Process for accessing a user IT account

Occasionally it is necessary to access the electronic account of a member of staff (account holder) who is not present. This may be because there is a legitimate business need to do so or where it is required in order to comply with a legal obligation.

**Scope**

An account includes any University provisioned email account; University provisioned storage space (e.g. H:Drive/C:Drive, or cloud storage services); or University provisioned social media account. Note that research post graduates will be covered by this process where access is required related to work that they are undertaking for the University.

In all cases **only those items which are directly relevant to the task at hand should be accessed.**

The following scenarios set out the process that should be followed in allowing access and in undertaking any search of an account. Note that where access is required for the purpose of investigation into alleged breaches of any University policy consent will not be required and the process under Section 7 of the [University IT Regulations](http://www.cardiff.ac.uk/public-information/policies-and-procedures/it-regulations) should be followed.

1. ***If the account holder is not present but is contactable.***
	1. The line manager of the account holder should contact them and explain the business need that necessitates access to the account including any timescales during which access will be required.
	2. If the account holder confirms that they do not object, a call should be logged with the IT Service Desk with the confirmation and account access may then proceed by the line manager.
	3. If the account holder raises objections and these cannot be resolved locally, the line manager should contact the Information Rights Manager in Strategic Planning and Governance and explain the basis for the objection and the business objectives served by access. The Information Rights Manager will consider the request in line with the legal requirements and IT Regulations and provide appropriate advice to the line manager and Head of School/Department in order for the Head of School/Department to come to a decision. The decision will then be communicated by the Information Rights Manager to the account holder.

1.4 Where any access is granted the good practice recommendations as outlined at point 6 below will be followed.

1. ***If the account holder is not present and cannot be contacted for permission***

2.1 It is not always possible to obtain an account holder’s explicit permission to access their account, for example if they are absent due to work-related stress and it wouldn’t be appropriate, are not capable of giving consent due to a severe medical circumstances i.e. coma, or are on an extended absence with no means of communication.

2.2 In such cases, the Head of School/Department should send an email to the IT Service Desk, confirming the conditions in 2.1 are met and the reason, and authorising access to the account by their nominated individual(s). The business objectives served by access should also be stated. This will be forwarded to the Information Rights Manager for information.

2.3 Where access is granted the good practice recommendations outlined at point 6 below will be followed. The account holder’s line manager will be responsible for notifying the account holder regarding access when they feel it is appropriate to do so.

* 1. Where a member of staff is likely to be absent and uncontactable for some time and to avoid prolonged access being required, the Head of School/Department may authorise that an Out Of Office be set up on the email account which will provide an appropriate alternative contact email address.
1. ***If the account holder is deceased***

3.1 Where the University becomes aware of the death of an account holder and it is unexplained, the account will be put on legal hold until such time as it is established that the information will not be required for any evidential or legal purpose i.e. Coroner’s enquiry. At this point the account will be flagged for deletion as per the usual process. Where the death is not unexplained the established protocols to deal with such circumstances held in HR (staff) and Registry (students) will be followed.

3.2 Where there is business critical information contained within the account that is required by the School/Department, the process for access as outlined from point 2.2 above will be followed.

***4. Access to non-work related material held on University IT assets***

4.1 As per the University IT Regulations any information or data held on University controlled IT assets that is for private use is placed there at the account holders own risk. As such the University will not normally consider requests for access to that data from the account holder themselves or any third party, subject to the following exceptions:

- Where a request is received from a law enforcement agency or Coroner

- Where a request is received from a solicitor representing the account holder or their estate

4.2 In the above circumstances the account will be put on legal hold and the request should be forwarded to the Chief Information Officer or Director of Strategic Planning and Governance for consideration in consultation with the Information Rights Team.

4.3 Requests for access to work related personal data should be forwarded to the Information Rights Team in the first instance.

***5. University information held on non-University IT Assets***

5.1 University information should be handled in accordance with the Information Classification and Handling Rules. Where it is suspected that information is held on a private device in contravention of those rules the line manager of the account holder will request that the information is either returned and deleted, or simply deleted from the private device.

5.2 The account holder will be required to confirm that they have complied with any instruction to this effect from the line manager.

5.3 Where University information may have been compromised or inappropriately accessed due to it being held on a private device this will be raised as an information security incident via the IT Service Desk.

***6. Good Practice Recommendations***

* Two people are present when the account is accessed
* A record is kept of any items accessed
* The user is emailed afterwards with details of what has been accessed where appropriate
* The password to the network or email account is changed afterwards and no record kept of it

Requests for deletion of sent emails

Occasionally emails are sent in error to individuals who were not the intended recipient of that communication. The below process sets out the measures to be taken where such an event occurs and where a request is made for assistance in withdrawing the email. Under such circumstances it is important to act swiftly in order to minimise the impact of such errors.

It should be noted that technical assistance is only available where the email has been sent to recipients with a cardiff.ac.uk address. The University has no control over emails that have been sent to non-university email accounts. IT will communicate such limitations to the requestor.

Where the request is from the sender of the email the steps below should be followed.

Where the request is not from the sender it must be authorised in writing by the senders Head of School/Department or, where not available, the next most senior member of staff in the management chain.

In the case of emails constituting suspected breaches of the IT Regulations authorisation may also be provided by the Chief Information Officer or the Director of Strategic Planning and Governance . Steps 2-5 should then be followed.

1. Requests will only be considered where the contents of the email (including attachments), contain information that falls with the C1 Highly Confidential or C2 Confidential categories as outlined in the [University Information Classification Scheme](http://sites.cardiff.ac.uk/isf/handling/).
2. In order to aid identification of the email, the IT Service Desk should be provided with the full email address from which the email was sent including the date, time, subject, and a brief description of content. The full email addresses of the recipients should also be provided. Confirmation should be given by the sender that they have informed their line manager of the request
3. The IT Service Desk will log the call as an information security incident and notify the Mail team.
4. The Mailteam will undertake efforts to delete the email from all recipient’s Cardiff University mailboxes and a report will be provided to the sender and the Information Rights Manager into the success of the operation including where possible an indication of whether the mail had been accessed by the recipients.
5. In recognition that technical withdrawal of the email is not always guaranteed an email may be sent to recipients by the original sender. This should explain the error, and the action taken as well as any further action that may be required from the recipient. Any further action required will be monitored by the sender and updates reported to the IT Service Desk. A suggested template email is included below.

Misdirected Email - Template

Subject: Misdirected Email

Dear **[name]**

I am writing to make you aware that you may have been in receipt of an email from **[sender]** with the subject **[subject]** sent on **[date and time]**. This email was sent to you in error and contains confidential information. In accordance with University policy, the University has made efforts to withdraw this email from your inbox which has involved access to your account. No other content in your account was accessed in undertaking this exercise.

If the email has not been accessed and is not available in your account you need take no further action.

If the e-mail remains in your account you are requested to delete it immediately from both your inbox and trash and provide confirmation that this has been done. If you have accessed the e-mail I should advise that you are under a duty of confidentiality in accordance with the Student Code of Conduct/Staff Contract and the content of the email should not be divulged to anyone.

I would like to thank you for your co-operation in this matter.

If you have any further queries please contact me.

[Name]