UNIVERSITY OF GLASGOW

Information Governance Group

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

Thursday 25 August 2016 at 15:00 in Sandy MacDonald’s Office, Room 321, James Watt North Building

AGENDA

1. Minutes of meeting held on 11 May 2016 (DAW) (paper 1)

2. Matters arising
   - Update on Documentum Implementation in DP & FOI Office (JK)
   - Email retention policy implementation (SMacD)
   - CDocs migration (AP)
   - Guidance on scanning (LR)

3. Draft Guidance on Information Storage (AP) (paper 2)

4. Committee papers storage (JK) (paper 3)

5. Information Governance Policies
   - 5.1. Extraordinary Circumstances Access Policy (formerly Access to absentee email accounts) (CE) (paper 4)
   - 5.2. Cloud Storage Policy (CE) (paper 5)
   - 5.3. Computer Equipment Disposal Policy (CE) (paper 6)
   - 5.4. Password Policy (CE) (paper 7)
   - 5.5. Network Connection Policy (CE) (paper 8)
   - 5.6. Bastion Host Policy (CE) (paper 9)
   - 5.7. IT Monitoring Policy (CE) (paper 10)

6. Update on strategy implementation: local records officer pilot (JK)

7. Update on Retention Policy Services pilot (AP)

8. Digital Preservation Strategy (LR)

9. A.O.B

10. Proposed date of next meeting

Last modified on: 18 August 2016
Version: 1.0
UNIVERSITY OF GLASGOW

Information Governance Group

Minute of Meeting held on 25 August 2016 at 15:00 hours in Rm 321 James Watt North Building

Present: Dorothy Welch (Chair) (DAW), Johanna King (JK), Chris Edwards (CE), Sandy MacDonald (SMacD), Anna Phelan (AP), Lesley Richmond (LR), Helen McKellar (HMcK) (Clerk)

1. Apologies

Alison McGuigan

2. Minute of meeting held on 25 February 2016

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

3. Matters arising

Update on Documentum Implementation in DP & FOI Office

JK confirmed, that for the reasons intimated at the previous meeting, the DP & FOI Office did not intend to migrate any further files to Documentum.

Email retention policy implementation

SMacD advised a meeting had been held to clarify the rules worked to and an outcome was expected in the next couple of weeks. The policy would be fully implemented by the next meeting of the IGG.

Action: SMacD

CDocs migration

AP advised the first phase of the CDocs migration had been specified with migration to Documentum to commence in September and access considerations to be addressed latterly.

Action: AP

Guidance on scanning

DAW and LR had met with Estates and Buildings and additionally LR and JK had met with Procurement to discuss the message given to staff subject to office moves. The current scanning vendor had been specifically selected to address the needs of the Tay House move; however, the contract will be under review within two years. Estates and Buildings intend to offer a “soft-landing protocol” to staff into which records management and scanning advice should be incorporated. LR and JK to input to soft-landing protocol.

Action: LR & JK
3. Guidance on Information Storage

AP advised the draft had been circulated to some information owners and had received good feedback, in particular that it had raised awareness about the different information services available to staff.

DAW suggested a change to the term “School Administrator” in the Case Studies to “Teaching Administrator” to avoid confusion with the Heads of School Administration role.

It was agreed that the Guidance should be publicised across the University, subject to the approval of the Cloud Storage Policy. Internal Communications would be consulted on the most appropriate way to raise awareness.

Action: AP

4. Committee paper storage

HMck introduced a document mapping the current practice regarding committee papers storage across the University. It was highlighted that, while a small number of committees utilise Documentum and SharePoint and the majority use network drives, there is a varied and inconsistent approach throughout the University, with some more concerning practices in place, such as storage of papers on Dropbox. DAW suggested that the Group could share these findings with the College Secretaries to discuss the potential for more uniform storage and publication; however, it was decided that this contact should not be made until there was agreement on the recommended practice. This related to the future strategy for the use of both Documentum and SharePoint as well as the feasibility of an ‘intranet’.

5. Information Governance policies

DAW consulted the Current Information Policies document to see what work was outstanding. JK confirmed the CCTV Policy would be brought to the Group later this calendar year. CE advised that, with regard to the Policy on Confidential Data, this policy’s potential coverage is very wide and, following on from the suggestion noted at the February meeting, he had identified that an area requiring some ‘mandatory guidance’ was that of mobile device encryption. He proposed that a policy was required to address the risk posed by the many staff who do not use the standard staff desktop with its inherent encryption. CE envisaged some parts of a mobile device encryption policy could be incorporated into the Policy on Confidential Data but he regarded a separate policy as necessary to set out how to deal with issues raised by the use of mobile devices.

A proposal for the way forward, including for the Policy on Confidential Information, would be presented to the next meeting.

Action: CE

5.1 Extraordinary Circumstances Access Policy

CE presented the latest draft of the policy, highlighting the addition of a section on the deletion of emails. CE and JK confirmed this was in response to a recent incident in a School which had
Information Governance Group

highlighted the lack of a protocol for IT staff in receipt of queries about email deletions. Rather than including this section in the policy it was agreed that an internal procedure should be developed for IT Helpdesk staff to follow if they receive such a request.

DAW asked that the title be changed to specify IT access, to avoid confusion with access to buildings etc. Additionally, she requested that the term “sick” be changed to “incapacitating” in the Criteria for allowing access under Section 3 and that the last sentence of the second last paragraph under Section 5 Formal Request Procedure be amended. Subject to these changes and the deletion of Section 7 relating to the deletion of emails, the Group approved the policy. The updated policy would be published and notified to IPSC.

Action: CE

5.2 Cloud Storage Policy

CE presented the latest version of the Cloud Storage Policy. Discussion followed regarding risk. SMacD suggested it would be helpful to look at the legal obligations Microsoft had signed up to: IT and DP & FOI Office colleagues would get together to review this. The Group agreed the policy should be reviewed following discussions around personal data in OneDrive.

Action: SMacD, AP, JK, CE

5.3 Computer Equipment Disposal Policy

CE introduced the draft IT Equipment Disposal Policy which was a revised version of an old policy. He acknowledged that the document did not address the disposal of IT equipment to charities for which there was a demand. It was agreed that an approval process with IT Services should be incorporated to enable charitable recycling and that laptops considered for donation cannot have been used for any confidential work. SMacD and CE agreed to revise the paper to incorporate these suggestions and that it would be circulated again in advance of the next meeting.

Action: SMacD & CE

5.4 Password Policy

CE introduced the draft Password Policy. It was noted that the style of this document was different from the other policies. It was agreed that the wording regarding disciplinary action under the Enforcement heading should be clarified so staff understand which parts of the policy are subject to disciplinary action. CE would revise and shorten the policy, in line with those previously agreed by the group, for review at the next meeting.

Action: CE

5.5 Network Connection Policy

CE introduced the draft Network Connection Policy. DAW expressed concern about the extent and length of the document and CE advised that most users would not need to read the full policy but that College and School IT staff would require these minimum standards. It was agreed that a
Information Governance Group

separate policy and guidance documents would be more helpful for users. Rather than tweaking the existing policy, the document would be rewritten with the audience in mind: separate documents for network administrators and for end users could be drawn up. CE would split and revise the document for its different audiences.

Action: CE

5.6 Bastion Host Policy

CE introduced the Bastion Host Policy. DAW recommended that, under the Policy section, the breakdown of “College, School and research group” should be reduced to just College and School/Research Institute with any research group requirements being sanctioned by the Head of School/RI. JK queried the audience as the information contained in the policy would appear to be in excess of end users’ requirements. CE advised the aim of the policy was to standardise the IT set-up in Colleges and Schools and to help in circumstances when researchers set up their own servers. It was agreed that the audience for the policy would be stated at the beginning of the document. CE would revise the policy for the next meeting.

Action: CE

5.7 IT Monitoring Policy

CE introduced the Network Service, Systems and Data Communications Monitoring Policy, which he explained was designed to fulfil the University’s requirement to inform system users of what monitoring activities are undertaken. It was agreed that the policy should be streamlined: there was scope for the policy to be more generic, for example, advising readers that the web may be monitored, but not exactly which data fields would be monitored. It was queried if the monitoring of printers was included within the policy as print logs, which include document titles, are retained indefinitely. The period that print or other monitoring logs are kept should be documented in a retention schedule rather than a policy. CE would revise the policy to provide a more end user friendly, high level overview of the University’s monitoring activities.

Action: CE

6. Update on Strategy Implementation: Local Records Officer pilot

JK reported that she had spoken to Alison McGuiggen from Planning and Business Intelligence to gauge the receptiveness to the Data Steward role, previously identified as having potential overlap with the proposed Local Records Officer role. There had been concern within the Data Quality Group that such a role could lead to the onus falling solely on named individuals, with others regarding themselves as exempt from assuming any responsibility at all: this could, likewise, apply to the LRO proposal. Alison had also advised that funding has been secured to employ a data capability expert to help define their requirements in relation to the role and responsibilities. JK will report back to the Group following the outcome of that meeting.

Action: JK

7. Update on Retention Policy Services pilot
Information Governance Group

AP advised that a meeting had been held with Ann Hastings of Human Resources to discuss the proposal of piloting RPS within HR: work would commence after completion of the current P&DR cycle. AP highlighted that there were potential linkage issues with the CORE HR system in terms of any resulting impact, or lack of update, to the CORE system following deletion of records held within Documentum. She noted that there was likely to be a cost associated with undertaking any work with the CORE system provider.

AP further advised that the Documentum team had undertaken conference calls with reference sites already using the RPS module. The most directly comparative user was McGill University in Canada. The Documentum team has subsequently installed RPS and plans to undertake formal training with a view to then passing that knowledge on to DP & FOI Office staff. AP to update the Group regarding progress at the next meeting.

Action: AP

8. Update on Digital Preservation Strategy

LR presented a draft Digital Preservation Policy to the Group and advised a Digital Preservation Strategy was to be developed over the next three years. Rather than a policy, the document was a statement of intent designed to show that the University recognises the need to retain and preserve its digital information. The group was unclear what requirements the policy was placing on staff at present. LR advised the main requirement at this stage was to identify what digital information needs to be kept, document it on a retention schedule and commit to retaining it until it can be put into the (as yet to be developed) preservation system. LR agreed to revise the policy to clarify its purpose.

Action: LR

7. A.O.B.

CE reported that IT Services are investigating an Information Security online training module that could be made available to staff through Moodle. The Group welcomed this development and asked to be kept updated as investigations proceed.

Action: CE

8. Date of next meeting

DAW requested a schedule of dates for the rest of the year, to allow for matters from the Group to be reported to the IPSC shortly thereafter.

Action: HMck/SH