Information Systems

Data Security
Policy for portable devices and storage media

Purpose of this Document

This document describes the University's Policy for ensuring the security and proper management of confidential data that is held, used on or accessed via portable computing devices and portable storage media.

This document will be reviewed every 12 months

Author:	Matt Mason
Version:	1.3
Date:	Sept 2017

NOTTINGHAM
TRENT UNIVERSITY

Review/Approval History for this Document:

Organisation	Action	Date
Information Systems Management Team; Legal services	Provide overall direction for content	
SMT	Approve document for publication	

Document Control:

Version	Author	Date	Version details	Reviewer	Date
0.1	DS/BT	12 May 2011	First Draft		
0.2	RHAE	16 May 2011	Updates to first draft		
1.0	RHAE	27 June 2011	Update to version 1 folloing approval at SMT	**SMT**	06-06-11
1.1	MM	8 May 2012	Annual review		
1.2	MM	8 May 2012	Annual review	P Nicholson	07-04-14
1.3	MM	11 May 2015	Annual review and minor additions	P Nicholson	13-05-15
1.3	MM	20 Sept 2017	Annual review, no changes		

Contents

Review/Approval History for this Document: 2
Document Control: 2
Contents 2
Executive summary 3
Governance 3
Definitions 3
Policy 4
Other supporting documents and material 5
Process Owner 6
Process Manager 6

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 content of this policy has been informed by reference to related legislation (primarily the Data Protection Act 1998 – the "DPA"), guidance issued by the Information Commissioner, and recommendations arising from Internal Audit reviews.

The Information Commissioner has (and is increasingly using) the power to impose significant financial penalties of up to £500,000 and potentially onerous procedural requirements on those who fail to properly protect data relating to individuals (Personal Data).

This policy is intended to promote and embed good practice in the management and use of data, particularly personal data and commercially sensitive data, and in so doing minimise the risk of action against the University and its employees for breaches of legislation, regulations or contractual obligations.

Governance

Oversight of the execution of, and compliance with, this policy rests with the Information Security & Audit Manager.

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 NTU 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 NTU 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 DPA. A breach of that obligation can bring significant financial penalties and other sanctions for those responsible. The DPA 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. Information on this service (Zendto) is available from the IS Service Desk.

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, IS approval of the device must be sought (IS 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.

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 NTU can only be used to access or store Confidential Data if its use has been approved by IS 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
Personal Digital Assistant (PDA)	Power on password/pin; auto time out keyboard lock; encryption if available
USB Memory Stick	USB device must employ hardware based encryption with software to setup and manage the passphrase to use device.
CD/DVD	Data must be encrypted prior to storage
Floppy Disk	Data must be encrypted prior to storage
Tape	Tapes to be stored on site in fireproof safes with limited access
Other devices which allow storage of files eg. 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. Please contact ITS 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.

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

4.1 The user **must immediately** notify the IS Security Manager of the occurrence of any of the following and comply with reasonable instructions or directions from IS 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

- NTU's IT Asset Management Policy
- NTU's Computer Use Regulations
- DPA guidance on the ICO's website at: http://www.ico.gov.uk
- 10 Steps to Data Security
- Data Protection Policy

Process Owner

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

Process Manager

The Information Security & Audit Manager is responsible for the dissemination and implementation of this policy.