THE UNIVERSITY of EDINBURGH

People and Money Data Access Protocol

Purpose

The purpose of this protocol is to define the terms and conditions for individual access to data within People and Money.

Introduction

These terms and conditions relate to access to data accessed via all apps within the university's People and Money system (Oracle Fusion).

Members of staff are provided with access to People and Money via individual UUN authentication, following appropriate authorisation and implementation of account access (see example People and Money Access application form on the HR A-Z Forms webpage). The access process is managed by the People and Money Service.

It should be noted that HR, Finance and Student Services are the Staff, Financial and Student data owners including the data held in People and Money. People and Money Service is the curator of People and Money data, however delivered, and for as long as it exists the data is subject to the following **Terms and Conditions:**

Terms and conditions for individual access to staff, workers, student or supplier data regardless of data:

Specific Terms

1. You must only access information about identifiable individuals (**staff, workers, student or supplier)** when it is necessary for you to do your job.

2. You can only access and use the data for purposes associated with your job role. (https://www.ed.ac.uk/data-protection/data-protection-policy)

3. You must follow the guidance on disclosing information about **staff, workers, student or supplier** when releasing data to third parties. It may be a criminal offence to disclose this information in any circumstances. (https://www.ed.ac.uk/data-protection/data-protection-guidance)

4. Printed documents containing **staff, workers, student or supplier** data must be securely destroyed.
(https://www.ed.ac.uk/data-protection/data-protection-policy)

General Terms

5. Do not access information about identifiable individuals on a screen that can be seen by other persons not covered by points 1-4.

6. Always lock your machine when leaving it unattended.

7. Only store data on University of Edinburgh systems and comply with university 'Bring Your Own Device' (BYOD) Policy: "*Use of Personally Owned Devices for University Work".*
(http://www.ed.ac.uk/files/imports/fileManager/BYODPolicy.pdf)

8. Any download data should be stored on an access limited area of the University network, in Office 365 or on an encrypted device and deleted when no longer needed.
(https://infosec.ed.ac.uk/how-to-protect/encrypting)

9. Follow local procedures for job role and handling personal data.

10. You must adhere to the University of Edinburgh's Confidentiality agreement.
(https://www.ed.ac.uk/data-protection/data-protection-policy)

11. Comply with the Guidelines on the processing of mass emails and e-announcements.
(https://communications-marketing.ed.ac.uk/internal-communications)

12. Adhere to the University of Edinburgh's Information Security Policy.
(https://infosec.ed.ac.uk/information-protection-policies)

13. Adhere to the University of Edinburgh's Computing Regulations.
(http://www.ed.ac.uk/information-services/about/policies-and-regulations/computing-regulations)

14. Adhere to the University of Edinburgh's Data Protection Policy.
(https://www.ed.ac.uk/data-protection/data-protection-policy)