UNIVERSITY OF GLASGOW

Information Governance Group

A meeting of the Information Governance Group will be held on:
Wednesday 11 January 2016 at 14:00 in Sandy MacDonald’s Office, Room 321, James Watt North Building

AGENDA

1. Minutes of meeting held on 25 August 2016 (DAW) (paper 1)

2. Matters arising
   - Email retention policy implementation (SMacD)
   - CDocs migration (AP)
   - Guidance on scanning (JK)
   - Draft Guidance on Information Storage (AP)
   - Extraordinary Circumstances Access Policy update (CE/DAW)

3. Information Governance Policies
   3.1. Policy on Confidential Data Handling & Information and Risk Classification (CE) (paper 2)
   3.2. Mobile Device Encryption (CE) (paper 3)
   3.3. Cloud Storage Policy (CE/SMacD) (paper 4)
   3.4. Computer Equipment Disposal Policy update (CE/SMacD) (paper 5)
   3.5. Password Policy (CE) (paper 6)
   3.6. Network Connection Policy (CE) (paper 7)
   3.7. Bastion Host Policy (CE) (paper 8)
   3.8. IT Monitoring Policy (CE) (paper 9)
   3.9. CCTV Policy update (JK)

4. Update on Retention Policy Services pilot (AP)

5. Digital Preservation Policy (WN) (paper 10)

6. A.O.B
   6.1 Information Commissioner’s Office review

7. Date of next meeting – 19 April 2017

Last modified on: 21 December 2016
Version: 1.0
UNIVERSITY OF GLASGOW

Information Governance Group

Minute of Meeting held on 11 January 2016 at 14:00 hours in Rm 321 James Watt North Building

Present: Dorothy Welch (Chair) (DAW), Johanna King (JK), Sandy MacDonald (SMacD), Anna Phelan (AP), Chris Edwards (CE), William Nixon (WN), Helen McKellar (HMck) (Clerk)

Apologies: Alison McGuiggan

William Nixon was welcomed as a member of the Group, replacing Lesley Richmond.

1. Minute of meeting held on 25 August 2016

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

2. Matters arising

Email retention policy implementation

SMacD confirmed the policy had now been implemented and staff leavers can access email for 30 days from their leaving date, and emails are then retained for another 30 days prior to deletion. SMacD added the caveat that if a backup is taken during those 30 days this is then retained for a year. This will be subject to change should staff email provision move to Microsoft Office 365.

CDocs migration

AP advised the first phase of the CDocs migration is scheduled for week commencing 16th January 2017, whereby the content and metadata will be moved to Documentum. Access considerations will be addressed latterly.

Action: AP

Guidance on scanning

JK advised she had consulted with LR prior to her departure and no update had as yet been received from Estates and Buildings. LR passed on details of the relevant contact and JK will pursue this directly.

Action: JK

Guidance on Information Storage

AP reiterated the intention to circulate this Guidance document upon approval of the Cloud Storage Policy.
Extraordinary Circumstances Access Policy update

DAW advised the Group that this policy had been approved by IPSC subject to a minor amendment that has since been made. CE confirmed the finalised policy is now published online.

3. Information Governance Policies

3.1 Policy on Confidential Data Handling & Information Risk and Classification

CE reminded the Group of previous discussions regarding the Policy on Confidential Data and that a need for a definition or some classification of what the term confidential data encompasses had been identified. To this end, the Information and Risk Classification document had been drafted to help staff identify at a broad level the types of information they work with. The Group agreed this was a helpful approach, although there was some discussion regarding the number of risk levels into which information could be categorised. SMacD commented it would be best to retain the three risk categories to encourage a degree of discipline as regards all information handled at the University. The Group was asked to pass on any suggested examples to illustrate the risk categories to CE in advance of the next meeting where it was expected that the approach would be formally ratified.

DAW queried the status of the Policy on Confidential Data given the new focus on identifying risk categorisation. CE advised that the Risk Classification document may be a first step to replacing the Policy on Confidential Data; however, it requires to be revisited to extract those elements that should be retained or developed into separate guidance documents. CE to update the Group at the next meeting.

Action: CE, All

3.2 Mobile Device Encryption Policy

CE introduced the Mobile Device Encryption Policy underlining that this is an area where there is a definite requirement for advice and guidance. DAW queried the requirement for the Recovery Keys section of the document, and CE agreed to move this to the end of the document. Other suggested amendments included removing the sentence in parentheses in the third paragraph under Why It’s Important and that the phrase “may wish to” should be changed to “should” in the third paragraph under Recovery Keys. AP highlighted the risks associated with Office 365 syncing data onto mobile devices and suggested a reference to this should be added to Section 7 of the document.

The Group approved the policy subject to the above-mentioned minor amendments in order that the policy can be submitted to the next IPSC meeting.

Action: CE

3.3 Cloud Storage Policy

CE advised that, while the policy had not been updated since the last meeting, following the Group’s acceptance of the risk classification approach, this could be tied into the Cloud Storage Policy to help...
Information Governance Group

staff make decisions as to whether it was or was not appropriate to store their data within a cloud-based system. SMacD requested that this policy be held over until the next meeting as there is also a need to address how advice regarding research data is incorporated into the policy.

Additionally, AP queried whether a Privacy Impact Assessment had been undertaken in reference to the business case for moving staff email to Office 365. JK and CE confirmed a PIA would be required for such a project and that IT Services should draft this to pass to IPSC for consideration.

Action: SMacD, CE

3.4 IT Equipment Disposal Policy

CE advised that a new section had been added to the draft to cover the charitable donation of IT equipment. Within this procedure, the onus is on those groups wishing to make charitable donations to develop a procedure for carrying out such donations, with any procedure developed to be agreed with IT Services, the DP & FOI Office and Safety & Environmental Protection Services. AP suggested removing the requirement for written notes to be taken by a witness and leaving as Head of Service to confirm the device was not used to store high risk data. The policy was approved subject to the simplification of the procedure under Section 7. CE to make the required changes prior to submission to the next IPSC meeting.

Action: CE

3.5 Password Policy

CE introduced the revised Password Policy which had been reduced from eight pages to one page. DAW suggested changing the wording “passwords should be” to “passwords must be”. AP queried whether advice should be included on the use of password management software and CE agreed it required investigation and was on the roadmap for the future but would not be included in this iteration of the policy. Subject to the amendment mentioned, the Password Policy is to be submitted to the next IPSC meeting.

Action: CE

3.6 Network Connection Policy

CE introduced the revised Network Connection Policy, highlighting that this remains a technical policy as the main audience for the document are technical staff, with a requirement to understand the approved technical methods for connecting to the University’s networks. DAW queried whether this was a policy that would be required to be passed by IPSC or if it would be sufficient for it to be promulgated within the IT community at the University. CE speculated there may be a requirement for approval and further amendments. It was suggested the policy should be reviewed again, with CE to consult with College IT Managers prior to bringing the resulting outcome to the Group for approval.

Action: CE

3.7 Bastion Host Policy
Information Governance Group

CE advised the changes previously suggested by the Group had been incorporated into the policy, however, like the Network Connection Policy, this document is directed at a technical audience. DAW suggested both policies should be handled together and discussed with College IT Managers, prior to being brought back to the Group for approval.

Action: CE

3.8 IT Monitoring Policy

CE advised the IT Monitoring Policy had yet to be updated. DAW asked if it could be brought to the meeting after next.

Action: CE

3.9 CCTV Policy update

JK reported she had met with Gary Stephen, the University’s new Head of Security, and had discussed the ad hoc nature of CCTV presently in place at the University, with both parties keen to rectify this. Following on from this discussion, JK plans to revise the draft CCTV Policy with the aim of having two parts to the document, one for the operational and technical requirements to be taken forward by GS, and the legal framework to be taken forward by JK. JK is to provide an update at the meeting after next.

Action: JK

4. Update on Retention Policy Services pilot

AP reported that colleagues in Human Resources had advised that, due to competing priorities, they are unable to move forward as the pilot area for RPS at present, with availability reduced until at least April. AP also updated the Group about a change of ownership regarding the Documentum system, which has recently changed hands from EMC to Dell and then to Opentext. As such, AP feels it would be prudent to assess the new owners’ approach to Documentum before moving forward with Retention Policy Services as a bespoke Documentum product. JK reiterated that the need to tackle the HR records held within Documentum remains. AP agreed and advised that IT colleagues planned to investigate deleting documents via a different means rather than utilising RPS.

Action: AP

5. Digital Preservation Policy

WN presented the amended Digital Preservation Policy to the Group, advising that it references supporting policies that the Working Group has yet to develop. The Group agreed that the policy was a lot clearer and more focused than the previous draft. JK queried what was meant by the term “digital preservation solution” in section 4.2 and WN advised he would review this wording. WN reported that the Working Group had been investigating the Preservica system and an update could be provided for the next meeting. WN to advise the Group when the policy would be ready to pass to IPSC, with AP suggesting it may be helpful if more of the supporting documentation was available in advance of this.
6. **A.O.B.**

JK reported that the Information Commissioner’s Office had contacted the DP & FOI Office about a 2-day review visit, potentially to take place in November. The Group’s views were sought as to whether it would be beneficial for the University to participate. It was agreed it would be helpful to have more information regarding the scope of the ICO’s review. JK advised that the University’s response to the survey circulated would help inform the ICO as to the most appropriate areas to focus upon. JK would complete the survey, in consultation with CE, supplied by the ICO, and would keep the group advised of any developments.

**Action: JK, CE**

AP enquired whether Group members were aware of investigations into the use of the Board Packs system for committee papers. DAW advised Court Office were investigating the system but no purchase had been made at this stage. The Group would be updated of any developments regarding the use of this system.

**Action: DAW**

7. **Date of next meeting**

The next meeting is scheduled for 19 April 2017.