Permission to take Data Off-Site

Personal Data should never be taken offsite in any form or downloaded onto non-UCB equipment via the Internet without prior approval. If you need to work on some personal information at home, you should read the instructions below and the form should be completed and approved by your Data Champion or the Data Protection Officer before any data leaves UCB. Non-UCB equipment is not necessarily as protected as that available to you on-site, so you must give your assurance that the data that you are working on at home cannot be accessed by anybody else and ensure that anything you save at home is deleted.

Name of Staff Member wishing to take data out of UCB	
Type of Data Being taken outside UCB	
How is the file stored? e.g. Surface pro/ USB	
Reason for removal of data	
Length of time data will be off-site	

Data Security Rules

Where we refer to the "personal data" below, this covers both "personal data" and "sensitive personal data" as defined by the Data Protection Legislation.

NEVER give your password to ANYBODY. If you believe somebody else knows your password, please change it immediately and inform UCB if you think there may be a problem.

NEVER store personal data on unencrypted transportable media. Transportable media is basically anything that can easily be removed from UCB, so things like USB memory sticks, CDs, DVDs, floppy disks, laptops etc. must not contain unencrypted personal data.

NEVER store personal data on an unencrypted laptop or Surface Pro. Laptops are an easy target for thieves and it is very easy to access data from a laptop, even if they don't know your password, so you should never store any personal data on an unencrypted laptop.

NEVER store personal data on a private PC, laptop or personal transportable media. Under no circumstances should personal data ever be stored or transported on non-UCB equipment/media.

NEVER email personal data to a colleague or external contact. Email is an insecure delivery and storage mechanism so it is unsuitable for transmitting or storing personal data without encryption.

If you currently have personal data which is stored insecurely, you must secure it immediately. You must remove any personal data from insecure locations. We would recommend you password protect any Word or Excel documents.

If you need to send personal data within or outside UCB then contact UCB about secure delivery mechanisms. Personal data should only be sent when absolutely necessary, and must be delivered securely. UCB's IT Support Unit can provide advice on how this can be best achieved.

Personal data may not be passed to any third party without written permission from UCB. The transport used for any such exchange must also be secure and the third party must agree in writing to comply fully with these rules.

If you become aware of ANY loss of personal data you must contact UCB immediately. The loss of any personal data is a serious matter and must be reported without delay, providing as much detail as possible using the Data Breach Procedure and form found at www.ucb.ac.uk/about-us/data-protection-resources.

By signing this form you are giving your assurance that you have read UCB's Data Protection Policy and rules and you will take every precaution to ensure the data will be encrypted and kept secure and will return it to UCB and delete any files held elsewhere.

Name: _____

Department:_____

Signature:_____

Date:_____

Authorisation

Name of Authorising Person: _____

Signature of Authorising Person:_____

Date:_____

Date last revised: 15/09/2022 v1.2