of Practice. The revised CCTV Code of Practice had been approved by Dr Gerry Webber, as convenor of Digital Strategy and Investment Committee, with the exception of those sections covering the use of unmanned aerial systems (drones). The use of drones would be handled as a Risk Management issue by the University, requiring agreement from a Level 3 budget holder via Procurement to purchase drones and liaison with Health and Safety to conduct a risk assessment.

03	Information Security Roadshows	Oral Report

The Portfolio & Services Engagement Manager reported on the latest round of Information Security Roadshows:

- While the roadshows continued to be successful, it was felt that the current format was in need of a refresh.
- The scheduling of the roadshows to run early in the first trimester had been effective at drawing students, who were often approaching staff for assistance with connecting their devices to University systems, this presented an opportunity to discuss information security.
- IS were considering revising the locations of the roadshows, as while currently they received good through traffic, passers-by tended to be on their way elsewhere with limited time.
- New freebies were also under consideration, and the PSEM invited members to offer any suggestions.

04	Information Governance Co-ordinators Network	Oral Report

The SGO(RM) reported that the revival of the Information Governance Co-ordinators Network was under consideration. Networks had existed previously for both records management and data protection, however it was envisaged that the revived network would provid co-ordination and promotion of best practice in records management, freedom of information and data protection, across the University.

The SGO(RM) requested feedback from members on the possibility of having select administrative staff as a first point of contact for information governance queries and issues, and requested they respond with names of staff who could potentially take on the IG Co-ordinator roles, and suggestions for how the network could be implemented in practice in their areas.

The SGO(RM) would circulate a draft remit to members, and when required set up network meetings and brief IG Co-ordinators.

The group discussed issues, noting that while there were benefits to distributing IG contacts across the University, there was a potential risk that other staff would see data protection etc. to be the responsibility of the IG co-ordinators and not theirs. The need to keep promoting the message that information governance was the responsibility of all staff was reiterated, as was the requirement to co-ordinate IG with information security.

05	Communication of Information Governance Matters	Oral Report

The SGO(RM) reported that, with the restriction on sending all-staff email newsletters, IG newsletters would continue to be sent to the members who were encouraged to forward relevant information on to colleagues in their respective areas of the University.

06	Property and Facilities Records Management Update	Oral Report

The Head of Campus Services reported on progress with Property and Facilities ongoing Records Management project. The department had set aside two days dedicated to

records management. A Records Retention Schedule had been created in liaison with the SGO(RM), beginning with the Maintenance team due to statutory requirements involved with their records. The project had involved significant deduplication and disposal of records, as well as moving records onto SharePoint.

The SGO(RM) noted that Property and Facilities were producing a very comprehensive Records Retention Schedule tailored to their specific requirements.

07 Freedom of Information Report to September 2016 UIGG(16/17)01

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

- The number of Freedom of Information requests had slightly increased over the same period last year, but there had been a notable increase in the numbers of questions from requesters.
- The highest number of requests had been submitted by the media, followed by commercial organisations.
- Information Services and Student and Academic Services had received the most requests.
- One review of a decision, regarding a request relating to PREVENT, had been conducted and upheld the initial decision.
- Benchmarking using statistics from the Scottish Information Commissioner showed that Edinburgh Napier University performed well, and that legislative compliance and risk mitigation were good.
- The Office of the Scottish Information Commissioner was now providing 'learning points' in email newsletters, including:
    - Organisations need to ensure any search for information is thorough and can be shown to be thorough
    - Organisations do no need to respond to an initial request deemed to be vexatious, but would need to respond to any follow-up request for a review and ensure the requestor was sent the necessary information on how to proceed further
    - All staff should be able to identify a Freedom of Information request

The group discussed some issues raised by the learning points. Routine requests should be dealt with at point of contact, and passed to Governance Services when staff are unclear whether the information should be released.

The SGO(RM) reported that the required out of office email automatic response was still not in use by all staff, and would circulate the current preferred wording to members to promulgate, and additionally would liaise with Information Services to explore the possibility to append the FOI message automatically.

08 Data Protection and Records Management Report to September 2016 UIGG(16/17)02

The SGO(RM) informed members that she had taken over the role of data protection officer, and that Governance Services would be recruiting a second Governance Assistant to deal with records management. She then spoke to the paper, highlighting the following points:

- There had been no data breaches during the reporting period, although one had been averted when an email sent to the incorrect recipient had been recalled by IS without being read.
- The Information Commissioner's Office had levied a record £1.5 million in fines, and that increasing fines were likely in order to match the penalties under the EU General Data Protection Regulation (a maximum fine of 4% of turnover, capped at €20 million). Breaches of particular note to ENU were:
  - An email containing sensitive personal data sent to the incorrect recipient (£150,000 fine)
  - Documents left in an abandoned building (£100,000 fine), which highlighted the importance of effective records management with the future move of support staff to the Stones
  - A laptop containing sensitive personal data stolen from an employee's home (£15,000 fine), which highlighted the importance of securing mobile devices either by using encryption or accessing university systems remotely.

  The group discussed issues relating to the security of mobile devices. The Information Security Manager thanked those staff already using encryption to secure devices and emphasised the need for University-owned devices to be sent to Information Services to be properly set up. The Clerk would discuss with Procurement regarding sending an email to purchase card holders and Agresso users to encourage this. Users with existing devices could contact the IS Service Desk to arrange.

  It was re-iterated that the Virtual Desktop Service was the most secure method to access University systems.

  The issue of reaching students was raised, particularly those involved in research projects which required access to personal data. It was suggested that information governance could be promoted to students through Ethics Committees, as well as via their supervisors through workshops or the Research & Innovation Office conference. The SGO(RM) would also liaise with the Professor of Hospitality & Tourism Management and the Head of Student Administration to explore developing an ethics requirement form which would promote IG best practice.

- While the effect of Brexit on adoption of the EU GDPR was currently unclear, any UK data protection legislation would likely need to comply with EU regulations. The SGO(RM) was liaising with staff across the University to conduct Privacy Impact Assessments, which were an important requirement of the GDPR and best practice in data processing. ICO had not yet provided detailed guidance on the GDPR, due to the uncertainty caused by Brexit.
- No subject access requests had been received during the reporting period.
- The new EU – US Privacy Shield arrangements for the transfer of personal data had been adopted, all University contracts with third parties in the USA would need to be compliant.
- Property and Facilities were negotiating with a new contractor to provide confidential waste console bins, including mobile consoles to offer a secure alternative to the use of confidential waste sacks.
- The staff data processing statement had been updated to account for the potential use of profiles for academic staff on the externally-facing staff directory.

- 63 requests from staff and students had been received over the reporting period, including a number regarding the new iPoints. The SGO(RM) recommended the use of screen privacy filters for staff PCs that were potentially in view of the public.
- Funding had been secured from the Leadership Foundation for Higher Education to update the Information Governance online training modules.
- The SGO(RM) commended Property and Facilities on the work in completing their records retention schedule, and noted that Finance were nearing completion on their RRS.
- The University had renewed the contract with ReStore for offsite storage for a further three years.
- School Support Services had implemented their Information Architecture Project, the SGO(RM) planned to invite a representative from the SSS to a future meeting of UIGG to discuss how the project was working in practice.

ACTION: All – Check if contracts with third parties in the USA comply with the EU-US Privacy Shield requirements.

09	**Information Security / Network and Security Services Report**	**Oral Report**

The Information Security Manager reported on current information security issues:

Work was underway to remove local administrator rights from staff PCs. These rights allowed staff to install programs and modify system settings on their own PCs, and was considered incompatible with the University's information security requirements.

IS were investigating methods to improve password management within the department, e.g. to audit the use of IS administrator credentials. Any system put in place by IS could potentially be rolled out to other areas of the University. A self-service system for user password management and recovery is currently available online to staff and students.

IS were developing systems for mobile device management to centrally control system settings of University owned devices. There were potential issues, such as the requirement that IS be aware of all University owned devices, and the ethical and privacy issues of controlling personal devices. Access to some systems or data may have to be restricted to University devices or via the Virtual Desktop Service, if it was determined that a personal device could not be adequately secured.

The ISM was reviewing information security policies and training materials which needed to be updated, and was liaising with Human Resources to promote mandatory IS training.

The ISM was to deliver a briefing to Research Integrity Committee on information security, and was liaising with the Schools to ensure compliance with Government requirements for research funding.

Email continued to be the main source of day to day threats, with some university accounts having been compromised and used to send phishing emails and malicious attachments. There was a need to raised awareness with staff of the issues and risks involved. IS were gathering information from staff who had been victims of phishing emails, to refine their warning messages accordingly. It was considered important to promote the message that staff would not get into trouble for reporting these issues.

10	Information Services Project Updates	Oral Report

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

Remote Access to Data Project.
This project seeks to address the security concerns with off-campus working by providing staff with easy to use, secure access to University systems and records across a variety of devices for both individual and collaborative use, as well as controlled third party access and a secure offline working environment. The broad requirements of the project were thought likely to result in a suite of systems to provide the overall service.

Information Services had gathered the requirements and sent out enquiries to a number of suppliers, with the plan to be able to produce a shortlist within two to three weeks.

Office365 for Staff
The project was ongoing with a plan to take a phased approach to rolling out Office365 to staff, beginning with moving staff email to the cloud. Initial testing was underway, with IS developing further test plans, e.g. for generic mailboxes. The University had become part of a Fast Track scheme with Microsoft, which offered access to additional expertise.

The project was in an early stage and, as a managed service, Office365 presented some potential information governance issues which have been captured in a dedicated governance and security workstream and would be discussed further.

Next meeting date

Currently scheduled for **Tuesday 21 February 2017**, at **2.00pm**, in the **Siegfried Room, Craiglockhart Campus**.