AGENDA

**Items for discussion**

1. Framework for information governance policies (MJ) (paper 1)
2. Policy dissemination and awareness raising (MJ) (paper 1)
3. Update on Information Security online training module (CE)
4. Survey, event management and polling, and bulk-emailing tools (JK/SH) (paper 2)
5. Avoiding breaches by email (DAW)

6. **Items for formal approval**
   - IT Monitoring Policy (CE) (paper 3)
   - 2018/19 IT Regulations (MJ) (paper 4)

7. **Items for information**
   - HESA Data Futures (SMcD/DAW)
   - GDPR preparedness update (DAW)
   - Data Governance platform (SMcD)
   - Data protection modules used by other HE institutions (JK/SH)

8. A.O.B
9. Date of next meeting – August/September 2018

*Last modified on: 18 April 2018
Version: 0.2*
UNIVERSITY OF GLASGOW

Information and Data Governance Group

Minute of Meeting held on 25 April 2018 at 10:00 hours in the Principal’s Meeting Room, Gilbert Scott Building

Present: Dorothy Welch (Chair) (DAW), Chris Edwards (CE), Mark Johnston (MJ), Craig MacDonald (CMacD), William Nixon (WN), Anna Phelan (AP), Jane Townson (JT), Stacey Harper (SH) (Clerk)

Apologies: Johanna King (JK), Steve McDonald (SMcD), Alison McGuiggan (AMcG)

1. **Note of last meeting**

   The note was agreed as a correct record.

   The Information and Data Governance Group remit has been reviewed and approved.

   The IT Systems Patching and Vulnerability Management Policy had been amended and circulated. The policy had been approved and will be presented at the next meeting of the Information Policy & Strategy Committee (IPSC).

2. **Framework for information governance policies and policy dissemination and awareness-raising**

   MJ presented the Information and Data Governance Group High Level Policy Review paper, aimed at both identifying gaps in University of Glasgow information governance policies and raising awareness.

   **Awareness-raising**

   The Group agreed that staff, postgraduate research students and affiliates should be targeted for awareness raising and mandatory training on information security and management. While training will initially be promoted to support GDPR compliance, completion should be policed through the annual Performance & Development Review process. Graduate Schools would ensure completion of training by PGR students. A recommendation will be made to IPSC regarding the linking of training and PDR.

   MJ will review the communications plan for implementation in awareness-raising to the targeted groups and bring a revised version to the next meeting of the Group.

   **Action: MJ**

   **Comparing policy frameworks**

   The Group discussed the findings: MJ had identified a gap regarding the managing of assets owned by the University but not maintained by standard builds, including systems at external organisations or campuses, and Apple products. The Group agreed that guidelines – rather than policies – should be developed to cover different devices, systems, and activities and incorporated into training.

Page 1 of 4
The following points were agreed, based on observations in the above-titled section of the paper:

- The current practice of treating staff and student passwords the same is appropriate.
- Data sharing agreements should be put in place for third party access to sensitive data rather than any additional policy.
- Summaries of each information governance policy should be drafted to guide users.
- Payment card security and PCI-DSS compliance should be dictated by a Finance policy, not an IDGG policy.

The Group agreed that guidelines and awareness-raising on information security and management should extend to physical security.

3. **Update on Information Security online training module**

CE reported on the feedback he had received from members and others on the Information Security training module. That included concern over the length and the number of clicks involved, and a need for more focus on what individuals needed to do (practical guidance) rather than theoretical advice. CE will make minor amendments and attempt to shorten the training before a roll out to select Schools and Services ahead of the 25 May GDPR enforcement date. AP will look into making the module available via Core. The training will be launched (softly) in the summer, as part of the preparation for GDPR, with completion made mandatory thereafter, to be picked up in the 2019 PDR exercise. It was agreed that the pass mark should be 60% at least in the initial phase.

**Action: CE & AP**

4. **Survey, event management and polling, and bulk-emailing tools**

The Group identified that staff across the University utilise various online management tools for their functionality and ease of use. However, there are data protection implications for sharing personal data with the companies who manage these tools. Wherever possible, staff should be directed to local services, e.g. University-managed bulk-emailing options. If no local options are available, data sharing or contractual agreements should be developed with identified online services. Disclaimers advising staff to use online services at their own discretion should be drafted as a last resort.

MJ will review access to the Bristol Online Survey tool and discuss availability and access options with current licence manager, Kirsty Scanlon. The DP & FOI Office will review the possibility of a data sharing agreement with Eventbrite, as that has proven to be the most popular and functional event management service used by staff. It was acknowledged that polling software (for meetings) represented a low risk.

**Action: MJ/JK**

5. **Avoiding email breaches**

The Group discussed how the current email management system makes it difficult to distinguish between staff and student email addresses, and as a result students can receive emails intended for staff: this represented the highest incidence of reasons for data breaches. Suggestions for avoiding these breaches included separating staff from student emails in the global address books, or adding...
Information Governance Group

a “student” or “staff” suffix to an email address. MJ will provide a paper for the next meeting on possible technical solutions.

Action: MJ

6. Items for formal approval

IT Monitoring Policy

The Policy will be approved and sent to IPSC following minor amendments:

- Removal of section 3.3
- Section 4: Removal of first sentence in paragraph one and revise to “Chief Operating Officer and University Secretary” title.
- Annex A: Clarification that systems listed under “IT Services and Applications” are not an exhaustive list and removal of “Physical monitoring” section

Action: CE

2018/19 IT Regulations

The IT Regulations were approved and will be presented to the next IPSC meeting.

7. Items for information

HESA Data Futures

The HESA Data Futures programme will allow HESA to harvest data on a rolling basis rather than receive an annual data upload from the University. A working group is in place to discuss this change. To be discussed further at the next IDGG meeting.

Action: SMcD

GDPR Preparedness

DAW noted briefly that the University’s GDPR preparedness is moving forward with focus on priorities and biggest implementation challenges.

Data Governance platform

In SMcD’s absence, DAW advised that supplier demos would be available in May.

Data protection modules used by other HE institutions

SH informed the Group that, in most instances, colleagues in other HE institutions are still looking at data protection training options. In lieu of a bespoke module, University of Edinburgh has made their training slides available online with a voiceover script. The DP & FOI Office is considering implementation of a similar training format.

8. A.O.B.

None
9. **Date of next meeting**

The next meeting of the IDGG is due to be scheduled in August or September 2018.