Edinburgh Napier
UNIVERSITY

UIGG(15/16)13

EDINBURGH NAPIER UNIVERSITY
RISK, RESILIENCE AND AUDIT MONITORING COMMITTEE

UNIVERSITY INFORMATION GOVERNANCE GROUP

Minutes of the meeting held on Tuesday 13 October 2015
at 2.30pm in the Siegfried Room, Craiglockhart Campus

Present
H Mizen (Senior Governance Officer Data Protection & Legal)[Co-Convenor]; D Watt (Senior Governance Officer, Records Manager)[Co-Convenor]; J Baillie (Campus Support Assistant/Technician); C Biggar (PA to Principal); B Cameron (Interim Head of HR Strategy); E Clark (Governance Assistant); A Deegan Wood (Planning Officer); J Dickson (Faculty Quality Advisor); S Duncan (Head of Campus Services); L McElhone (Head of Student Administration); B Merchant (Portfolio & Services Engagement Manager); L Smith (Operations Support Manager)
Apologies
R Bews (Appeals, Complaints & Conduct Officer); D Cloy (Assistant Secretary); O Dellal (Assistant Faculty Operations Manager); G Ferguson (Director of Property & Facilities); N Kivlichan (Head of Market Intelligence and Evaluation); L Mabberley (Assistant Director Marketing Brand and Communications); J Moxey (Network Services and Security Manager); A Ramsay (HR Adviser Team Leader); G Sharkey (Faculty Director for International Developments); Simona Simeone (Assistant Faculty Operations Manager); D Spiers (Lecturer); C Sutherland (Systems Officer); N Turner (Head of Research and Innovation Office)
In Attendance
D Dack (Campus Manager) [For items 12 and 13 taken at the start]; M Mackay (Administration Assistant)[Clerk]
Opening Remarks
Members were welcomed to the first meeting of the new academic year, and a specific welcome was extended to B Cameron, who was attending her first meeting. The apologies were **noted**.

1	Remit and Constitution	UIGG(15/16)01

The remit of UIGG remained unchanged from the previous session. The administrative changes to the constitution were **noted** and an additional change was agreed to combine the listing of nominees from IT Services and Library Services to Information Services.

The Group discussed further changes required following the academic re-structuring which took effect on 1 August 2015, had abolished the three faculties, created six Schools and an overarching School Support Service. Members agreed that replacing the previous Faculty representatives with a School representative from each campus would be the pragmatic way forward and that School Manager would be an appropriate level for these.

It was agreed that the SGO (DPL) would contact the Director of the School Support Service to discuss representation.

The Group discussed the potential for increasing the number of academic representatives on UIGG. It was commented that there had been difficulty with engagement from academics in the past. The SGO (DPL) was due to set up a meeting with the Head of Research and Innovation Office to discuss information governance issues arising from research projects and would also raise appropriate representation on UIGG.

2	Membership	UIGG(15/16)02

Members **approved** the current membership of UIGG, subject to the comments made in 1. above.

The next two items were discussed out of agenda order to allow the attendance of D Dack, Sighthill Campus Manager, (SCM) Property & Facilities Services.

12	Use of Body-Worn Radio Audio Recording	UIGG(15/16)08

The SGO (DPL) introduced the SCM who spoke to the paper. It was noted that this comprised a proposed draft policy statement and operational guidance on the use of body-worn radio audio recording systems, both of which were intended to be as straightforward as possible. The Group was advised that a reference to the making of such recordings had been added to both the staff and student data protection fair processing statements.

The Group noted that the University used TRBOnet, a digitally encrypted secure system for day to day communication across the University's estate which had the facility to activate audio recordings and that Security staff had been trained in the use of the system. The recording function would be activated by Security Control at the request of the wearer, although a 'Man Down' facility could also be used in an emergency situation, reference to which should be added to the guidance.

The operating procedure would be for the wearer to warn those present that recording would be activated before then requesting the recording and again, once recording had started. The current system was capable of recording for a maximum of two minutes and would be usable anywhere on the University estate where Security had a presence, including the University grounds and student accommodation.

The system would be used in addition to CCTV and the data gathered would be treated similarly to CCTV images, with regard to secure and appropriate record retention and disclosure requirements. As with CCTV images, the audio recording system had been set up to routinely store data from recordings on campus for 14 days and from student accommodation for 28 days. There was also the capability to download data as required for evidential purposes, for secure storage in the Security Control safe and unless otherwise required, would be kept for six months and then destroyed in accordance with the Safe Disposal of Confidential Waste.

In response to queries: the SCM advised that Security staff radios, and therefore the audio recording system, were reliant on the University's network and that Security had been working with Information Services to set up the system and; the SGO (DPL)

confirmed that the use of the facility as proposed conformed with legal and evidential audit requirements but agreed to make this clearer in the text.

The revised guidance would be circulated to members prior to going to RRC for approval.

| 13 | Update on Review of CCTV Code of Practice | Oral Report |

The SGO (DPL) informed members that in May 2015 the UK Information Commissioner had issued new guidance on the use of CCTV, which had been referred to the Security Team for review with reference to the University's CCTV Code of Practice. The SCM advised that this review had been done and no substantive revisions were required. However, as the use of Unmanned Aerial Devices, i.e. drones, had not been covered in the University's code to date, it was agreed that a section on this should be added. The Group noted that there had been recent requests for a policy or University guidance on the use of drones as a result of which the Health and Safety Team had been consulted. The University Secretary's view was being sought on the best way forward with this.

| 3 | Minutes of the Meeting held on 02 June 2015 | UIGG(14/15)18 |

Members **approved** the minutes of the meeting on 02 June 2015 as an accurate record.

| 4 | Matters Arising from the Minutes |

a) Minute 2a) – Information Governance Newsletter. The Senior Governance Officer (Records Manager) informed the Group that the second Information Governance Newsletter had been issued. 'Click-through' statistics were increased from the previous newsletter, with Records Retention Schedules being the most accessed link.

   60 responses had been received to the newsletter survey, and had highlighted a need to further promote the IG training offered. The upcoming Information Security Roadshows with Information Services would offer an opportunity to do so.

b) Minute 2c) – Policy Review Schedule. The SGO (RM) informed members that the ongoing review of policies was in compliance with the Schedule. The current schedule was available on the UIGG SharePoint site.

c) Minute 2d) – The Portfolio & Services Engagement Manager reported that the Information Security training module should be live by Friday 16th October. The modules would be University branded and accessible with a University login ID. Systems were in place to allow the University to track which staff had completed the training, and had read and indicated their understanding of policies. It was planned to use a series of emails to promote the training module to staff.

   Information Services were liaising with Human Resources to integrate these into the PDR process. Although as the PDR process was being reviewed, integration was unlikely at the current time.

   The current system was considered a proof of concept and could be built on in the future. The system could also be used to track access to external modules, such as the Information Governance training.

It was noted that:
- there was an audit requirement for all staff to have read and accepted the University's Information Security policy; and
- being able to demonstrate the training which was available and how this had been communicated/delivered to staff were important mitigating factors in the event of a data breach that was reported to or investigated by the Information Commissioner UK.

The SGO (DPL) sought suggestions on how to promote training, in particular to academic staff, whose take-up of IG training and engagement with the Information Security Roadshows was disappointing. Members suggested conducting training sessions specifically tailored to academics, or exploring other methods such as recording a briefing session and making it available online.

5	Information Security Roadshows	Oral Report

The PSEM informed members that another series of Information Security Roadshows would be held on consecutive in the week commencing 26th October 2015. The roadshows would be used to launch the Information Security Training Module, as well as promote training by Information Services and Governance Services, and the Virtual Desktop Service for students.

The roadshows would also feature advice on handling email attachments, securing mobile devices, privacy settings on apps and avoiding online security threats.

Provisional dates were being considered for further roadshows in January and April 2016.

6	Annual Report to Risk and Resilience Committee	Oral Report

The SGO (DPL) requested that members provide any input or comment for the Annual Report to the Risk and Resilience Committee prior to its submission for the meeting in November.

7	Access to Information Policy	UIGG(15/16)03

The SGO (RM) presented the Access to Information Policy Statement for review, and requested that members send feedback by 20 October, to allow any amendments prior to submission to RRC in November. It was noted that the statement contained a reference to Faculties, which would be removed.

8	Email Management Policy	UIGG(15/16)04

The Group approved the updated Email Management Policy Statement.

9	Records Management Policy	UIGG(15/16)05

The SGO (RM) presented the Records Management Policy for review and requested that members send feedback by Tuesday 20 October, to allow any amendments prior to submission to RRC in November.

| 10 | Records Manager's Report to September 2015 | UIGG(15/16)06 |

The SGO(RM) spoke to the paper and highlighted some points:

- The number of Freedom of Information requests was lower than the same period last year, but individual requests were tending to be increasingly complex.
- There had been no requests for review of responses during the period of the report, and all requests had been answered within the statutory deadline
- Information Services had received the highest number of requests
- Sector benchmarked statistics indicate that the University performs extremely well

- The Annual Report from the Office of the Scottish Information Commissioner showed similar trends to the previous year, and public perception of Freedom of Information was still positive

- Records Retention Schedules had progressed well, and the review under the UIGG Policy Review Schedule, as well as the academic re-organisation, offered an opportunity to standardise School RRSs, subject to the specific requirements of each school.

| 11 | Data Protection Policy Statement | UIGG(15/16)07 |

The SGO (DPL) presented the Data Protection Policy Statement for review under the UIGG Policy Review Schedule. The Statement had not been amended from the previously approved version, but would require a comprehensive review when the new EU regulation was published.

| 12 | Use of Body-Worn Radio Audio Recording | UIGG(15/16)08 |

The SGO (DPL) introduced the SCM who spoke to the paper. It was noted that this comprised a proposed draft policy statement and operational guidance on the use of body-worn radio audio recording systems, both of which were intended to be as straightforward as possible. The Group was advised that a reference to the making of such recordings had been added to both the staff and student data protection fair processing statements.

The Group noted that the University used TRBOnet, a digitally encrypted secure system for day to day communication across the University's estate which had the facility to activate audio recordings and that Security staff had been trained in the use of the system. The recording function would be activated by Security Control at the request of the wearer, although a 'Man Down' facility could also be used in an emergency situation, reference to which should be added to the guidance.

The operating procedure would be for the wearer to warn those present that recording would be activated before then requesting the recording and again, once recording had started. The current system was capable of recording for a maximum of two minutes and would be usable anywhere on the University estate where Security had a presence, including the University grounds and student accommodation.

The system would be used in addition to CCTV and the data gathered would be treated similarly to CCTV images, with regard to secure and appropriate record retention and

disclosure requirements. As with CCTV images, the audio recording system had been set up to routinely store data from recordings on campus for 14 days and from student accommodation for 28 days. There was also the capability to download data as required for evidential purposes, for secure storage in the Security Control safe and unless otherwise required, would be kept for six months and then destroyed in accordance with the Safe Disposal of Confidential Waste.

In response to queries: the SCM advised that Security staff radios, and therefore the audio recording system, were reliant on the University's network and that Security had been working with Information Services to set up the system and; the SGO (DPL) confirmed that the use of the facility as proposed conformed with legal and evidential audit requirements but agreed to make this clearer in the text.

The revised guidance would be circulated to members prior to going to RRC for approval.

13	Update on Review of CCTV Code of Practice	Oral Report

The SGO (DPL) informed members that in May 2015 the UK Information Commissioner had issued new guidance on the use of CCTV, which had been referred to the Security Team for review with reference to the University's CCTV Code of Practice. The SCM advised that this review had been done and no substantive revisions were required. However, as the use of Unmanned Aerial Devices, i.e. drones, had not been covered in the University's code to date, it was agreed that a section on this should be added. The Group noted that there had been recent requests for a policy or University guidance on the use of drones as a result of which the Health and Safety Team had been consulted. The University Secretary's view was being sought on the best way forward with this.

14	Staff Fair Processing Statement	UIGG(15/16)09

The SGO(DPL) spoke to the paper and the Group discussed a number of changes to the Staff Fair Processing Statement:
§2.6: a reference to the use of body-worn audio recording (minute 12 refers) had been added;
§2.7: it was suggested the wording be amended to ensure clarity that PA's would have access to the Outlook calendar and mailbox of the senior staff member they supported;
§3.4: the reference to HR Director's Depute would be amended to 'a direct report to the HR Director;
§4.1: it was noted that the public version of the staff directory would be available in the near future, and would include staff email and telephone numbers, but not photographs or room numbers;
§7.3: this had been added as a result of issues arising from staff leaving under the Voluntary Severance Scheme, the reference to Outlook folder would be amended to 'University email account' and a reference to C: drive would be added; the PSEM agreed to consult with relevant colleagues in IS on the proposed procedure;
§10.3: the SGO(DPL) would consult with the Head, Research and Innovation Office to ensure this was up to date;
§10.5: the reference to the UK Border Agency would be amended to UK Visa & Immigration

15	Student Fair Processing Statement	UIGG(15/16)10

The Group noted the Data Protection Statement for Students for session 2015/16.

16	Update on New EU Regulation	UIGG(15/16)11

The SGO (DPL) spoke to the paper. It was commented that while the key issues raised by the new EU Regulations were still to be determined, the resource implications were likely to be significant as University policies, procedures and processes would need to be reviewed to ensure compliance. Members were encouraged to raise the potential implications with their teams for discussion and feedback.

17	Data Protection Officer's Report to May 2015	UIGG(15/16)12

The SGO (DPL) spoke to the paper and commented that queries and requests for advice continued to be many and varied. Specific reference was made to:
- One University data security breach which had occurred during the reporting period; and
- A recently reported data breach which underlined the need for short-term/temporary staff to be trained and briefed in information governance compliance and University procedures

As an action following a data breach at the University in January, the Group discussed the sending of bulk staff and student emails. It was commented that all areas should have a policy and procedure for sending such emails, including system-generated ones, to ensure clarity over who should be authorised to send bulk emails and check/control their content. Consultation was underway, with Governance Services liaising with Corporate Communications. Members were invited to give their input to the SGO(DPL)

The Group also discussed access to University systems by staff who had left the University. The current process was understood to be that a monthly report of leavers was sent from Human Resources to Information Services (IS) so that leavers' access to University systems could be removed. The PSEM agreed to confirm the current process with IS colleagues and liaise as necessary to review.

18	Network and Security Services Manager's Report	Oral Report

The PSEM reported on current key work being undertaken by the Network and Security Services Team which included:
- The Information Security web pages had been updated;
- Penetration and vulnerability scans of the University's network were ongoing, no critical vulnerabilities had been identified to date. The network had been shown to be resilient to vulnerability testing by IS's contractor;
- A paper on information security vulnerabilities would be presented to the next meeting of UIGG;
- A new lost device procedure had been implemented, including advice on remotely wiping a lost or stolen device;

- Information Services had delivered bespoke training on encryption to the Department of Learning and Teaching Enhancement

19	Next meeting dates

25 February 2016 (Thursday), Room 6.B.14, Sighthill Campus
31 May 2016 (Tuesday), Room 7.B.14, Sighthill Campus

All meetings are scheduled to commence at 2.30pm.

20	Valediction

Members noted that G Sharkey would be leaving the University and the SGO (DP & L) thanked her on behalf of the Group for her contributions to its business.