School of Technology
IT Governance and Guidelines

Overview

The School has two IT Committees, the IT Strategy Committee (ITSC) and the IT Advisory Committee (ITAC), to advise the Council of the School and the School's departments on their use of IT and in particular in ways in which the departments can benefit from one another's expertise and ensure that their systems and data are secure. In general, reports to the Council will have a strategic element and will thus come from ITSC even when they originate with ITAC.

The School's IT Business Manager works for the School on IT strategic development and needs-analysis within the School, guided by these committees. He/she also works within the UIS championing the needs of the School, ensuring that these needs are met and that issues are resolved swiftly when they occur. As such the Business Manager is responsible for facilitating inter-departmental and department-UIS communications, ensuring on behalf of the IT committees and the Council of the School that IT strategy and policy is understood and acted on, and providing help and guidance on IT matters generally.

The IT Committees

The ITSC has an overall remit for Strategic planning in respect of IT systems and infrastructure required for teaching, research and administration in the School. Its members are primarily senior IT users from the School's departments appointed by their Head of Department. They will be aware of the needs and expectations of their department through a departmental IT Committee or similar body.

The ITAC has an overall remit to advise on best practice in the provision of IT facilities in the School's departments, including the technical appropriateness, feasibility and selection of IT systems and infrastructure proposed for teaching, research and administration throughout the School. Its members are primarily the senior IT staff member ex officio from each of the School's departments.

The formal Terms and Conditions, membership and minutes of the meetings of these committees are available on the School website at https://www.tech.cam.ac.uk/Committees/other-committees .

Cyber Security

Heads of departments are ultimately responsible for cyber security in their departments in much the same way as for health and safety. The Chair of the ITSC is the risk owner for the cyber security risks in the School Risk Register. To assist them with this, the Council of School on the advice of the IT Committees, has agreed the following guidelines. These provide a framework which will need to be supplemented by advice from experienced IT professionals including the members of ITAC.

1) The University's Cyber Security Strategy https://help.uis.cam.ac.uk/service/security/for-it-staff/cyberstrategy recommends that departments use Cyber Essentials as an appropriate technical standard for their cyber security. All departments should therefore aim to obtain Cyber Essentials certification for as much of their IT infrastructure as

is practicable and appropriate. Those departments which have already obtained this certification have found it to be useful both as a practical internal checklist ensuring good practice, as well as providing formal assurance to research funders and other partners where needed.

2) Cyber Essentials (https://www.cyberessentials.ncsc.gov.uk/requirements-for-it-infrastructure/) details requirements under five technical control themes:

- firewalls (boundary and in each computer)
- secure configuration (not simply the default as supplied)
- user access control (e.g. see 6 below)
- malware protection
- patch management (inc running current versions for which patches are available)

All departments should aim to satisfy these technical standards even where they are not currently seeking certification.

3) GDPR training is now part of the standard induction training supervised by HR, i.e. it is recognised that all new staff must do this. The basic Cyber Security awareness training should similarly be a mandatory part of staff induction training throughout the School. It is recognised that it is hard to obtain reliable data to verify participation so self-certification may be required.

4) Departments must have boundary firewalling to protect their network from attack from the wider University network and the internet as whole. The device(s) used to provide this may also be used to segment a departmental network into areas with different security requirements, and/or management domains, to limit the effect of security compromises, and to protect more vulnerable computers or those with particularly sensitive data from the rest of the network.

5) The University defines four levels of data security which relate the type of data to the storage needed to keep it adequately secure: https://help.uis.cam.ac.uk/service/security/data-sec-classes Data owners are responsible for ensuring that their data is appropriately classified and appropriate storage selected, especial care being taken for the higher levels. HR data can be hard to classify (typically being at the top end of Level 2 or into Level 3) and advice should be sought from an IT professional who is aware of the issues. An appropriate solution will ensure that: the data is encrypted in transit and when stored, the storage is guaranteed to be in a country with the same GDPR provisions as the UK, and access to the data is only be granted to the appropriate set of authenticated users. At the other end of the security scale, the UIS Moodle service is only intended for hosting widely shareable information, such as teaching materials and non-sensitive committee papers, i.e. Level 0 and some Level 1 material; it is not suitable for Level 2 or 3 data.

6) As part of their response to the University's GDPR guidelines, all departments have set up information asset registers (IARs) documenting where personal data is stored and there must be mechanisms in place to keep these up to date. As well as personal data, the School risk register includes the risk that research data containing commercially confidential and/or highly valuable data may be compromised. This implies that at least an initial minimal risk assessment should be conducted for each dataset which may contain such data and a list kept of these, probably most conveniently in the IAR, so that effort can be targeted where it is most needed. This is potentially a very large piece of work and the resource used should be proportionate to the risk for each dataset. The University's Information Security Risk Assessment (ISRA) process is a useful mechanism for performing these assessments - https://help.uis.cam.ac.uk/isra.

7) As well as the storage and other computer systems being secure, the accounts with access to them must be appropriately protected by secure passwords authenticated by a trusted server, e.g. in the UIS Blue Active Directory domain. Where higher security is needed, e.g. for Level 3 data, two factor authentication (2FA) should be used. Issues to do with secure choice of passwords and

keeping these secret are covered by training (see 2 above). The use of a password manager is strongly recommended since this makes it easier to follow good practice and have different passwords for different systems: passwords which have been used for less secure accounts, e.g. on external systems which may have been hacked or poorly secured and maintained local PCs, should not be considered secure.

8) The Council of the School expects to receive assurance via the termly minutes of the ITSC meetings that effective cyber security measures are in place in all the departments. This assurance is based on reports from each department to ITAC noting: compliance with the above points; listing any unmitigated risks detected by the UIS Friendly Probing Service (FPS); and detailing any security incidents and the action taken. The University's ISC has asked that the Schools be sent a summary FPS report and that the School IT Business/Relationship Managers have access to the detailed data. This emphasises the need for the School to be able to provide assurance on cyber security to the University but does not affect departments' responsibility for their own cyber security.

IT Requirements – Identification and Action

A key element of the School's IT strategy is that the use and adoption of centrally provided services is strongly preferred when these meet the core operational requirements. Where there is no central solution, consideration should be given to the possibility of a School level solution.

There is a standing item on the ITAC agenda for written reports from the departments on IT activity, new developments, and issues. These are passed to ITSC where members have the opportunity to add further comments. The key points from these reports provide an opportunity to identify areas for seeking UIS solutions and/or potential inter-departmental cooperation within the School and are highlighted in the committees' minutes.

The University encourages School IT Committees to contribute to the IT Strategy of the University through their representatives on the Information Services Committee (ISC) and its sub-committees, and directly with UIS via the School's IT Business Manager. Both IT Committees contribute to this through regular agenda items to identify and prioritise gaps in central IT provision affecting the departments, and by identifying areas where departmental developments may be of benefit to the wider University. These minutes are submitted to the ISC Ops Committee for wider University note.

e-Learning Collaboration

The School's Academic Vision 2019 notes under Strategic Principles "*However, it is clear that there is the potential for increasing activity in cross-School themes in research and education where, e.g. strategic research themes might be identified and encouraged ... to add value to existing research and to bring in further research income. It will also make the School more attractive to industrial funding by offering larger, strategic themes in areas of critical importance (e.g. decarbonisation). … the potential for the application of digital learning is huge.*". IT clearly has a key role to play in this and under Education and Training, the Vision goes on to note "*Digital learning is growing in importance in higher education and particularly so for part-time and professional courses. … It is expected that the newly-appointed Director of Education will be leading this initiative with the Chairman of the School's IT Strategy Committee.*".

The IT Committees have collaboration and sharing of IT expertise and tools in their Terms of Reference and the above emphasises the current importance of this. Work has been done recently by ITSC to produce an overview of digital learning applications in the School with the aim of seeing how these currently separate initiatives might benefit from one another. In collaboration with other School committees, ITSC will identify strategic application areas. ITAC will identify suitable common technologies in light of work recently done by UIS to identify a set of core programming languages and development environments to be used for any future projects.

IT Procurement

ITAC has a remit to advise on the provision of IT resources at School level, e.g. shared licences, jointly developed software, and shared facilities. In practice this has only applied to shared licences but the committee is expected to be aware of opportunities for obtaining discounts and terms and conditions through joint purchasing and larger quantities. Consideration should always be given to both open source and commercial solutions when procuring IT resources, taking into account the total cost of ownership and the relative advantages of the two support models.

24 Oct 2019