UNIVERSITY OF GLASGOW

Information Governance Group

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

Tuesday 20 June 2017 at 14:00 in Sandy MacDonald’s Office, Room 321, James Watt North Building

AGENDA

1. Minutes of meeting held on 19 April 2017 (DAW) (paper 1)
2. Matters arising
   - Guidance on scanning (JK)
   - Information Commissioner’s Office Review (JK)
   - Retention of HR data (JK)
3. 2017/18 Computing Regulations (SMacD) (paper 2)
4. Information Governance Policies
   - 4.1 Digital Preservation Policy (WN) (paper 3)
   - 4.2 Cloud Storage Policy (CE) (paper 4)
   - 4.3 Network Connection Policy (CE) (paper 5)
   - 4.4 Bastion Host Policy (CE) (paper 6)
5. Communication strategy for IGG outputs (AP/CE/SMacD) (paper 7)
6. A.O.B
7. Date of next meeting – September 2017

Last modified on: 15 June 2017
Version: 1.0
UNIVERSITY OF GLASGOW

Information Governance Group

Minute of Meeting held on 20 June 2017 at 14:00 hours in Sandy MacDonald’s Office, Room 321, James Watt North Building

Present: Dorothy Welch (Chair) (DAW), Johanna King (JK), Chris Edwards (CE), Sandy MacDonald (SMacD), Alison McGuigan (AMcG), William Nixon (WN), Stacey Harper (SH) (Clerk)

Apologies: Anna Phelan (AP)

1. Minute of meeting held on 19 April 2017

The Group agreed that the minute of the last IGG meeting provided an accurate record of that meeting.

2. Matters arising

Guidance on scanning

JK advised that work has not progressed on staff guidance for scanning. She will draft a high-level guide, and present it at the next IGG meeting.

Action: JK

Information Commissioner’s Office Review

JK reported that she was contacted by the ICO on Friday 16 June, offering a visit in November/December. The Group discussed whether inviting the ICO to review the University’s compliance would detract from GDPR preparation or if it would offer any additional assistance to that of the Pricewaterhouse Cooper audit. JK will discuss the requirements of the Review directly with the ICO, and report back to the group.

Action: JK

Retention of HR data

JK informed the Group that she had contacted HR to progress record deletion in Core. HR cannot commit to the project until their planned update of Core at the end of 2017. The Group expressed concern that excessive retention of personal data has data protection and GDPR liability implications. SMacD indicated it may be possible to manually delete records. AP will investigate options for manual deletion.

Action: AP

3. 2017/18 Computing Regulations

SMacD reported that only minor changes are required to be made to the existing Computing Regulations. It was agreed that changes would be made to paragraphs 20 and 22, where the
Information Governance Group

document makes out-dated references to the “Policy on Confidential Data” and the “Secretary of Court” respectively. SMacD will amend the references and put a new date on the document footer.

Action: SMacD

4. Information Governance Policies

4.1 Digital Preservation Policy

WN presented a slightly revised version of the Digital Preservation Policy, with an amendment to section 4.2 and an expansion of the policy’s scope in section 2. WN advised that the University is now digitising postgraduate research theses and some student research data, so PGRs will be included in the last paragraph of section 2.

WN also advised that the Digital Preservation Working Group views this policy as a framework and is now ready to use it as a foundation for practical work such as the JISC pilot discussed in the 19 April IGG meeting and various record audits.

SMacD suggested that section 4.2, paragraph 2 should open with “Guidance and related policies will be created...” as policies will have more authority in impelling staff compliance.

With the incorporation of SMacD’s suggestion and the inclusion of PGR students in scope, the Group was content to approve this policy. It will be presented at the next IPSC meeting.

Action: WN

4.2 Cloud Policy

CE introduced the revised Cloud Storage Policy, stating that the Policy is no longer focused specifically on cloud storage, it is now a Cloud Policy incorporating all cloud activities. He further indicated that the policy covers all key requirements for consideration with cloud use, including risk assessment, appropriate consultations and contracting with cloud providers. A number of comments had been sent directly to CE from AP.

The inclusion of section 9 was queried by JK; CE advised that it is a relevant and important section as it flags the risks of synchronisation across devices and highlights the necessity of appropriate security precautions. The Group agreed that this section should remain in the policy.

Section 5 was discussed, with DAW noting that a list of approved cloud providers could raise complications by necessitating regular updates to the policy as the list changes. The Group agreed that it must be easy for staff to know which providers they can use, but the policy must also be kept up-to-date. WN proposed retaining section 5, but altering the wording to explain that the providers listed are the recommended providers for general purpose cloud activities. The Group agreed with this suggestion.

DAW requested the removal of the final bullet in section 7d.

CE will make the required amendments and circulate the policy for approval ahead of the next IGG meeting.
4.3 Network Connection Policy

CE introduced new draft of Network Connection Policy, with a new summary at the start of the policy.

JK suggested a one-page accompanying guidance document to highlight the key points and requirements of the policy for the benefit of general staff.

CE proposed and will present a paper that merges the summaries from all revised policies onto one document for ease of communication to all staff.

The Group agreed that the recent WannaCry ransomware attack highlighted the need for both this policy and the ability to enforce it. SMacD recommended seeking authority from IPSC to restrict access to the University network for staff who are not compliant with this policy. CE will draft a proposal for presentation at the next IPSC meeting.

The Group approved this policy.

Action: CE

4.4 Bastion Host Policy

CE added a summary to open this policy. The Group agreed that the name of the policy should be changed; CE proposed “Server Management and Configuration Policy”. The policy was otherwise approved by the Group.

Action: CE

5. Communication strategy for IGG outputs

CE presented the Communication Strategy as a document intended to describe the audiences IGG should reach and the appropriate channels for communicating developments, and offering a checklist of steps to take for communication. SMacD recommended that the document should be amended as the Group gains experience in communicating to the University.

The Group agreed that an information governance website would be a useful tool for communication, but not an Information Governance Group site as written on the document. JK suggested that until awareness is suitably raised across the University, the Group should follow the same steps for communicating updates to existing policies as are laid out for launching new policies. This would help address the gap in staff recognition of current policies.

DAW advised that communication should focus on user need, and requested consultation with and involvement from Phil Taylor and Tasha Quinn in the Communications and Public Affairs Office.

Action: AP, CE

6. A.O.B.
Information Governance Group

The Group discussed implementing mandatory staff training on information governance. It was agreed that this would be important for critical policies with which staff must be familiar and compliant. It was suggested that the issue of mandatory training, in relation to evidencing adequate training and awareness, may be raised as part of the forthcoming PwC Audit on GDPR Readiness.

7. Date of next meeting

The next meeting is to be scheduled for September 2017, in advance of the 25 September IPSC meeting.