Leeds Beckett University
Access to staff email accounts and staff[1] filestores

Context

1. In usual circumstances, the university will not access filestores or mailboxes without the knowledge of the individual concerned.

2. From time-to-time, however, it may be necessary for the university to have access to filestore or email accounts of individual members of staff, either when those staff are absent from the university, or in order to facilitate an investigation under disciplinary or other procedures. This document sets out the protocol by which this will be authorised.

3. This protocol distinguishes between instances of staff being absent and instances where access is required for investigations.

4. The university recognises its responsibility under data protection legislation[2], and will act proportionately in accessing filestores or mailboxes, only where there is a legitimate business need to do so. This protocol is designed to inform staff when such access may be granted, why, and by whom.

Access to accounts when staff are absent

5. Where a member of staff is absent from the university on annual leave, maternity / paternity/parental/adoption leave, or other planned absence (including for medical reasons and on sabbatical), and is expected to be away from the university for a significant period, then arrangements should be made with the relevant manager for delegate access to be given to filestores and/or mailboxes before that individual takes leave, if this will be necessary for business purposes. Usually, the use of group mailboxes and shared drives, and the activation of out-of-office messages will be sufficient to cover planned periods of absence.

6. Where a member of staff is absent for reasons of ill-health, or for any other reason that could not be foreseen, and access is required to that individual's filestore or mailbox, then authority (as set out below) will be given on request of the relevant Dean of School / Director of Service to the Director of IT Services.

7. Normally, access will be granted to the absent member of staff's line manager, or another individual within the management chain, but on occasion it is recognised that different arrangements may need to apply. For example, if granting access to a particular individual in these circumstances might compromise any other processes that are ongoing then a different approach may need to be taken. The line manager

---

[1] The definition of staff for this purpose includes anyone who has a 'staff' email account and/or filestore, so would include associates and contractors with such access, not just employees.

[2] The Information Commissioner has produced guidance (https://ico.org.uk/media/for-organisations/documents/1064/the_employment_practices_code.pdf) which includes good practice on these matters. This protocol is part of the university's attempts to duly inform staff.

should consider any research materials stored by the member of staff concerned, and ensure that these are treated in accordance with appropriate ethical considerations.

8. In such circumstances, it will be for the Director of IT Services, in discussion with the University Secretary (or, in their absence, the Deputy University Secretary), to determine appropriateness of a request to grant access, and to whom.

9. Efforts should be made to advise the member of staff whose filestore or mailbox is to be accessed, although it will not preclude access being given if it is not possible to contact the member of staff. The method of communicating with staff will depend on the circumstances.

10. Emails marked 'private' (using the Outlook designation) will not be accessed in these circumstances. Members of staff should ensure that emails which are personal are marked as private to prevent inadvertent opening.

Access to accounts to facilitate investigations

11. On occasion, it may be necessary for access to be granted to a member of staff's filestore or mailbox to facilitate investigations under the disciplinary, grievance or other policies of the university, such as those that relate to harassment, or the prevention of fraud and anti-bribery. This would include instances where a member of staff has been suspended pending investigation, or where no suspension has been enacted and there is reason to believe that a member of staff has committed some form of serious misconduct. Access shall be limited to those files and emails which appear relevant to the allegations or issues under investigation.

12. Authority to access must be given by the University Secretary (or, in their absence, the Deputy University Secretary) in consultation with the Director of Human Resources (or, in their absence, the Deputy Director). Access will only be given to the investigating officer under the relevant procedure, and where appropriate to the HR advisor supporting the investigation. In granting access in such circumstances, consideration will be given to the nature of the allegations and the level of seriousness and thus the need for access without prior warning.

13. Where a member of staff is research-active particular care will be taken to ensure that any sensitive research material is not included in any review. If possible, the relevant Director of Research would be consulted before authority is granted.

14. Where access is required to the filestore or mailbox of a member of the University Executive Team (UET) and the University Secretary is absent, the Deputy University Secretary must consult the Vice-Chancellor first.

15. Where access is required to the filestore or mailbox of the University Secretary, the Director of Human Resources should seek the authority from the Vice-Chancellor, without involvement of any member of the University Secretary's Office.

16. If access is to be granted to the filestores or mailboxes of either the Vice Chancellor, the University Secretary or the Director of Finance, then the Chair of the Audit Committee should be advised.

Records

17. The Director of IT Services will keep a record of access given to individual filestores and mailboxes, noting the duration and level of access given. They must review, regularly, whether access continues to be necessary, consulting with the Dean / Director, or the University Secretary, as appropriate.

Appropriate use / Confidentiality

18. Any individual accessing another's filestore or mailbox should be reminded of the need to ensure only appropriate use of that filestore or mailbox.

19. These protocols are intended for considering activity which relates to the individual's employment within the university.

20. Due confidentiality will be respected when reviewing emails or files including in compliance with the needs of research ethics policies and procedures.

21. Staff are reminded that use of the university's email system is primarily for business use, and is subject to our email use policy [and any other relevant policies], which is available online. Personal use is permitted in certain circumstances (as set out in university policy).[3]

Approved by the University Executive Team
27 June 2017
Amended August 2017, for discussion with Trades Unions
Amended December 2017 after review by DWF
Further changes made May 2018

[3] See http://www.leedsbeckett.ac.uk/public-information/it-security-policies/