



School IT Committee Meeting

Wednesday, 20th June, 2018

Present: Gordon Smith (Chair) (GS), Richard Bartlett (Secretary) (RB), Caroline Edmonds (CE), Matt Burgess (MB), Nigel Berryman (NB), Bertie Gottgens (BG), Andrew Leedham (AL), John Sinclair (JS), Guy Williams (GW), Mary Dixon-Woods (MDW), Chris Wallace (CW), Lydia Drumright (LD), Soren Brage (SB), Dennis Norris (DN), Nigel Berryman (NB), and Randy Read (RR)

1. Apologies: Guy Williams (GW) and Matt Burgess (MB)

2. Minutes of the Previous Meeting

The minutes of last School IT Committee meeting held on 28th March were approved.

3. Matters Arising

RB gave the Committee a brief progress update on GDPR. The UIS was now considering a priority modification of the Information Asset Register (IAR) to include research data, as (outside SCM) the University does not have properly managed records of what personal data was held as part of research (at present this was held in separate ethics committees minutes or similar unstructured data). RB added that he intended to find out more about these plans, and in particular, the design, impact and implications for SCM data.

RB had an action to present a paper to the next HoD meeting regarding the multiple requests from different users in the School to the UIS for new computational resource. RB reported that there had been a delay in getting the first draft to CW and he was now gathering information from HPC (Paul Sumption) about the outstanding requests to understand what the unsatisfied need was; and based on this evidence, he would present a proposal which was proportionate to the problem.

RB had a further action to request that a note was published in the Regius' School newsletter regarding BYOD, and he reported that this had been delayed due to a lack of response from Trust IT.

4. Policy

RB confirmed that there were no updates or changes on policy.

5. Information Security

RB updated the Committee on risk. He said risk was perceptibly rising, with attacks on the CSCS network increasing in frequency and audacity. A penetration test conducted by UIS was unable to gain access to the SDHS (the stated goal) but was able to compromise one customer server and four CSCS Raven accounts and CSCS DNS via a spear phishing campaign. Lessons learnt were being processed now, both in CSCS and UIS (e.g. passphrase should be mandatory for all password re-setters, and critical targets should possibly opt out of having their password reset by anyone except UIS). Recent attacks have locked out the accounts of some quite senior staff (including Heads of Department) and CSCS was currently exploring ways of blocking these attacks in conjunction with the CERT team at UIS. GS queried what advice should be given to the School users.

Action point (2) – RB to discuss information security with the Campus IT group with a view to agreeing advice and guidelines for School users.

A discussion then ensued on best practice for password selection and management. RB referred to the guidance from the National Cyber Security Centre, including the recommendation to use password manager software, and the Committee agreed on the need to advise users to think about their passwords.

6. Strategic planning

RB reported that a CSCS strategy for 2018-2021 was in the final draft stages and would be shared at the next committee meeting. He added that from reviewing the CSCS strategy he was reminded that the intention was to review progress against aims and objectives under this agenda item, and to facilitate this a more structured report would be prepared for the next meeting. He told the Committee that, in summary, CSCS was largely achieving its stated objectives but improvements have been slower than predicted. The cause of this continued to be issues with recruitment and retention.

LD queried when costs would be reduced for end users, and a discussion then ensued on this issue. RB advised her he was planning to consider this issue in the near future and discussions were also taking place in the UIS where a working group had been set up for this purpose. CE emphasised that changes to costing models would not take place overnight and the UIS would need to change its costing model first before CSCS could make any changes. CE told the Committee that she and the other School Secretaries would meet up with Rachel Hooper, Deputy Director UIS Departmental Operations, very shortly, to discuss this issue. CE added that RH had spent the last year reviewing existing services and changes and she intended to start making changes to the costing model for the financial year commencing 2019. RB ended the discussion by advising the Committee that progress on reducing charges for servers and storage should have been by the next Committee meeting in November/December.

7. Performance

Not discussed.

8. CSCS Finances

RB told the Committee that no financial report was due for this meeting, however he gave a brief update on the financial position. He said the finances were largely the same as previously, with one exception in that staffing cost centres (UEF and cost recovery) were building a surplus due to vacant posts; a clawback of unspent UEF would be requested to fund contractors in order to reduce the risk of staff shortages in the Infrastructure Team.

9. University IT (UIS and ISC)

AL gave a brief update on UIS matters:

New Director - Professor Ian Leslie (IL) had been appointed as the new Director of the UIS.

Video conferencing - IL was very keen to make progress on video conferencing to reduce the University's carbon footprint and has taken this on as a personal project. AL advised the Committee that he did not think there would be one solution for everyone and different solutions might be recommended for different use cases. He said he should have more to report at the next Committee meeting

Infrastructure Programme – the new storage service (one of 8 work streams under this programme) should go live in September. Once this is live they would start work on the new virtual infrastructure service with a potential service launch by the middle of next year.

Finance Systems (CUFS) – Rebecca Redman had been appointed as a programme manager to manage the projects looking at these systems and envisages a resolution by 2020.

Secure Research Computing Project – this project was ongoing. High level requirements have been collected and the HPC team has designed platform options. The Committee will consider these options very shortly.

Information Security – there were a number of matters to report. The UIS was looking to update its friendly probing service as the current commercial offering being supplied by Nessus is removing some of its current functionality which will prevent the service working in its current form and also drastically increasing costs. The team are currently trialling OpenVAS as a replacement for the Nessus back end but will also look at other commercial products if necessary. In addition, penetration testing was currently being offered across the University by Graham Rymer who has recently joined CERT. The implementation of the new intrusion prevention system was going well.

10. NHS IT matters

LD reported on a couple of NHS IT matters.

- Clinical Informatics now had a data request service for anonymised data for use in research studies. They had had 52 requests for data and had been able to supply data for all but 3 of these.
- A new tissue management system on LIMS (Laboratory Information Management System) had been introduced and was running very well. The system was quite costly but costs would come down as more people used it. CRUK–CI had recently come on board and were now using the system.

A discussion then ensued on BYOD (Bring Your Own Device). GS told the Committee that many academics were not aware that they only needed one device plus BYOD, instead of one University computer and one NHS computer, however he was keen for the former option to be the default for everyone. The functionality was just as good but it was cost-saving for the NHS and space-saving for the University.

Action Point (3) – LD to liaise with AC to measure uptake of consultants and clinical academics using BYOD and provide that list to RB.

Action Point (4) – RB to target those Clinical Academics not on the list of those using BYOD with communications.

11. Any other business

CE informed the Committee that following the student occupation of Greenwich House, the Registry was revisiting business continuity plans to review the remote access arrangements. She said that the risk to the embedded Clinical School Departments was low but there was potentially a higher risk to standalone departments and the Clinical School building itself, and she added that departments would be asked to consider this risk in their Emergency Action Plans and Business Continuity plans, in the near future.

12. Date of Next Meeting

TBC