UNIVERSITY OF ST ANDREWS
IT SERVICES
USE OF CLOUD COMPUTING SERVICES WITH UNIVERSITY INFORMATION AND DATA

PURPOSE

1. The purpose of this document is to provide direction and in some instances specific instructions on the use of information and data for which the University is responsible ("the information"), with 'Cloud' computing services. Cloud computing can be defined as "Using a network of remote servers to store, manage and process online data".

AIM

2. The University aims to provide environments where collaboration can take place on and off campus, without threatening the privacy of individuals or the interests of the institution and its stakeholders. If information or data that the university is responsible for is held out with devices that the University has ownership and/or control over, there is a risk that its confidentiality, availability or integrity may be compromised. The impact of this can be significant – individuals can be harmed as a result of their privacy being violated; the University can lose the trust of others; suffer reputational damage and be exposed to significant monetary penalties from regulators.
3. To achieve the aim of providing access to collaborative environments which do not threaten the privacy of others or the University's interests, the University's approach to deploying and using cloud computing services will be consistent with meeting the relevant legislative requirements from the Data Protection Act 1998 ("the DPA") and relevant University Policy and Regulation, notably the Student and Staff Codes on the use of personal and sensitive data and the University Information Classification Policy and supporting implementation guide (2015).

OBJECTIVES

4. The objectives of this guidance are to:
   a. Clarify what cloud computing services can and cannot be used;
   b. Detail what class of information can and cannot be placed into cloud computing services;
   c. Highlight the specific privacy and information security risks that can exist when cloud computing services are synchronised with devices that are not owned and/or controlled by the University; and
   d. Inform staff where to get advice on the use of alternative technologies or services where it is not appropriate to place information into a cloud computing service.

WHAT CLOUD COMPUTING SERVICES CAN BE USED?

5. Information that falls within the classes of **CONFIDENTIAL** or **STRICTLY CONFIDENTIAL** (please see the University Information Classification Policy) should only be used with a third-party Cloud service with which the University has an authorised contractual agreement. IT Services will maintain and publish a list of authorised Cloud computing services.
6. Currently (April 2015) the University has one such agreement. This is with JISC Connections and the JANET Ltd Framework[1] for Microsoft Office 365.

[1] https://www.ja.net/products-services/janet-cloud-services/microsoft-office-365

7. The agreement which the University has entered into for these services is consistent with best practice guidance issued by the statutory authority with responsibility for overseeing the enforcement of the DPA – the UK Information Commissioner[2]
8. If there is a requirement to make use of another Cloud computing service, then please e-mail contact the IT Service Desk with your request. Where existing Cloud bases services provided by or through the University do not meet business requirements then an assessment will be made to ascertain if a suitable contractual agreement can be created to provide access to an alternative service.

WHAT INFORMATION CAN AND CANNOT BE USED WITH A CLOUD COMPUTING SERVICE?

9. The implementation guide that supports the University Information Classification Policy (2015)[3] describes 4 classes of information: PUBLIC, INTERNAL, CONFIDENTIAL and STRICTLY CONFIDENTIAL.
10. Information that falls within the class STRICTLY CONFIDENTIAL cannot under any circumstances be used with a cloud computing service.
11. Information that falls within the class STRICTLY CONFIDENTIAL includes:

STRICTLY CONFIDENTIAL	EXAMPLES
Information that if subject to unauthorized disclosure, dissemination or loss could result in: a) Significant, unwarranted breach of a person's privacy, which more likely than not would cause substantial harm. This will certainly include information that the DPA defines as sensitive personal data. Sensitive personal data is information that concerns an individual's: • Racial or ethnic origins; • Political opinions; • Religious beliefs or beliefs of a similar nature; • Trade union membership; • Physical or mental health condition; • Sex life; • Involvement in any proceedings for any offence committed or alleged to have been committed by them, the disposal of such proceedings or the sentence of any court in such proceedings; and • Outcomes of criminal convictions. b) Substantial risk to the health, safety and wellbeing of individuals or groups. c) By prejudicial to the prevention or detection of a crime or to the apprehension and prosecution of an offender. d) The University being exposed to a civil claim for breach of confidence. e) Information protected by legal professional privilege, including legal advice privilege and litigation privilege. f) Significant financial loss (>£100,000) to the University through: • The revocation of a contract(s) for research or services; • Where information could be subsequently denied to the University, where the effect of that loss is critical business processes cannot run, or these are significantly impeded; and • Fine(s) set by a regulator.	• Accident reports • All medical information e.g. occupational health records/reports, fitness to work notes • Bank/credit card details (i.e. numbers, expiry dates, etc.) • Case files and correspondence surrounding investigations by a Regulatory body e.g. SPSO • Communications with Government (Ministerial level) • Communications with legal (counsel) • Communications with Police Scotland (operational matters) • Counselling records • Disciplinary proceedings • Grievance proceedings • Legal proceedings • Passwords and other forms of access control credentials

[2] https://ico.org.uk/media/for-organisations/documents/1540/cloud_computing_guidance_for_organisations.pdf
[3] INSERT URL [INFORMATION CLASSIFICATION POLICY IMPLEMENTATION GUIDE]

RESTRICTIONS SURROUNDING CONFIDENTIAL INFORMATION

12. Information classed as CONFIDENTIAL can be placed into a cloud computing service **where that service is not synchronised with a device that is not owned and/or controlled by the University**. For more information see SYNCHRONISATION, below.
13. Information that falls within the class CONFIDENTIAL includes:

CONFIDENTIAL	EXAMPLES
Information that if subject to unauthorized disclosure, dissemination or loss could result in: a) An unwarranted breach of a person's privacy, which more likely than not would cause a level of harm and/or inconvenience. This will certainly include information that the DPA defines as personal data. Personal data is information that identifies a living individual and relates to them in a significant biographical sense. This can also include opinions formed by the University on an individual and the University's intentions towards an individual. b) Disruption to day-to-day operations of the University, where disruption only affects a sub-set of the University community. c) Damage to commercial relationships. d) Loss of competitive advantage.	• Commercial contracts • Contracts of employment • Disaster recovery / business continuity plans • Documentation that contains decisions surrounding academic progression • Examination results • Payroll / banking details • Planning / forecasting reports • Procurement / invitation to tender documentation • Research grant applications • Strategic planning • Student transcripts • University Risk Register and controls

ALTERNATIVES

14. If it is necessary to place information into a Cloud computing service and have this synchronised with a non-University device, then in some instances a viable option may be to remove and/or take steps to render anonymous the confidential and/or highly confidential elements of information in a document/file etc. When it becomes necessary to finalise a document/file, it can be removed from the Cloud service and amended to include the sensitive information elements.
15. Files can be accessed remotely where these are held on the University network and accessed via the VPN service. While this provides secure access to information, the nature of the VPN service limits opportunities for others to collaborate on a document/file.

FURTHER GUIDANCE

16. The restrictions on the use of information classes as STRICTLY CONFIDENTIAL and CONFIDENTIAL when using Cloud computing services are designed to protect both the privacy of individuals and the interests of the University from harm.
17. If you have any questions about what information can or cannot be placed into a cloud computing service please e-mail dataprot@st-andrews.ac.uk
18. If you find that these restrictions make it difficult for you to undertake your work, please in the first instance contact the IT Service Desk.

CHANGES TO THE GUIDANCE

19. This guidance is based on best practice and an understanding of the privacy and information security risks to date. Guidance on what information can be placed into Cloud computing services may change in response to changes in best practice recommendations and any emerging threats to privacy and information security. IT Services will advise when this guidance changes.

SYNCHRONISATION

20. Cloud computing services can be synchronised to work with a range of devices that a person uses. This has a number of advantages; files can follow you on whatever device you are using, as long as the devices are synchronised with the Cloud service, collaboration and document sharing also becomes easier.

21. Difficulties arise when a synchronised device is not owned or controlled by the University and confidential information is then made available through that device. For example, information held on a family PC could then become available to a range of people. This presents a range of risks, as the University cannot guarantee that privacy and confidentiality can be maintained where information is held on devices out with its ownership and/or control.
22. To address the risk of confidential information becoming known to persons who do not have any right to see that information it is necessary to place some level of restriction as to when information cannot be placed into a Cloud computing service, where that service is synchronised with a privately owned device or other devices out with the University's ownership or control.