Policy on Third Party Access to Staff Accounts

This policy covers the granting of access to staff accounts by another member of staff in the course of their duties. Primarily it concerns Email, but extends to all resources attached to the user's GoogleApps account. It may also be used where access to local Keele-based filestore is needed.

1. Shared Email Access

A number of email accounts require multiple users to access the email accounts, which may be either in the case of a generic role account (such as admissions@keele.ac.uk) or in the case of a PA accessing a Director's email account.

In these circumstances, as the practice is required for the normal operation of business, requests for multiple accesses to IT accounts should be made through the IT Service desk and will be dealt with in accordance with normal practice. Account holders should however endeavour that nominated staff are provided with the necessary access codes to cover those situations where the holder is unavailable.

2. Email Access for Planned Absences

Where it is known that a member of staff will be absent from work, local arrangements should be made for the provision of access to emails and information that may be required for business continuity purposes. Examples of local arrangements would be:

- Storage of key documents onto shared network drives
- Forwarding of emails to relevant colleagues
- Email notifications added to email accounts to notify senders that emails will remain unread
- In some circumstances, colleagues may also consider delegating access to email accounts, as described above.

3. Email Access by Third Parties

On some exceptional occasions, access to email (and data storage) may be required by a third party member of staff for the purposes of business continuity. It is expected that this access will normally

only be required in the cases of unexpected absences of members of staff, where the key information is retained only within the absent individual's account.

In these exceptional circumstances, IT Services can grant access to the relevant email account (or data store) to a third party member of staff pending authorisation from the appropriate Head of School/Section and Deputy Director of IT Services. Notification of any third party access to an email account or data store will be provided to the absent individual.

4. Third Party Access Guidance

Third party access will only be provided in circumstances where there is a critical business need to access the information in the absence of the individual and when the relevant authority has been granted to the individual requesting the access.

Individuals requesting access are reminded that upon being granted access to an account they should only view the information that is required in relation to the business need and treat all other information seen in the process of accessing the account as strictly confidential.

Access granted under this policy may permit the Third Party to view folders and documentation that is either labelled, or appears to be of a personal nature. In these circumstances, the Third Party should be aware that whilst access to this information is provided, the viewing of this information is strictly prohibited.

This policy should not be used to grant third party access for the purposes of gathering evidence in support of disciplinary or grievance proceedings. Where cases of staff misconduct are being investigated, access to accounts may be permitted under the terms provided in the Monitoring and Interception of IT Systems Policy.

5. Third Party Access Process

In order to be granted third party access to an email account or data store, a fully completed 'Third Party Access Request Form' must be submitted to the Deputy Director of IT Services (or nominee) through the IT Service Desk.

Before third party access is granted, a Head of School/Service is required to confirm the operational need for the access and approve the request by signing the form. Where it is the case that the Head of School/Service requests the access, approval should be obtained from the Dean/Director or in their absence, the Deputy Vice-Chancellor and Provost.

It should be noted that where third party access is granted, the third party may have access to any private, confidential or sensitive materials associated with the respective user account. As a result, Third Party access should ONLY be authorised where this is absolutely necessary for operational purposes (and preferably with the individual's consent).

Any person who is granted access to another user's account should only view that material considered necessary for the operational reason for which access was granted. They are required to treat all material viewed as confidential and not to act upon it or disclose it to any other person except those directly associated with the operational requirement for which the access was granted. They must preserve the confidentiality of any private or personal data that they may view inadvertently whilst undertaking operational matters.

6. Shared Data

Where staff wish to share data with other colleagues, this data should be shared where possible on the University network drives or if across Schools/Directorates, through Google drives which allows multiple user activity within the same document.

7. Access to Accounts of Former Employees

Where there is a planned leaving of an employee, local arrangement should be made for the transfer of any data from that individual's email or data storage (s:\ drive) into an appropriate location for the purposes of business continuity. Examples of local arrangements include:

- Forwarding of key on-going business activity emails
- Saving of documentation onto shared network drives
- Appropriate electronic archiving of emails and documents onto shared network drives
- Hard-copy documentation archiving whereby electronic archiving is not possible
- Out-of-Office notification on email correspondence
- Notification to IT Services of the requirement to suspend or close an account, that should be made inactive
- Request to IT Services for the establishment of a 'mail forward' on a discontinued account.
- Removal of any personal or confidential information related to the individual employee planning to leave

Where a School or Directorate need to access the data of a former employee for business continuity purposes, the Head of School or Service should email a request to it.service@keele.ac.uk which outlines:

- The name of the account holder
- Type of access required (email or S:\ drive)
- Period in question (dates or approximate dates of the emails/files)
- Subject of the data required (search terms)
- Reason why it is required.

IT Services will then conduct a search on the account as per the terms outlined in this email and provide the relevant information where it is identified. It is noted that this may be particularly likely in the unexpected cases of staff leaving.

8. Mail Forwarding

Where the automatic forwarding of emails for a former employee is required and sufficient justification for the need of access is provided under 5 above, the request should clearly stipulate the length of time the forwarding of emails is required for.

It is expected that in normal circumstances, on-going automated email forwarding will not continue for longer than 4 weeks, although requests for longer periods may be made in writing to the it.service@keele.ac.uk

9. Out of Office Messages

In the cases where retrospective access to an email account is not required to a member of staff email account for business continuity purposes, IT Services can enable an 'out of office' message to be sent in response to any email received to the absent member of staff's email account.

An Out of Office message can be provided upon written request to it.service@keele.ac.uk or through the IT Service Desk. It is the responsibility of the individual requesting the 'out of office' message to provide the contents of the message.

CONDITIONS FOR 3RD PARTY ACCESS TO STAFF ACCOUNTS

A copy of the form (below) must be completed and submitted to IT Services on each occasion that access is required to either the Mailbox, GoogleApps or University Drive (normally S:\ drive) of a member of staff during their **unexpected absence** or whereby an 'out of office' message is required, again due to unexpected absence.

Before third party access to an account is granted, the Head of School/Service is required to confirm the operational need and approve the request by signing the form. In addition, the Deputy Director of IT Services (or nominee) or in the case of IT Services staff, Director of Finance or Deputy Vice-Chancellor and Provost, should sign the form to provide the required authority.

If a Head of School/Service requires personal third party access to the account of one of their staff the application form must be authorised by the Dean/Director, or Deputy Vice-Chancellor and Provost in his/her absence. In the event of a Dean or Director requiring third party access to the account of one of their staff, the application must be approved by the Deputy Vice-Chancellor and Provost or Vice Chancellor.

It should be noted that where third party access is granted, the third party will have access to any private, confidential or sensitive materials associated with the respective user account. As a result, access should ONLY be authorised where this is absolutely necessary for operational purposes (and preferably with the individual's consent).

Any person who is granted access to another user's account should only view that material considered necessary for the operational reason for which access was granted. They are required to treat all material viewed as confidential and not to act upon it or disclose it to any other person except those directly associated with the operational requirement for which the access was granted. They must preserve the confidentiality of any private or personal data that they may view inadvertently whilst undertaking operational matters.

On signing the Third Party Access Request form, both the person who is to be provided with the access and those providing the authority, are certifying that they have read and understood these requirements.

This form should not be used for the purposes of gathering evidence in support of disciplinary procedures.

Keele University

THIRD PARTY ACCESS REQUEST FORM

To be completed by the person requiring access:

A1. Details of the account to which access is required (the person requiring access completes this part)

Name of Account Holder:_____Username of Account Holder: _____

School/Department:_____Access Required: Email ☐ S:// Drive ☐ Both ☐ (tick box)

Other ☐ Please Specify: _____

Please note: Email and S:\ Drive access should only be requested if absolutely necessary.

For email access please provide users email address: _____

Account holder aware? ☐ Not aware? ☐

Reason for Access Required:

_____

_____

A2. Details of the person requiring access (the person requiring access completes this part)

Name:_____Username: _____ Email Address: _____

School/Department: _____ Position: _____

Period Access Required: From _____ to _____

I have read and agreed to the Conditions governing my access to another user's data.

Signed: _____ Name: _____ Date: _____

B. To be completed by the requestor's Head of School/Service and sent to IT Services once completed.

I authorise the person named in Section A2 to access the user account of the person named in Section A1 for the reason and period specified. Where access to both email and the S:\ drive has been approved, I confirm that this is necessary for business continuity purposes.

Signed: _____ Name:_____Date: _____

Position: _____

C. To be completed by the Deputy Director of IT Services (or Director of Finance/Deputy Vice-Chancellor and Provost if for a member of IT Services Staff.)

☐ I authorise the access detailed in Section A1 above, to be granted to the person specified in Section A2 for the duration stated.

Or

☐ The access is declined because:

_____

Signed:_____Name: _____ Date: _____

Actioned by:_____Name:_____Date: _____