Access to information during periods of staff absence

Author	Associate Chief Information Officer (Information Governance & Assurance)
Approved by	Vice Principal (Planning & Governance)
Approval date(s)	September 2015
Review date	September 2016
Version	1.0 Approved
Document type	Protocol [Document types list]
Activity/Task	Information governance and security
Keywords	[Insert_Keywords]
Document location	[Insert_Saved_location]
Confidentiality	Public

Version Control Table

Version Number	Purpose / Changes	Author	Date
0.1	Initial draft	C Milne	14-April-2015
0.2	Revised following feedback received (18 May 2015): staff on research leave, Human Rights Act and producing records when information is accessed	C Milne	18-May-2015
0.3	Section 2.3 revised to emphasise that private non-work information e.g. holiday photographs are outwith the protocol's scope	C Milne	16-Jun-2015
0.4	Revisions made in response to comments received from UCU	C Milne	14-Aug-2015
1.0	Approved following discussions with Trade Unions (presented as Paper 03/15)		September 2015

Table of contents

1. Introduction

From time to time circumstances will arise when it becomes necessary for the University to access information held in e-mail and files (electronic and paper) when a member of staff is not present at work e.g. unplanned absence due to illness, on research leave,. There is a balance to be struck when accessing information in those circumstances. The University allows staff to make reasonable use of ICT facilities for personal use. That privacy has to be protected. However, in order to continue to function it may be necessary for steps to be taken to access materials when staff are not present, to help ensure that the operation of the University is not affected.

This protocol defines the circumstances under which access to information held in email and files can be made during periods of absence, either planned (e.g. annual leave, research leave) or unplanned (e.g. illness), and the steps to be taken when a member of staff returns to work where information has been accessed in their absence.

2. Objectives and scope

The objectives of this protocol are to:

- Raise awareness amongst staff that information held in e-mails and files may be accessed by authorised persons for business continuity reasons;
- Set out the controls that are to be followed before information can be accessed during the absence of a member of staff; and
- Alert staff to the steps that should be taken to minimise the likelihood that the University may seek to access information from e-mail and files during periods of absence.

2.1. Intended audience

This protocol applies to all members of staff and the University Court.

2.2. Where the protocol applies

This protocol applies to all e-mail and file systems where the University is:

- Recognised as the owner of the information and/or data held within e-mail and files etc.;
- Entitled to use information provided to it by a third party; and
- Responsible for personal and/or sensitive personal data as the data controller.

2.3. Where the protocol does not apply

This protocol does not apply to information held within shared mailboxes or group file shares, which have their own access arrangements, or to private information created or received for non-work purposes e.g. holiday photographs.

2.4. Principles

- Access to information in the absence of a member of staff must always be authorised by an appropriate University officer, within the conditions set out in this protocol.
- Access must always be necessary to support legitimate business continuity activities i.e. if the information in question were not available to the University and a function or obligation could not then be delivered or met, then access will be legitimate.
- Every effort will be made to first contact the member of staff, to understand if information can be secured without a search.
- Only the minimum amount of information necessary to provide business continuity should be accessed.

- Records must be created and maintained of the authorisation and any information that is subsequently accessed.
- The actions taken in the absence of a member of staff to access information will be explained to them on their return.
- It should be noted that confidential correspondence between staff and OHS or Trade Union representatives would not normally fall into this definition.

2.5. *Legislative and regulatory framework*

The University is responsible for protecting information and data that identify and relate to living persons, as per the provisions of the Data Protection Act 1998 (“the DPA”) and Human Rights legislation (right to a private life). This protocol is designed to ensure that any impact on a person’s personal life is minimised, while enabling the University to conduct its operations fairly and lawfully.

2.6. *Relationship with existing University Policy and Regulation*

This protocol provides overall direction and support for balancing protection of privacy while allowing for continuation of activities. There are a number of University policies, regulations and procedures which also provide (often specific) direction on managing the *confidentiality, integrity* and *availability* of University information and systems, notably the Information Security Policy and the Codes on the use and protection of personal and sensitive personal data. Relevant University policies and procedures currently include:

- The University Information Security Policy (2011);
- Regulations governing the use of University information and communications technology (ICT) facilities (2012);
- Student and staff Codes on the collection and use of personal and sensitive personal data (revised annually); and
- The Human Rights Act 1998.

3. Procedure

3.1. *Request for authorisation to access*

The Head of School/Unit or in their absence a deputy should e-mail the University’s data protection function dataprot@st-andrews.ac.uk detailing:

- The details of the member of staff who is absent – their name and the expected date when they will be available for work;
- Details of the information to be accessed and where it is believed that this is held e.g. e-mail;
- The reason(s) why access is required – this should note the projected impact on the University if the information in question is not made available; and
- The date by which a decision on authorisation must be made.

3.2. *Authorisation*

The criteria for authorisation will normally be the conditions set out in SCHEDULE 2 and 3 of the Data Protection Act 1998, notably SCHEDULE 2, paragraph 6(1).

In cases where it is assessed that authorisation is not appropriate, the request will be referred to the Vice Principal (Governance and Planning), who will make the final decision on authorisation.

The outcome of the authorisation process will be confirmed by either the Head of School or Unit, or the Associate Chief information Officer (Information Assurance & Governance) with the requestor (see Section 3.1 above). The authorisation will state what information is to be searched for and retrieved.

3.3. Retrieval of information

3.3.1. Electronic information held centrally

This information will normally be retrieved by IT Services staff. The information to be searched for and retrieved will be strictly limited to that set out in the approval.

Folders or e-mail messages marked PERSONAL should not normally be opened.

3.3.2. Marking items as private

Staff should mark their personal correspondence and information which is received or created outwith their duties of employment etc. as PERSONAL. The terms CONFIDENTIAL and STRICTLY CONFIDENTIAL should not be used for identifying personal information such as a folder of family photographs, as those terms are used to classify, identify and protect University information.

3.3.3. Information held in the School/Unit

This information should be retrieved by 2 members of staff from the School/Unit.

3.4. Return of information

Information of relevance, falling within the scope of the authorisation that is sourced from central e-mail and/or file systems will be made available to the requester. If there are any questions over the relevancy of any information retrieved, then the University Freedom of Information Officer or the Associate Chief information Officer (Information Assurance & Governance) will be advised and a decision will made by them on what information if any will be returned.

A briefing note summarising the steps taken to search for and retrieve the information will also be returned – even in the event of a null return i.e. when the requested information is not found.

3.5. Steps to be taken on the return of the member of staff in question

- The line manager or the Head of School, or Unit will brief the member of staff on the steps taken during their absence to locate and retrieve the information in question;
- An explanation of the approval process will also be given;
- The work that took place with the information in question should also be described; and
- A discussion should take place to determine what steps if any should be taken to improve access to business critical information with the view to minimising the requirement to apply this protocol at a future date.

4. Proactive steps to minimise the likelihood that information may need to be accessed during periods of absence

The following steps are indicative of the actions that should normally be taken to ensure that information remains available to the University:

- Storage of information within file shares that are only accessible to one person (the network account holder) should be minimised – information should normally be stored within shared files, where only those authorised to access the information can do so;
- Where relevant e-mail messages and any accompanying attachments should be transferred into a relevant shared file area;
- Prior to planned periods out of the office e.g. annual leave, attendance at conferences information that others are likely to require access to should be identified and appropriate arrangements for access made; and
- ***Only*** where it is judged reasonable to do so, attempts may be made to contact the member of staff concerned to ascertain if the information in question can be made available remotely e.g. via email or a file(s) etc. transferred to an accessible shared file area. In those circumstances the password assigned to the member of staff who is away from the University must not be shared or made known to any other person.

5. Responsibilities

All members of staff granted access to University information and systems have a responsibility to respond positively to this protocol. Specific responsibilities include:

5.1. Vice Principal Governance and Planning

- Adjudication, on steps to be taken to secure compliance with the protocol.

5.2. Associate Chief Information Officer (Information Assurance & Governance)

- Promoting the protocol and its implementation across the University;
- Providing training and awareness; and
- Working with Schools and Services to assess levels of compliance and to provide support to address any gaps.

5.3. Heads of School and Units

- Ensuring that this protocol is followed as appropriate; and
- Working with staff to minimise the need to implement this protocol (see section 4 above).

6. Methodology

The development of this protocol was partly informed by external benchmarking, drawing upon similar protocols, procedures or policies in use at other universities.

7. Review

This protocol will be reviewed at regular intervals. The review period will be approved by the Vice Principal (Planning and Governance) and recorded on the accompanying coversheet. Any significant change to University Policy or procedures primarily concerned with information *confidentiality, integrity and availability* may trigger an earlier review.

8. Protocol breaches

It will be a serious breach of this protocol where an attempt has been made to access information, or where information is accessed without authorisation (as described herein).

In the first instance any suspicion of a breach of this Policy should be reported to the Service Desk (IT), or the Associate Chief Information Officer (Information Assurance & Governance).

It will also be a breach of this protocol if information over which the University has a legitimate right of access (see section 2.2 above) is classified as PERSONAL, to deliberately place such items out of reach.

Where it is found that this Protocol has been breached, the Vice Principal (Governance and Planning) or their nominee will assess if further actions under University policy or regulation, including disciplinary, are required.

9. Availability

This protocol will be published on the University Website. The protocol can be made available in different formats, please direct any requests to the Associate Chief Information Officer (Information Assurance & Governance).

10. Contacts/further information

Enquiries regarding these Regulations can in the first instance be directed to the University Associate Chief Information Officer (Information Assurance & Governance).