Using Your Own Applications and Devices Policy

Originator name:	James Newby
Section / Dept:	Business Support, on behalf of Information Security Steering Group.
Implementation date:	26 October 2015
Date of next review:	
Related policies:	Information Security Policy Acceptable Use Policy Data Protection Policy Social Media Policy Research Data Management Policy
Policy history:	

Version History

Version	Author	Revisions Made	Date
1	James Newby	First Draft – incomplete for ISSG discussion	20 January 2015
2	James Newby	Changes made following input from ISSG meeting	9 March 2015
3	James Newby	Changes made during final revisions by sub-group	17 March 2015
4	JN/GW	To incorporate extension of provisions to cover personally acquired applications. Input from GW, AK and JN	August 2015
5	GW	To explicitly reference removable media	26 October 2015

Approval History

Equality Analysis

Version	Reviewed by	Comments	Date
1	Jo McCarthy-Holland	Low equality impact	10 March 2015

Committee Sign Off

Version	Committee Name	Date of Sign Off
1	Information Security Steering Group	18 March 2015

1	**Introduction**
	The University generates and stores large volumes of data as a result of its activities. Whilst IT Services are constantly reviewing and developing the technical and systems enhancements needed to improve data security, all staff must be aware of their responsibility to handle confidential and sensitive data securely. Such data generally remains secure while stored within University-provided services and applications. However, security can be compromised by exposing data to personally-acquired applications (apps) or Cloud services (paid-for or free-to-use). The ubiquity and variety of staff owned devices, purchased for personal use but able to access, store and transmit University owned data makes it impossible for IT Services to implement fully effective technical solutions to ensure they are always used appropriately. This policy outlines the requirement which staff and students must follow when using their own computing and storage devices or personally-acquired (own) applications to handle University owned data.
1.1	**Purpose**
1.1.1	The University understands and acknowledges that most staff use their own devices and applications to access, store and transmit University data for legitimate work purposes which enhances their effectiveness and benefits the institution. This policy does not therefore seek to inhibit the use of these apps or devices, but the fact that the University cannot ensure that its data security can be maintained means that staff must take a high level of personal responsibility for their configuration and use. The University must ensure that adequate organisational and technical measures are in place to prevent a breach of data security as a statutory obligation under the Data Protection Act but also to protect its valuable intellectual property and commercially sensitive information. This policy's core purpose is to balance the data security risks with the operational benefits arising from the widespread use of Cloud-based consumer applications and staff owned devices.
1.2	**Scope**
1.2.1	The policy covers all University staff and students with access to University IT networks, databases and systems. Whilst its requirements will be relevant to the use of any personally-procured app or device, it is assumed that University owned and provided equipment and services will always be configured to a standard consistent with the latest University information security requirements. University issued devices and applications must be used by staff in accordance with the Acceptable Use and other relevant policies (see list of related policies). Devices and applications acquired by staff personally and only used for personal purposes (i.e. not used to access, store or transmit University data) fall outside the scope of this policy. Digital equipment, devices and apps come into scope when used to handle University data as a risk then arises of loss, disclosure or inappropriate use of University data. Staff using their own devices or apps for work purposes, should make themselves aware of this policy's requirements.
1.3	**Equality Analysis**
1.3.1	The policy has been assessed to exert a low equality impact so a full equality assessment is not required and has not been undertaken.
1.4	**Definitions**
1.4.1	**Device** – fixed or mobile computing equipment (e.g. server, desktop PC, laptop, tablet, smartphone) or any equipment capable of digital data storage (e.g. USB key/memory stick, disk drive, media player, CD/DVD, digital tape). **Application (app)** – software used to perform a particular function that may be paid for, free-to-use, open-source or personally written. It may run locally and/or from a remote

	location and accessed as a web-service (Cloud/SaaS). The app may be available on one or more personal and/or corporate owned devices. **Information security**: the preservation of the confidentiality, integrity and availability of information. **Information**: data which has meaning. **Information asset**: all data with meaning that can be exploited to advance the University's objectives or confer competitive advantage. **Sensitive data**: data which includes elements requiring some form of restriction of its availability. This normally includes personal information or data with commercial value to the University. **System owner**: Head of Unit (Department or Faculty) or their nominee with prime responsibility for managing and maintaining an information system, database or network; this includes the day to day operation **Handling data** – the accessing, storing or transmission of data. This includes accessing the web via University networks.
1.5	**Legislative context**
1.5.1	The University must meet its obligations under the Data Protection Act which governs the security, processing and retention of personal data. The University is also subject to the Freedom of Information Act which governs the access to its information it should make available to the public.
1.6	**Health & Safety Implications**
1.6.1	No health and safety implications arise from the implementation of this policy.
2	**Policy**
2.1	**Principles**
2.1.1	All staff using their own apps or devices to access, store and transmit University data are expected to be aware of basic information security good practice. It is a requirement that they have viewed the Information Security training video available at [insert link] and completed the Data Protection and Information Security online training module available at [insert link].
2.1.2	**Do not use personal apps or devices for storing, accessing or transmitting personally identifiable or commercially sensitive information** The University has determined that the benefits of allowing staff to use their own apps and devices under appropriately controlled conditions justify the information security risks involved. However, these benefits arise from the convenience and productivity enhancements of being able to access personal calendars, emails, contacts and documents containing less sensitive data and should not extend to handling highly sensitive or commercially confidential data. Staff should therefore comply with the principle that the use of their own apps and devices is appropriate for activities that help them "keep in touch with the office" but not for the handling of sensitive information. The boundary between the two categories cannot be specified but staff must seek the advice of their manager or IT Services if they are unsure.
2.1.3	**Device functionality and information security threats are constantly changing so the rules will be updated frequently** As technical requirements and solutions will change over time and new information security risks will emerge constantly, the requirements and criteria for the issuing and use of apps and devices will change frequently. The guidelines are therefore included in appendix 1 of this policy and are subject to change from time to time.
2.2	**Procedures**

2.2.1	When using their own apps or devices to access, store, manipulate or transmit University data, all staff must comply with the following basic measures: • Configure smartphone and tablet devices to highest available password setting. Four digit passwords are not considered sufficiently secure and most devices will support passwords of at least six digits. • Staff owned devices that are also used for personal purposes should not be used to download personal or commercially sensitive University data. • Personal or commercially sensitive University data should only be transmitted using University provided devices and in an appropriately secure fashion. • Personally acquired applications, file stores and cloud based data repositories must not be used to manipulate, transmit or store University data. • Any device or application procured at the University's expense must be acquired via the normal IT equipment/software purchasing processes. • Smaller mobile devices such as mobile phones and tablets that are used to synchronise with University outlook accounts or access University data should not be shared with other non-University users (such as family members). • Staff must report the loss of any personally owned device to IT Services if it is within the scope of this policy so the risk of a data breach can be assessed.
3	**Governance Requirements**
3.1	**Responsibility**
3.1.1	Information security remains the responsibility of all University staff but the following specific responsibilities are assigned to the following individuals and groups: • Overall responsibility for the University's strategic plans for information security rests with the executive board member serving as the Chair of the Information Security Steering Group (ISSG). • The Chief Information Officer is responsible for ensuring that the arrangements for governing the scoping, development, implementation and maintenance of University IT systems, networks and databases comply with the principles of good information security. This includes the development of network access controls to ensure that only appropriate access is available to those using their own devices • System owners are responsible for ensuring that IT systems they manage are configured appropriately and used effectively and that local rules for the appropriate use of staff owned devices are in place • All staff who are users of information systems must manage the creation, storage, amendment, copying, archiving and disposal of information in a manner which safeguards and protects its confidentiality, integrity and availability. This includes the use of staff owned devices to access, store or transmit University owned data. • All staff are responsible for accessing and engaging with all information security training and guidance provided by the University.
3.2	**Implementation / Communication Plan**
3.2.1	This policy will be initially communicated to managers via a Leaders Alert. Further dissemination will then take place as part of the broader plan to use all available communication channels to raise information security awareness among all staff.
3.3	**Exceptions to this Policy**
3.3.1	As this policy outlines the key principles of good information security practice and relates it to the use of staff owned applications and devices, exceptions to its principles and procedures are not expected. Any individual who wishes to use a personally owned app or device for purposes not allowed by this policy, for example, to access store or transmit sensitive University information must seek the prior approval of the University's Chief Information Officer