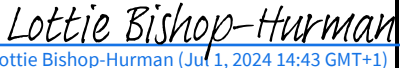





ECTU Central Office POL04: Bring Your Own Device - Data Security Compliance when Accessing ECTU Workspaces from Personal Devices

Version No:	1.0
Issue Date:	02 Jul 2024
Effective Date:	17 Jul 2024

Authorship and Approval			
Name and Designation	Author/Reviewer /Approval/ Authorisation	Date	Signature
Lottie Bishop-Hurman Data Manager - Digitally Enabled Clinical Trials	Author	01-Jul-2024	 Lottie Bishop-Hurman (Jul 1, 2024 14:43 GMT+1)
Kenton D'Mellow Data Management & Programming Team Lead	Reviewer	01-Jul-2024	 Kenton D'Mellow (Jul 1, 2024 15:02 GMT+1)
Joyce Thomson Chief Operating Officer	Approver	01-Jul-2024	 Joyce Thomson (Jul 1, 2024 15:06 GMT+1)

Document Revision History		
Version No.	Effective Date	Summary of Revisions
1.0	17 Jul 2024	Initial Creation

The user of this document is responsible for ensuring it is the current version.

1.0 PURPOSE

This policy outlines the bring your own device (BYOD) requirements ECTU staff must meet in order to comply with data security compliance and information governance, including encryption standards.

2.0 SCOPE

This policy applies to all members of ECTU who use their own devices, including tablets, smartphones, PCs, laptops, etc. for work purposes involving accessing data that could be considered sensitive or personally identifiable. This policy does not apply to accessing the Microsoft Multi-Factor Authenticator application.

This policy will be reviewed every year.

3.0 POLICY

3.1 Staff Induction and Training on the use of personal devices

- Staff are trained in the process for accessing ECTU work interfaces on personal devices via the Data Protection Essentials and Information Security Essentials courses provided by the University. This training is mandatory for new staff during the induction period. Existing staff are required to conduct this training annually in line with DSPT requirements.
- Staff are required to read and receipt this policy as a means of acknowledging the requirements around the ECTU's BYOD stance.

3.2 Requirements for Accessing ECTU Data on a Personal Device

3.2.1 University managed devices should be used for work that could potentially involve participant identifiable or sensitive information.

3.2.2 University of Edinburgh permits staff to use their own devices for limited work purposes. For example, accessing emails and multi factor authentication (MFA). Staff are only permitted to use personal devices that are equipped with a biometric/ active passcode. Personal laptops/computers must be equipped with BitLocker or FileVault.

3.3 Device encryption

3.3.1 University of Edinburgh policy states that all portable devices processing any university information must be protected by encryption. This refers to all data types and not just sensitive data. For guidance on how to encrypt devices, including smartphones and tablets, please see the Information Services Group website at <https://www.ed.ac.uk/infosec/how-to-protect/encrypting>.

The user of this document is responsible for ensuring it is the current version.

3.4 User Responsibilities

- 3.4.1** Users must not deliberately put their device at undue risk of being stolen, lost or accessed by unauthorised persons.
- 3.4.2** Stolen or lost equipment must be reported as soon as possible to ig.ect@ed.ac.uk.
- 3.4.3** Users will not store any participant identifiable or sensitive data on personal devices.
- 3.4.4** Where available users may connect their personal device to the University of Edinburgh's wireless network to get internet access.

3.5 Data Security Incidents resulting from the use of personal devices

- 3.5.1** Any deviations from sections 3.2 to 3.4 are considered "data security incidents". These must be reported to the Digitally Enabled Clinical Trials (DECT) team in detail, by emailing ig.ect@ed.ac.uk, including date and time of the near miss, who is reporting the near miss, who is responsible, and details of the occurrence.
- 3.5.2** The DECT will notify the Chief Operating Officer of any incidents, including any further action needed to ensure data security in the future.

4.0 RELEVANT DOCUMENTS AND REFERENCES

The user of this document is responsible for ensuring it is the current version.









ECTU Central Office POL04- BYOD-Data Security Compliance when Accessing ECTU Workspaces from Personal Devices v1.0


Final Audit Report


2024-07-01


Created:	2024-07-01 (British Summer Time)
By:	Tanya Tharakan (tanya.tharakan@ed.ac.uk)
Status:	Signed
Transaction ID:	CBJCHBCAABAAHIBmocleWpUBGv7Xgww0jl6QRWzbe1oi


"ECTU Central Office POL04- BYOD-Data Security Compliance when Accessing ECTU Workspaces from Personal Devices v1.0" History

-  Document created by Tanya Tharakan (tanya.tharakan@ed.ac.uk)
2024-07-01 - 14:19:17 GMT+1- IP address: 192.41.114.230
-  Document emailed to lottie.bishophurman@ed.ac.uk for signature
2024-07-01 - 14:23:41 GMT+1
-  Document emailed to Kenton D'Mellow (Kenton.D'Mellow@ed.ac.uk) for signature
2024-07-01 - 14:23:42 GMT+1
-  Document emailed to Joyce Thomson (joyce.thomson@ed.ac.uk) for signature
2024-07-01 - 14:23:42 GMT+1
-  Email viewed by lottie.bishophurman@ed.ac.uk
2024-07-01 - 14:42:30 GMT+1- IP address: 104.47.11.126
-  Signer lottie.bishophurman@ed.ac.uk entered name at signing as Lottie Bishop-Hurman
2024-07-01 - 14:43:29 GMT+1- IP address: 195.213.97.229
-  Document e-signed by Lottie Bishop-Hurman (lottie.bishophurman@ed.ac.uk)
Signature Date: 2024-07-01 - 14:43:31 GMT+1 - Time Source: server- IP address: 195.213.97.229
-  Email viewed by Kenton D'Mellow (Kenton.D'Mellow@ed.ac.uk)
2024-07-01 - 14:56:07 GMT+1- IP address: 81.78.139.15

 Document e-signed by Kenton D'Mellow (Kenton.D'Mellow@ed.ac.uk)
Signature Date: 2024-07-01 - 15:02:22 GMT+1 - Time Source: server- IP address: 81.78.139.15

 Email viewed by Joyce Thomson (joyce.thomson@ed.ac.uk)
2024-07-01 - 15:05:49 GMT+1- IP address: 104.47.11.62

 Document e-signed by Joyce Thomson (joyce.thomson@ed.ac.uk)
Signature Date: 2024-07-01 - 15:06:28 GMT+1 - Time Source: server- IP address: 94.14.215.249

 Agreement completed.
2024-07-01 - 15:06:28 GMT+1