UNIVERSITY OF GLASGOW

Information & Data Governance Group

A meeting of the Information & Data Governance Group will be held on:

Wednesday 3 October 2018 at 12:30 in the Principal’s Meeting Room

AGENDA

1. Minute of last meeting (paper 1)

2. Items for discussion
   - Avoiding email breaches - technical solutions (MJ) (paper 2)
   - Communications Plan for awareness raising (MJ) (paper 3)
   - Patch and Vulnerability Policy (DAW)

   Excerpt of IPSC minute 18 May 2018:
   “Dorothy Welch introduced the policy and explained that this was also a new one. A discussion followed on Section 4.1 relating to roles and responsibilities and whether the message was explicit enough in relation to individual staff ensuring that their own personal devices are kept secure and up-to-date. It was agreed that this should be clarified in the policy. Dorothy Welch will take it back to IDGG for further review and discussion.”

3. Items for formal approval
   - Data Protection Policy (paper 4)
   - Records Management Policy (paper 5)

4. Items for information
   - Data Governance pilot for HESA Data Futures (SMcD) (paper 6)
   - Data breaches quarterly report (JK) (paper 7)
   - Update on survey and event management tools (Bristol Online Survey, Eventbrite) (MJ/JK)
   - Update on Data Protection training progress (JK)
   - Update on Information Security online training progress (MJ)

5. A.O.B
6. Date of next meeting – December 2018

Last modified on: 27 September 2018
Version: 1.0
UNIVERSITY OF GLASGOW

Information and Data Governance Group

Minute of Meeting held on 3 October 2018 at 12:30 hours in the Principal’s Meeting Room, Gilbert Scott Building

Present: Dorothy Welch (Chair) (DAW), Johanna King (JK), Mark Johnston (MJ), Steve McDonald (SMcD), William Nixon (WN), Craig MacDonald (CMacD), Helen McKellar (HMcK) (Clerk)

Apologies: Jane Townson (JT)

DAW introduced the meeting advising that the membership of the group had been streamlined to align with the Group’s remit.

1. Minute of last meeting

The minute was agreed as an accurate record.

DAW noted that the IT Monitoring Policy and IT Regulations agreed at the last IDGG meeting had subsequently been approved by IPSC.

2. Items for discussion

Avoiding email breaches – technical solutions

MJ introduced the paper on reducing email breaches explaining this explored all the different approaches that could be taken, although some would be more technical and difficult to implement. MJ’s recommendations are, firstly, a proposal to add (STUDENT) to the display name. Secondly, on which MJ sought input from the Group, utilising MailTips to highlight or remove student addresses from an email before sending. The Group agreed the first option would be preferable as a succinct visual reminder that an email included student recipients. MJ confirmed there was no plan to add (STAFF) to staff accounts as this would be visible to external recipients as well.

CMacD raised that inclusion of (STUDENT) may be less desirable for research students trying to build a portfolio, a group the University had already distinguished by providing an “@research.gla.ac.uk” email address. The Group noted this point but regarded the inclusion of (STUDENT) as the optimal solution at present. DAW asked that this be implemented and views could be sought by way of evaluation after three to six months. MJ to advise of an estimated timeline for implementation.

Action: MJ

JK raised the risk presented by the auto-populating of email addresses but the Group viewed this as a functionality most staff find useful.

DAW stated that it would be necessary to advise staff and students that the addition of (STUDENT) to email addresses would be happening. WN suggested that the Information Security and Data
Information & Data Governance Group

Protection training could be included in an item in MyCampus News and MJ added that it could be promoted in an all-staff email planned regarding the Information Security training.

Action: MJ

Communications plan for awareness-raising

MJ introduced his proposal for raising awareness of the Information Security training module, including inserting the course into the current PDR cycle and its inclusion as one of the training opportunities PGR students are to be directed to by the Graduate Schools. MJ agreed to co-ordinate with the DP & FOI Office in order that Data Protection training can be embedded in the Graduate Schools as appropriate too.

MJ suggested it would be beneficial to have a discussion with HR to see if use could be made of Core for reporting on progress with the Information Security training module. DAW agreed to raise this with Christine Barr. Additionally, DAW agreed to address the other actions listed on the Communications Plan.

Action: DAW

JK advised it may be helpful to seek input from Liz Buie in the Communications Team regarding point 7 of the paper’s Communication Plan as she had provided direction on the timing of GDPR training.

More general discussion of communication followed, with the suggestion that there would be value in moving all the information policies and associated documentation to a single site as oppose to the current situation where they are linked and embedded in other documents. CMacD suggested a “What’s New” section of the Governance webpages and the Group agreed relevant new policies should be added there.

Action: MJ/JK

Patch and Vulnerability Policy

DAW advised this policy had been updated in line with comments from IPSC and thanked Chris Edwards for making the required amendments.

3. Items for formal approval

Data Protection Policy

JK introduced the Data Protection Policy, advising there had been significant revisions to the policy, not just to reflect the change in legislation to GDPR, but also to highlight the responsibilities of all staff. The Group agreed to pass the policy to IPSC for approval subject to an amendment to Section 3.4, regarding Heads of Academic/Service Units’ responsibilities, to read “ensuring compliance with this Policy in their capacity as Head of Unit”. Additionally, in Section 5.1, the effective date of GDPR training becoming mandatory to be noted as “current academic year”.

Action: JK/DAW

Records Management Policy
Information & Data Governance Group

JK advised the most significant changes to the Records Management Policy were the responsibilities placed on all staff, e.g. to follow the data minimisation principle and to put agreed retention schedules into practice in their areas.

The Group agreed to pass the policy to IPSC for approval, subject to amending the second point under Section 4.3 to read “promoting good records management practice locally”. Furthermore, DAW suggested an addition to the Appendix of some examples of what constituted (and did not constitute) a record. CMacD added that examples of good practice would aid staff in their understanding of the policy and JK agreed that the policy could be supplemented with a relevant case study on the DP & FOI Office webpages.

Action: JK/DAW

4. Items for information

Data Governance pilot for HESA Data Futures

SMcD presented an update on the data governance management solution that has been going through implementation over the last three months. The aim is to increase the function of data governance across the University by adopting common practices and mitigating the risk from systems being overly burdensome. SMcD described the University has having a “contingent” operating model, whereby there is no single process or technology model that fits the University and its data. SMcD described the Technology Supported Operating Model that would enable key areas to improve through the use of technology, e.g. profiling their data and undertaking change impact analysis. A University Report Catalogue would assist staff in understanding what types of data and reports can be accessed across the University and the Report Certification and Approval Workflow would allow experts to approve reports as the certified correct data. SMcD advised the system (Alteryx) is intuitive to use, however, it is proposed to offer functionality workshops and develop a communications plan.

SMcD asked the Group for their thoughts about how to engage user groups and key tasks for user groups, covering data owners and system owners as well as consumers of data. MJ intimated he would value a more detailed conversation with SMcD on this topic as he saw scope for more roles to be brought out. SMcD also asked for further discussion with JK to cover data protection matters.

SMcD requested the Group be mindful of any instances of new systems or data uses that could benefit from having data governance principles engrained into processes and project initiations. MJ reflected that having a process for project-driven change could aid in identifying such opportunities. JK added that it would be valuable to embed data protection considerations at these times as well.

CMacD commented that it would be helpful to bring in user stories to illustrate how the system could support staff at School level.

Action: SMcD/MJ/JK, all

Data breaches quarterly report

JK advised there had been 24 data breaches logged in the first quarter since GDPR came into force on 25th May. Of these, the majority involved human error, for example where emails had been sent to the wrong recipients, but there were also those that indicated a requirement to change processes, e.g. not using windowed envelopes to issue sensitive mail. There has been an issue with time being lost due to breaches not being immediately reported, or with full details not being
disclosed at first contact with the DP Office. In order to mitigate the risks of receiving incomplete information at first report, the DP & FOI Office has identified a need for a script to ensure all the relevant information will be requested at the first opportunity and the same data requested by all members of the team.

JK noted the DP & FOI Office has specific points of contact in some areas, such as with the Communications Team, and highlighted it would be helpful to have similar contacts in IT, where someone knowledgeable about the area could co-ordinate where breach management requires IT involvement. MJ responded that IT Services have been working on a Major Incident Management process which is to be taken to IPSC, whereby such incidents can be raised to the IT Senior Management Team and there could be scope for this to dovetail with the breach handling requirements. MJ agreed to discuss these requirements further after the IPSC meeting. JK added the ongoing necessity of awareness-raising in order that breaches are swiftly identified.

Action: JK/MJ

Update on survey and event management tools

MJ provided an update that Bristol Online Surveys are now owned by JISC and there have been some concerns regarding the terms and conditions. MJ proposes to have a meeting with Kirsty Scanlan and Sara Somerville to look at how BOS can be made more consumable across the University. MJ also noted he had met with Alistair Wilson, Claire Munro and JK on 15th August to discuss a list of third party systems where their terms and conditions are not GDPR compliant but there is a business need for the services/functionality that they offer. MJ indicated that CRM is central in providing a solution to these issues; however, such a project would affect everyone across the University. MJ proposes to work with Chris Ellis to look at core requirements for CRM and initiate a project to take to IPSC.

JK reported that the DP & FOI Office, along with the Contracts Team, are experiencing difficulties with advising staff that systems are not GDPR compliant but are unable to provide a suitable alternative. This presents a very real danger that staff will use these systems anyway. DAW advised that the risk of using some systems would be higher than others and needs to be balanced with the business need, with any decision to use such systems being documented to show a case had been made.

Action: MJ

Update on Data Protection Training progress

JK reported 844 participants had completed the online GDPR training module so far, with only one negative feedback comment received.

Update on Information Security online training progress

MJ reported 415 staff, 2 PGR students and 9 other students had completed the online Information Security training course, roughly equating to 100 people per month.

5. A.O.B.
Information & Data Governance Group

None.

6. Date of next meeting

The next meeting of the IDGG is due to be scheduled for December 2018.