MANAGEMENT OF PORTABLE ELECTRONIC DATA STORAGE DEVICES AND MEDIA POLICY			
Department	ICT Services		
Author	Legal Services Advisor		
Authorised By:	Director of Operations		
Implementation By:	Associate Director for IT Services		
Policy Reference:	POIT1718008		
Policy Replaced:	POIT1617007		
Version No:	1	**Approval Committee:**	VCB
Date approved:	17.04.18	**Minute no:**	17.96.07
Status:	Approved	**Implementation Date:**	May 18
Period of approval:	3 years	**Review Date:**	May 21
I have carried out an equality impact assessment screening to help safeguard against discrimination and promote equality.			✓
I have considered the impact of the Policy/Strategy/Procedure *(delete as appropriate)* on the Welsh language and Welsh language provision within the University.			✓

Executive Summary

This document describes the policy for ensuring the secure storage and management of confidential University related data held on or accessed via portable devices and storage media. The purpose of this document is to ensure that information is kept securely from unwanted use and protected from loss and/or becoming unavailable for use.

Governance

Oversight of the execution of, and compliance with, this policy rests with the Associate Director for ICT

Definitions

Portable Device: Hand-held and other hand-portable computing equipment which is used for accessing, storing or processing University data, including (but not limited to) laptop PCs, tablets, mobile telephones and PDAs.

Portable Media: Readily-transportable items used to store data in electronic form (whether temporarily or long-term), including data sticks (“flash drives”), floppy disks, compact discs (CDs and DVDs), plug-in external drives and media players (mp3 players).

Confidential Data: Information about or connected with the University's business (including Personal Data and Sensitive Personal Data, as defined below) which the user has an obligation to treat as confidential and protect from unauthorised use, access or release.

Personal Data: Means any information about any living, identifiable individuals.

Sensitive Personal Data: Is a sub-set of Personal Data, and means personal information about an individual's racial or ethnic origin; political opinions; religious beliefs; trade union membership; physical or mental health or condition; sexual life; commission or alleged commission of any offence; any proceedings for any offence actually or allegedly committed by that individual, the disposal of such proceedings or the sentence of any court in such proceedings.

User: A member of WGU staff or other person making authorised use of a portable device or portable media to store, access or manipulate Confidential Data

Policy

1. General duty to protect data

1.1 All WGU employees and those who are formally engaged to work or act on behalf of the University have a contractual obligation to take adequate steps to prevent unauthorised use or disclosure of Confidential Data and must take reasonable care to protect the portable device or media from loss or theft.

1.2 In addition, the protection of Personal Data is a legal obligation imposed by the GDPR and the DPA. A breach of that obligation can bring significant financial penalties and other sanctions for those responsible. The GDPR requires adequate steps to be taken to protect Personal Data, with even greater care expected to protect Sensitive Personal Data in view of its private nature.

1.3 Sensitive Personal Data must not be stored on a portable device or media except as provided for in section 2.3.

1.4 A breach of this Policy may result in serious disciplinary action using the University Disciplinary procedure, irrespective of any penalties or sanctions which may be imposed by the Information Commissioner in respect to any failure to protect personal or sensitive personal data

2. Minimising the transfer of Confidential Data to portable devices and media

2.1 As a general principle, Confidential Data should be held securely on the University's core systems, should be accessed and managed using only those systems, and should not be downloaded for storage or remote manipulation on portable devices or media.

2.2 Wherever available, secure online file transmission procedures must be used in preference to portable media to send Personal Data directly to authorised external recipients.

2.3 In the event that it becomes essential to place confidential data on a portable device or media or where use of portable media is the only viable option for transferring data transfer, ICT approval of the device must be sought (ICT will ensure that the portable device or media must meet the minimum protection criteria specified in Section 3 below). Once approved, copying to the device needs no further approval. However,

the portable device or media must be kept secure and handed back to ICT once you have transferred your data to ensure that the data on the particular device is removed securely and in accordance with the University Data Protection and Data Disposal policy Section 5c – Disposal of Data

2.4 Data copied to portable devices or media must be deleted at the earliest opportunity.

2.5 Personal Data must never be stored in unprotected form on portable devices or media.

3. **Minimum Protection Criteria**

3.1 Portable devices or media used to access or store Confidential Data must meet the minimum security requirements specified in the table below.

3.2 These requirements apply irrespective of who owns the equipment or media involved; i.e. a portable device that is not owned or supplied by WGU can only be used to access or store Confidential Data if its use has been approved by ICT and it meets the security requirements described in the table below.

DEVICE OR MEDIA TYPE	**SECURITY REQUIREMENT**
Laptop PC, tablet PC or equivalent	Device must use whole disk encryption
Mobile phone	Power on password/pin; auto time out keyboard lock; encryption if available
USB memory stick/USB flash drives	USB must employ hardware based encryption with software to setup and manage the passphrase to use device
CD/DVD/external hard drives or memory cards	Data must be encrypted prior to storage
Floppy disk	Data must be encrypted prior to storage
Tape/microfiche	Tapes or microfiche to be stored on site in fireproof safes with limited access
Other devices which allow storage of files e.g. IPad, IPod, MP3 players	These devices should not be used unless they offer protected storage whilst in transit. IPods and MP3 players do not offer this protection so therefore should not be used. please contact ICT service desk about specific devices

Diabled access devices that contains storage	These devices should not be used unless they offer protected storage whilst in transit. contact ICT service desk who will provide advice on these devices
Personal Digital Assistant (PDA) or recording devices	These devices should not be used unless they are secure. PDA or recording services do not offer this protection and therefore should not be used for any personal data. please contact ICT service desk about specific devices

Where a password/passphrase or PIN is required to unlock a device, this must be protected by the individual and NOT shared or given to anyone else. Sharing or giving your password to someone else, giving them access to personal sensitive data may lead to disciplinary action.

4 Action to be taken in the event of actual or suspected loss of Confidential Data

4.1 The user **must immediately** notify the Director for ICT, the Data Protection Officer and the SIRO or in his absence the Deputy SIRO of the occurrence of any of the following and comply with reasonable instructions or directions from ICT to minimise any attendant risk:

4.1.1 Theft or loss of a portable device on which Confidential Data was stored or could be accessed;

4.1.2 Theft or loss of portable media containing Confidential Data, including media sent to an external recipient which has failed to reach its destination;

4.1.3 Actual or suspected use of the user's portable device to gain unauthorised access to Confidential Data;

4.1.4 Any other incident involving a portable device or media under the user's control which represents an actual or potential compromise to the security of Confidential Data.

Other supporting documents and material

- IT Asset Management Policy
- IT Security Policy
- Data Protection Policy
- Data Protection and Data Disposal Policy
- DPA guidance on the ICO website at: http://www.ico.gov.uk

5. Process Owner

The Associate Director of ICT is responsible for the development, compliance monitoring and review of this policy and any related procedures.