Information Strategy

Third-party and cloud-based information services' usage policy

The purpose of this document is to lay forth the policy which regulates the use of information services delivered (in whole or in part) for or on behalf of the University by a third party: this includes that subset of third-party service popularly encapsulated by the word 'cloud'. It should be clear that policy is not immutable: in particular, in a field such as this, where emerging technology is interwoven with emerging law, we must be able to react to changes. In the formulation and continuous reformulation of policy, we must be guided by advice from within the University and beyond, taking due consideration of legal precedent, and having due regard to the practices and experiences of our colleagues in other institutions.

July 2015

Document properties

Authority

Director, Computer Centre

Sponsor

Director, Computer Centre

Responsible officer

Assistant Director (Governance and Corporate Services), Computer Centre

Recent version history

Current version, July 2015, supersedes the verion of June 2014.

1 Introduction

First and foremost, let us be certain: cloud-based service is simply a form of third-party service, so the requirements should be identical. Equally, third-party service is just service, so there should be no lessening of any protective environment compared with Brunel-based service. No matter where our data, our processing or our service might be located — and that should really be 'located', since precise location is muddied by replication, mirroring, backup, resilience, staging, routing and all the other shape-shifting technologies which are brought to bear — our service is to our user community and to our data subjects, and they deserve the highest levels of care and respect.

Secondly, since there will be cost/risk assessments, we must always ensure that full economic costing models are used in any such decision, especially where allegedly 'free' options inveigle themselves into the reckoning, for such options always have on-costs and on-risks.

2 Information security

Third-party and cloud implications for information security are discussed within the University's Information Security Policy: the primary chapters are *D — Outsourcing and third parties* and *Z3 — Cloud use*, but the entire Policy is relevant, and any third-party/cloud usage must be aligned to the Policy *in toto*.

With the use of third parties, a defining characteristic is the ceding by the University of certain aspects of control of the data (including any derived data), their storage, their accessibility, and their deployment. Each of these will require to be validated, through the application of due diligence and the confirmation by appropriate testing, against laws and ethical norms in respect of the security and privacy of the data, and against any regulatory framework which applies to data of their type.

3 Due diligence

The application of due diligence will encompass all aspects of data use: the following sub-headings address the major areas across all data, but it remains the responsibility of the senior officer of any unit of the University exploring the use of third-party/cloud services to undertake all due diligence, whether described below or not.

A key counterpoint in due diligence is risk assessment (see also below): due to the abandonment of at least some measure of control when moving data or a service to a third party or to the cloud, the senior officer of any unit of the University exploring the use of third-party/cloud services will need to provide such assessments to the University's Risk Manager.

3.1 Financial diligence

It is clearly vital that strict standards of financial rectitude must prevail. The financial health of any company with whom we may work must be investigated, and cloud companies require particular scrutiny. This is because of the insubstantial and non-material nature of the service, where even the 'plant' may be as nebulous as the name 'cloud' suggests. Often such a service is arranged by a broker who will sub-contract and re-contract, changing suppliers (who may themselves be mere brokers) with startling frequency. If any of these links should dissolve into financial failure, the integrity of the University's data is put at risk.

Allied to due diligence on the supply chain, we must ensure control of University money. Incremental cloud services are often hidden from full financial scrutiny within Brunel through payment in small quantities by corporate credit card. This extreme fragmentation of service is inimical to adequate management of University services and finances, and risks the contumely of auditors who may suspect attempts at concealment which may indicate an opening for fraud. The simplistic procurement authorities based on cost limitation (warranty up to £*x*) do not prevent the acquisition of cloud service 'under the radar' without controls. By the act of requiring a valuation on the service (typically, the cost of replicating the service in short order with a home-based service) and applying that valuation to procurement limits as if it were the 'cost', a more adequate measure of control will be obtained. This is not a simple control exercise: we must have the knowledge of the cost in re-homing the service to Brunel domicile in the case of corporate collapse or wrongdoing on the part of our supplier.

A cloud contract is no less a contract than any other: the contract terms must be reviewed and signed off by appropriately experienced staff. This holds good even if no money passes between the University and the supplier: indeed, there may well be need for more searching review of terms and conditions, due to well-founded scepticism of the existence of a free lunch. There should be no authority for anyone to conclude a cloud contract if such authority for a more physical service contract would not be vested in that person.

It is the duty of the senior officer of any unit of the University exploring the use of third-party/cloud services to undertake full financial diligence, including the preparation of a cost profile for in-house operation of the data storage and/or service.

3.2 Due diligence regarding territoriality and domicile

It is important to understand where our data are being held, and under which jurisdiction. Concern applies most particularly to personal data (within the meaning as ascribed by data protection legislation, a meaning which applies throughout this document) as regards protection against unwarranted disclosure, but the question of jurisdiction will apply to a cloud service irrespective of the class of data held and managed thereby.

As noted above, the problems of unknown supply chains and rapid re-location of data makes it more important still that any contract will specify domicile, territoriality and jurisdiction the full length of the

(branchable) supply chain: if such information is not forthcoming in an unambiguous and assurable way, due diligence is impossible and we should walk away from the potential supplier.

Questions of territoriality arise in the application of EU law (which applies to suppliers and to Brunel alike, due to our location within the boundaries of the Union), but also in laws on extra-territoriality as enacted or interpreted by other jurisdictions. A noted 2014 re-interpretation of US law[1] extends the territoriality of US law to data held at any worldwide location (and presumably at locations in orbit too) by any US company. This court order means that we can no longer rely upon European Economic Area domicile for inviolability of personal data, and must therefore mean that the presence of a US company in the potential cloud supply chain would place a cloud service supplier beyond the realm of safe service providers, at least for any personal data. Likewise, the inability of a potential cloud service supplier to be able to give demonstrable assurance that no US company would be involved in a cloud supply chain would effectively debar that supplier from providing service in respect of personal (or potentially personal) data holdings of the University.

It is the duty of the senior officer of any unit of the University exploring the use of third-party/cloud services to maintain awareness of the domicile (actual or potential) of Brunel data and/or services throughout the supply chain, paying adequate attention to statute and case laws in any relevant jurisdiction, and to be prepared (operationally and financially) to re-home the data/service back to Brunel at any time.

3.3 Due diligence regarding the security of data and services

The security of data encompasses the measures taken by a cloud supplier against the possibility of loss, theft or damage to University data held within the supply chain orchestrated by that supplier.

We need to know that no item of our data can be obliterated, but we need to be assured that any data which we delete will be properly erased from all copies held within the supply chain, according to agreed procedures for backup and resilience. Furthermore, at any change in subcontracting within the cloud supply chain, we must be assured (and must check that assurance) that all copies of our data are obliterated from storage managed by the departing subcontractor after the check on complete transfer to the new subcontractor is signed off.

We need to be assured that our data are completely inaccessible to anyone but the University, save for unavoidable access in bulk by the supply chain. we need to be assured of the adequacy of controls in the supply chain's use of the data, including (but not limited to) employee access to extract data or to copy and transfer the data without authority from the University.

---

1 discussed at http://www.arthurcox.com/wp-content/uploads/2014/05/Expert-comment.pdf and elsewhere

We need to be assured that nobody other than a duly authorised member or agent of the University is able to edit University data.

All this must involve, at the very least, availability of touch-logs so that the University may audit any transactions involving University data.

It is the duty of the senior officer of any unit of the University exploring the use of third-party/cloud services to maintain awareness of the levels of security which would be afforded to Brunel data and/or services throughout the supply chain, and to be assured of the adequacy of the suppliers' touch-logs for audit purposes.

3.4 Due diligence with respect to reliability and availability

Users of a University data service have no interest in whether it is domiciled within Brunel or in the cloud[2] — their interest lies in being able to gain access to the data on demand, except during predictable, relatively infrequent, and well-advertised times of scheduled maintenance.

Unscheduled outages (and as high a proportion as possible of scheduled maintenance periods) should cover availability through reliable switching to resilient and synchronised copies.

Corruption of data should be backtrackable both for audit/forensic purposes through event logs and for service availability through backups. Naturally, this means that multiple copies of our data will exist within the supply chain, and these will be the subject of due diligence on security matters as discussed above.

It is the duty of the senior officer of any unit of the University exploring the use of third-party/cloud services to maintain awareness of the levels of availability, resilience and reliability (actual or potential) of Brunel data and/or services throughout the supply chain, including the provision of information back to Brunel in the event of scheduled or unscheduled downtime or degradation of service.

3.5 Due diligence in legal and regulatory compliance

The University has general obligations under the law (which apply to any processor or controller of data), and there are further obligations which apply to Brunel because of its status as an educational establishment, as a Public Authority, and because we fall into other such categories. There are aspects of line-of-business regulatory compliance — from financial transactions to estate regulations, as well as those imposed on areas of research and education by professional standards bodies and

2 save, of course, that intelligent users may seek personal assurance of legal compliance, ethical treatment, etc., with respect to their data — and the University must be able to furnish such assurance to an enquiring user at any time

government licensing. All of these obligations should have been built into any Brunel-domiciled data storage, use and management.

There are also duties placed upon the University regarding activity beyond specific ICTS facilities, but which use such facilities for communication, storage, etc.; the University is still bound if the facility is placed in the cloud, and it must be confirmed that a cloud service provider is able to meet the University's compliance requirements. This would include (but is not limited to) all aspects of activity upon which the Counter-terrorism and Security Act 2015 impinges, with particular reference to monitoring, alerting, and evidence capture.

All of these obligations must be met if we contract to a cloud supplier, and the audit and assurance obligation is doubled. We must still comply at the Brunel end of the link, but we must assure ourselves of full compliance by our cloud suppliers, and by their subcontractors alike. We must ensure that the supply chain is capable of understanding any specific regulations which appertain to our data[3], and of taking adequate measures to ensure compliance: if we do not, those members of the University who commission the third party to act on the University's behalf will be in breach of compliance, and therefore in breach of University regulations. Such contempt is wholly unacceptable and may lead to disciplinary sanctions against offending users and/or their chains of management within the University.

It is the duty of the senior officer of any unit of the University exploring the use of third-party/cloud services to remain assured of the highest standards of legal and regulatory compliance relating to Brunel data at all points of the supply chain, including the immediate and full disclosure to Brunel's Governance, Information and Legal Office of any known, suspected or potential data breach or other such compromising of the integrity of Brunel data.

3.6 Due diligence to ensure maintenance of ethical standards

The line between compliance and ethics is not always sharply defined, but there must always be an overlap rather than a gap. In some areas (such as research ethics), there will be regulatory compliance built in to safeguard ethical treatment, or at the very least to allow ethical choices to be easier to make than those which will attract opprobrium. But at the nub of ethical standards is the great majority of data use and management. There are many occasions when there is a technical capability to undertake a particular action (such as to inspect data about a particular person) where neither business nor morality provides the grounds to do so. We must be able to assure ourselves that data and services managed through a cloud supplier are not misused in such a way — there should be no need for anyone in the

3 In situations of closely-drawn regulations, or of subject matter which is specific to education and research, it will often be the case that generic service suppliers have neither the knowledge of relevant regulation, nor the commercial will to be interested: in such cases it is likely to be advantageous to ignore cloud as an option, or at the most lax, to confine cloud options to such suppliers as JISC or the Government.

supply chain to be aware, let alone interested, in the data content, save to know the appropriate levels of access and management controls.

It is the duty of the senior officer of any unit of the University exploring the use of third-party/cloud services to remain assured of the highest standards of ethical treatment relating to Brunel data at all points of the supply chain, including the immediate and full disclosure to Brunel's Governance, Information and Legal Office of any known, suspected or potential shortcoming which might compromise the moral integrity of Brunel data and its management.

3.7 General acts of diligence

The proper exercise of due diligence is never an episodic tour of a collection of rubber stamps: it needs to be as autonomic as breathing. There are many areas where diligence is required in dealing with third-party and cloud contracting which cannot be tied down tritely into buck-passable box-ticking, and such a mentality is simply incompatible with our duty to the data and its subjects (whether or not these subjects are associated with the University). From listening out for corporate takeovers to monitoring the going rate for wholesale server/storage provision to checking back with a contracted supplier for reassurance that someone else's data breach was not committed by anyone in the supply chain for our cloud-based services, and on to other and new concerns which will pop up without warning, we must all be resolute in maintaining knowledge and assuring adequacy regarding all aspects of cloud service. Following logically from questions such as the above, we must always ensure that we have a Plan B for an orderly transfer to another provider in the event that our diligence might expose inadequate service.

It is the duty of the senior officer of any unit of the University exploring the use of third-party/cloud services to be constant in carrying out general matters of diligence relating to any proposed or existing contract or agreement with a third party or cloud supplier in relation to the integrity of Brunel data.

4 Reputation

Whether through ignorance or arrogance, it is all too easy to damage the reputation of the University while transacting business via a cloud service. It is, of course, just as easy to do so if the service is home-hosted, but the ceding of University control by using a cloud service makes the damage limitation and reputation retrieval substantially more difficult. Many people seem to have a blind spot when it comes to reputation and cloud: it is vital that we redouble our vigilance against any potential slippage in this regard.

4.1 Delivery

With a cloud service, we must cede the act of delivery to the third party who is providing the service. If that delivery is poor, our reputation suffers. Assurance of an adequate user experience is part of due diligence, particularly with respect to the section on reliability above. It is the duty of the senior officer

of any unit of the University exploring the use of third-party/cloud services to ensure that the service level of delivery does not compromise the University's reputation.

4.2 Presentation

Control of delivery is necessarily ceded to the provider to a greater or lesser extent, but we should be very alive to the pitfalls of ceding presentational control. For example, a survey undertaken via SurveyMonkey will have advertisements added by the service provider — that is the business model which brings revenue. Since we have no control over the advertisement placement (and may not even be aware of where the placements are, since they may be suppressed while acting as the 'controller'), we may end up with advertisements associated with Brunel business which run at variance with our activities, our values and our reputation. It might, for example, attach advertisements for, say, the University of Reading to a questionnaire about the effectiveness of Brunel Applicant Days — not helpful to our business of attracting students. Likewise, advertisements for local businesses (for example, a lap-dancing club) may run counter to our values, and political/solicitation advertisements will ruin our reputation for impartiality in analysis of research. It is the duty of the senior officer of any unit of the University exploring the use of third-party/cloud services to ensure that the service presentation cannot compromise the University's reputation through association with content bundled by the service provider without the consent of the Director of External Affairs of the University.

4.3 Branding

Branding gives us the capability for positive reinforcement of cloud services' adherence to Brunel's name and values: insistence on adequate and appropriate branding is the counterpoint to vigilance against inappropriate presentation.

Any cloud-based service acting as a Brunel service (*e.g.*, a blog, survey or catalogue) must contain clear branding as a Brunel entity, and must offer a direct link back to a Brunel web-page which confirms the authenticity of the service as of Brunel origin (preferably with confirmatory screenshots, placed on the local page, of all likely entry-points to the hosted service), otherwise the risk of 'passing off' cannot be considered adequately covered. The use of logos, etc., must be regulated by the University's Director of External Affairs (or a duly appointed agent), and third-party restrictions on their re-use must be written into terms and conditions for the service. Simply signing up to a third-party agency to undertake Brunel business 'under its own flag' is, equally simply, not good enough for our users to be assured of the University's status with respect to the service.

It is the duty of the senior officer of any unit of the University exploring the use of third-party/cloud services to ensure that Brunel business transacted under the service agreement is adequately and unambiguously branded as a Brunel service, with adequate confirmatory links to the Brunel website as described above.

4.4 Data use

If Brunel data are gleaned from a cloud-based service and our data subjects are ad-bombed by a third party (which could be Marks and Spencer, a political party or that local lap-dancing club), the trust in our ability to handle information effectively is reduced. Indeed, if the cloud service provider re-uses our data in such a way, we (that is to say, the senior officer of the unit of the University which commissioned the service) are likely to have breached data privacy legislation. But the damage is done, and our reputation is in shreds.

It is essential that the terms and conditions of any contract for cloud-based services give the University control over data re-use (and have punitive compensation for any data leakage by the provider or other users). If a service provider cannot or will not give a guarantee regarding the control of re-use of data (including derived data and site-visit data such as cookie content), then that provider cannot be considered to be a worthy or appropriate business associate of the University. It is the duty of the senior officer of any unit of the University exploring the use of third-party/cloud services to be assured of the adequacy of controls on data re-use, and to cease association with a provider if appropriate guarantees are not given, or are subsequently broken. It is furthermore the duty of the senior officer of any unit of the University exploring the use of third-party/cloud services to ensure that there is adequate recourse to an alternative service in the event that an association with a provider must be terminated for the above reasons.

5 Risk management

5.1 Risk assessment

As noted above, risk assessment must be made, and must be taken seriously, on a case-by-case basis, and indeed must be reviewed regularly on a case-by-case basis when dealing with proposed or existing third-party/cloud suppliers. However, as in other areas of University operation, the management of risk must incorporate the management and assurance of the risk assessment process, in part through the installation of adequate controls.

5.1.1 Insurance, intellectual property and compliance

The use of a cloud service brings the potential for essentially limitless cost — for example, in prosecuting or defending legal action, or in changing (or challenging changes to) terms and conditions. We must ensure *before* entering into a cloud service agreement that we have secured appropriate insurance against these costs, or that the University has agreed at the highest level to carry the risk. It is the duty of the senior officer of any unit of the University exploring the use of third-party/cloud services to ensure that any contract is underwritten by adequate University insurance or an explicit waiver therefrom, authorised by the Director of Finance (or by a duly appointed agent thereof).

One of the main areas of risk in ceding control to a third party is the potential for the dilution or loss of intellectual property rights and benefits, whether these rights accrue to the University (and may be vulnerable to unauthorised use by the service provider or others), or to a third party (in which case, the University should be indemnified against unknowingly breaching others' conditions of use). It is the duty of the senior officer of any unit of the University exploring the use of third-party/cloud services to ensure that all intellectual property rights are maintained and respected in any contract, and subsequently that each user of such third-party/cloud services so contracted will maintain and respect all intellectual property rights, whether or not these are explicitly claimed.

It is vital that any user of a Brunel cloud-based service (whether or not a member of the University) is not drawn towards the breaking of any law or instrument of regulatory compliance, and sufficient guidance must be placed (with maximum ease of access) in the means of use which offer greatest respect for compliance. It is the duty of the senior officer of any unit of the University exploring the use of third-party/cloud services to ensure that adequate guidance is made easily accessible to any user of the service, in order that full compliance with all relevant laws and regulatory instruments is assurable.

5.1.2 Privacy

A Privacy Impact Assessment (PIA) is an essential part of any due diligence prior to entering into a cloud service agreement if there is any hint that personal data may feature in the service, and again whenever there is any change to the type of data transacted under such an agreement. For example, one might consider the implications of loss of privacy through the tagging of a photograph placed on a social networking service with the subject's name (by a University member or a third party).

A comparison of privacy impact should always be made between a proposed cloud service and the nearest equivalent home-based service, or a service available for home hosting.

It is the duty of the senior officer of any unit of the University exploring the use of third-party/cloud services to ensure that a full PIA is undertaken, and that the University's Governance, Information and Legal Office signs off that Assessment, before any contract is concluded, and subsequently that a new PIA is undertaken (and duly signed off) on any change to the type of data being transacted under the said contract.

5.1.3 Security and reliability

In undertaking due diligence, security and reliability must be assessed. In many respects, security of data and service must be a *sine qua non*, though the levels of control may involve a risk/cost balancing exercise. In terms of reliability, there is a more flexible 'sliding scale' for the analysis of risk, but such analysis must be carried out and revisited periodically.

In all matters relating to the acceptance of risk, authority must be gained from the University's Risk Manager before the conclusion of any contract; likewise, any change in risk must be referred to the Risk Manager who will advise on any necessity to change suppliers if the current supplier's service poses unacceptable risk. It is the duty of the senior officer of any unit of the University exploring the

use of third-party/cloud services to assess all risks and to agree levels of risk acceptance with the Risk Manager according to this Policy. It is furthermore the duty of the senior officer of any unit of the University exploring the use of third-party/cloud services to review risks periodically, and to agree any continuing risk acceptance with the Risk Manager following such review.

5.2 Managing risk in cloud decisions

As noted above, risk assessment must be made, and must be taken seriously, on a case-by-case basis. However, as in other areas of University operation, the management of risk must incorporate the management and assurance of the risk assessment process, in part through the installation of adequate controls.

5.2.1 Contract

A cloud contract is no less a contract than any other: the contract terms must be reviewed and signed off by appropriately experienced staff. This holds good even if no money passes between the University and the supplier: indeed, there may well be need for more searching review of terms and conditions, due to well-founded scepticism of the existence of a free lunch. There should be no authority for anyone to conclude a cloud contract if such authority for a more physical service contract would not be vested in that person. Contract terms and conditions should be agreed within the University (with, as relevant, the Director of the Computer Centre, the Director of Finance, the Director of External Affairs, the University's Governance, Information and Legal Office and other officers of the University) prior to the conclusion of a contract. It is the duty of the senior officer of any unit of the University exploring the use of third-party/cloud services to ensure that adequate contract analysis and checking is undertaken, involving all relevant units of the University, and that adherence to the terms and conditions of the contract is maintained by all who come into contact with the service.

5.2.2 Audit

Managing risk in an ongoing contract involves an audit procedure. Such a procedure must be agreed with the service provider in the drawing up of a contract; unsatisfactory audit results will lead to a review (or, at worst, a suspension), and the contract must incorporate agreed procedures in such an outcome. It is important that audit procedures are set up as part of the contract with any cloud-based service provider; this will include the guarantee that suitable transactional audit logs are maintained by the service provider and are readily and immediately accessible to the University and/or its duly nominated agents for inspection and analysis. It is the duty of the senior officer of any unit of the University exploring the use of third-party/cloud services to ensure that such audit framework is built into any contract for the provision of such services.

5.2.3 Review

Any cloud-based service must be subject to periodic review[4], and any contract must build this into the association between the University and the provider. Review documentation will become part of the service information, which will become available to inform any need to change parameters of the service, or indeed to change providers. It is the duty of the senior officer of any unit of the University exploring the use of third-party/cloud services to ensure that such review takes place, and that the documentation pertaining to review is made available to any interested party acting on behalf of the University (whether internally or externally based).

5.2.4 Evolution

The landscape of our business changes rapidly, and the characteristics and viability of cloud services and of particular practices therewith are no exception. Any contract to provide cloud services must retain sufficient flexibility to allow for an easy shift to a more appropriate paradigm as developments roll out. Such evolution will not necessarily follow the review cycle; indeed, it is more likely that it will be disruptive to that cycle. It is the duty of the senior officer of any unit of the University exploring the use of third-party/cloud services to ensure that any contract to provide such services retains the capability to make a paradigm shift when there is major change to any factor (whether such change is generated from within the University or through technological development) feeding into the service.

4 An annual review is a useful default, but the nature of the service may demand more frequent review or, in a few cases, an extension to biennial review.

