Data Security & Protection – Staff Guide

Introduction

As an institution University College Birmingham needs to ensure best practice in data handling. This includes data handled by our staff and students, who are bound by the same regulations. We have all sorts of data on people and organisations and all of this needs to be stored securely. The UK General Data Protection Regulations and The Data Protection Act 2018 in May 2018 requires all organisations to have appropriate security to protect personal information against unlawful or unauthorised use or disclosure, accidental loss, destruction or damage.

This is an introductory document giving some simple recommendations on data security. UCB must comply with the new regulations, so please follow the rules below.

We realise that many of these rules may require you to take immediate action and that this may cause you inconvenience, but it is essential we secure all personal data.

No personal data should be taken off UCB premises without prior permission of the Data Champion or Data Protection Officer – Ruth Cartwright.

Data Protection Act definitions

Personal Data is defined as "Any information related to a natural person or 'Data Subject', that can be used to directly or indirectly identify the person. It can be anything from a name, a photo, an email address, bank details, posts on social networking websites, medical information, or a computer IP address."

Sensitive Personal Data is defined as "personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, genetic data, biometric data, data concerning health or data concerning a natural person's sex life or sexual orientation."

Processing, in relation to personal data, means an operation or set of operations which is performed on personal data, or on sets of personal data, such as—
(a) collection, recording, organisation, structuring or storage,
(b) adaptation or alteration,
(c) retrieval, consultation or use,
(d) disclosure by transmission, dissemination or otherwise making available,
(e) alignment or combination, or
(f) restriction, erasure or destruction

Data Security Rules

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

- **NEVER take any personal data off UCB premises** without prior permission of the Data Protection Officer (Ruth Cartwright) or the Data Protection Champion for your area.

- **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, etc. must not contain unencrypted personal data. This would also include hard copy documents such as class lists, registers, class notes etc.

- **NEVER store personal data on an unencrypted laptop, mobile phone 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, mobile phone or Surface Pro or personal transportable media.** Under no circumstances should personal data ever be stored or transported on non-UCB equipment/media.

- **NEVER store personal data on your PC hard drive or Windows desktop.** Data stored on your C: drive or on your Windows desktop is insecure. All files must be stored on network drives.

- **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. Any personal data should be encrypted before sending and a password sent separately.

- **When you send a global email to students, ensure their email addresses are bcc**. This will ensure that you do not inadvertently share personal email addresses with everybody.

- **Ensure email addresses that are predicted by Outlook are correct.**

- **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 and store them on a network drive.

- **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. The government are currently considering making loss of data a criminal offence.

1.2	*15/09/2022*	*DPO*
1.2	*21/08/2023 (reviewed)*	*DPO*
1.3	*08/08/2024*	*DPO*