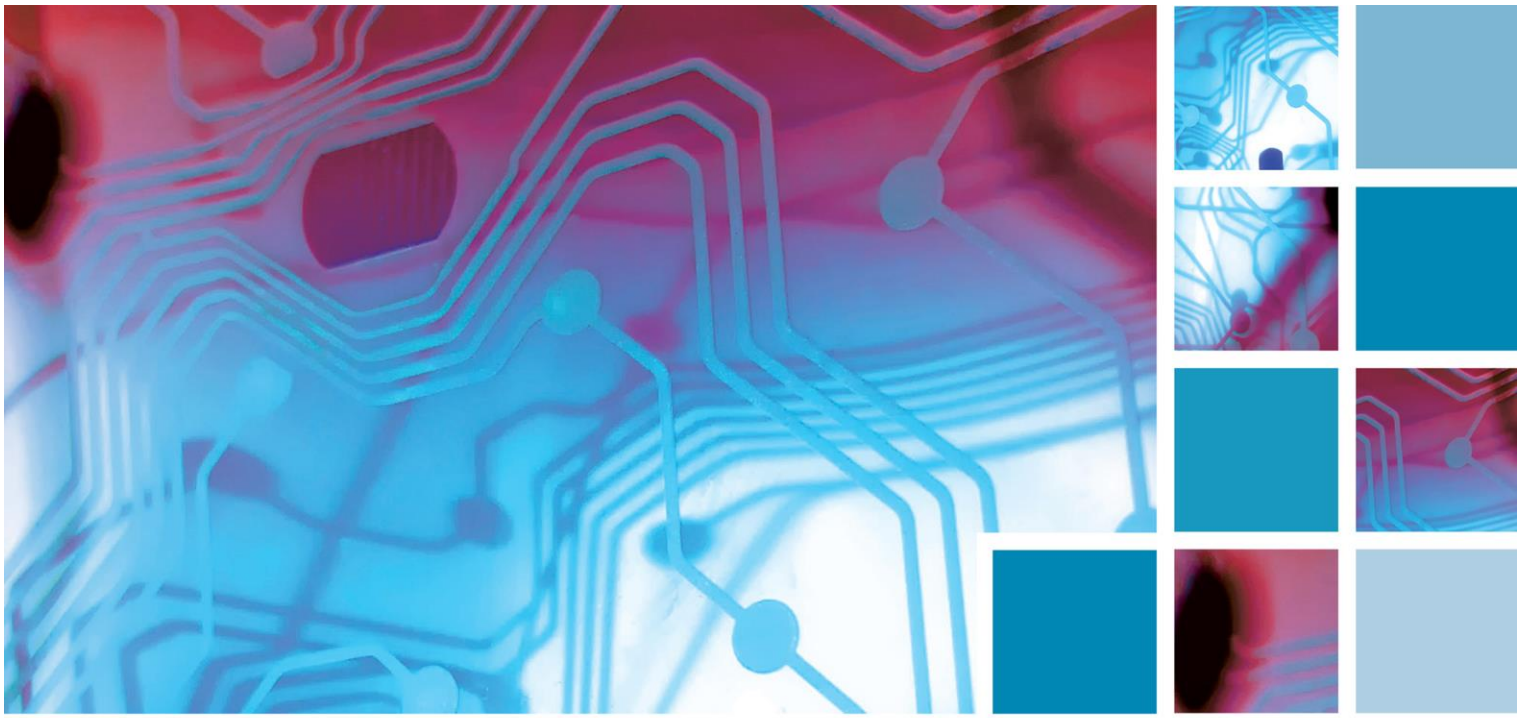

Information Systems

Bring Your Own Policy

Purpose of this Document

This document describes acceptable use pertaining to using your own device whilst accessing University systems and services.

This document will be reviewed every 12 months

Author:	Matt Mason
Version:	1.2
Date:	22 September 2017

NOTTINGHAM TRENT UNIVERSITY

REVIEW/APPROVAL HISTORY FOR THIS DOCUMENT:

Organisation	Action	Date
IS Management Team	Provide overall direction for content	May 2012

DOCUMENT CONTROL:

Version	Author	Date	Version details	Reviewer	Date
0.1	Matt Mason	20/05/13	First Draft	Mike Day; Peter Nicholson	20/05/13
0.2	Matt Mason	05/06/13	Amendments	Peter Nicholson	05/06/13
0.3	Dan Ladle	13/06/13	Copy Editing	Matt Mason	13/06/13
0.4	Tracy Landon	09/07/13	Amendments	Dan Ladle	06/08/13
1.0	Dan Ladle	06/08/13	Amendments	Matt Mason	11/09/13
1.1	Matt Mason	11/05/15	Amendments	Peter Nicholson	13/05/15
1.2	Matt Mason	22/09/17	Amendments	Peter Nicholson	25/09/17

CONTENTS

Executive Summary

This policy defines acceptable use by University users whilst using *"their own"* devices, systems and applications, for accessing, viewing, modifying and deleting of University held data and accessing its systems.

Intended Audience

This policy document applies to:

- All Users accessing NTU Services
- Any auditor, internal or external, appointed to review the process

Assumptions and Constraints

Nottingham Trent University ("the University") is a data controller, for the purposes of the Data Protection Act (1998). It is assumed that all staff have an awareness of the Data Protection Act (1998) and that they understand the consequences of the loss of University owned personal data.

Governance

IT management is regulated by the Computer Use Regulations for Nottingham Trent University available at http://www.ntu.ac.uk/cur

The policy will be subject to review, in line with University guidelines, for effectiveness.

Definitions

BYO – Bring Your Own refers to Users using their own device or systems (which are not owned or provided to you by the University) or applications, to access and store University information, whether at the place of work or remotely, typically connecting to the University's Wireless Service or VPN.

Data Controller - The Data Controller is a person, group or organisation (in this case the University) who determines the purposes for which and the manner in which any personal data are, or are to be, processed.

User – A member of staff, enrolled student, contractor, visitor, or another person authorised to access and use the University's systems.

Policy

Introduction

This policy covers the use of non-University owned/issued electronic devices which could be used to access corporate systems and store University information, alongside their own data. Such devices include, but are not limited to, smart phones, tablets, laptops and similar technologies. This is commonly known as 'Bring Your Own' or BYO.

If you wish to BYO to access University systems, data and information you may do so, provided that you follow the provisions of this policy and the advice and guidance provided through the Information Systems Service Desk.

It is the University's intention to place as few technical and policy restrictions as possible on BYO subject to the University meeting its legal and duty of care obligations.

Bring Your Own Policy

The University, as the Data Controller, remains in control of the data regardless of the ownership of the device. As a User you are required to keep University information and data securely. This applies to information held on your own device, as well as on University systems. You are required to assist and support the University in carrying out its legal and operational obligations, including co-operating with Information Systems should it be necessary to access or inspect University data stored on your personal device.

The University reserves the right to refuse, prevent or withdraw access to Users and/or particular devices or software where it considers that there are unacceptable security, or other risks, to its staff, students, business, reputation, systems or infrastructure.

Advice and Guidance

Advice and guidance on all aspects of this Policy are available via the Information Systems Service Desk:

Web: https://support.ntu.ac.uk
Email: support@ntu.ac.uk
Phone: 0115 848 8500 (then option 2)

Advice and guidance on Data Protection legislation are available from the University's Legal Services Department.

System, Device and Information Security

The University takes Information and Systems Security very seriously and invests significant resources to protect data and information in its care.

The use of your own device MUST adhere to the University's Computer Use Regulations.

In particular, when you use your own device as a work tool, you MUST maintain the security of the University's information you handle (which includes but is not limited to viewing, accessing, storing or otherwise processing).

From time to time, the University may require that you install or update University-approved device management software on your own device.

It is your responsibility to familiarise yourself with the device sufficiently to keep data secure. In practice this means:

- Preventing theft and loss of data (using Biometric/PIN/Password/Passphrase lock)
- Keeping information confidential, where appropriate.
- Maintaining the integrity of data and information.

You MUST NEVER retain personal data from University systems on your own device. If you are in any doubt as to whether particular data can be stored on your device you are required to err on the side of caution and consult with your manager, or seek advice from the Information Systems Service Desk.

You MUST:

- use the device's security features, such as a Biometric, PIN, Password/Passphrase and automatic lock to help protect the device when not in use.
- keep the device software up to date, for example using Windows Update or Software Update services.
- activate and use encryption services and anti-virus protection if your device features such services.

- install and configure tracking and/or wiping services, such as Apple's 'Find My iPhone app', Androids 'Where's My Droid' or Windows 'Find My Phone', where the device has this feature.
- remove any University information stored on your device once you have finished with it including deleting copies of attachments to emails, such as documents, spreadsheets and data sets, as soon as you have finished using them.
- limit the number of emails and other information that you are syncing to your device to the minimum required, for example only keep the past 24 hours of email in sync.
- Remove all University information from your device and return it to the manufacturers' settings before you sell, exchange or dispose of your device.

In the event that your device is lost or stolen or its security is compromised, you MUST promptly report this to the Information Systems Service Desk, in order that they can assist you to change the password to all University services (it is also recommended that you do this for any other services that have accessed via that device, e.g. social networking sites, online banks, online shops). You must also cooperate with University officers in wiping the device remotely, even if such a wipe results in the loss of your own data, such as photos, contacts and music.

You MUST NOT attempt to circumvent the device manufacturer's security mechanisms in any way, for example to 'jailbreak'[1] the device.

Further advice on securing personal devices (including advice on the risks of downloading untrusted Apps) is available from the Information Systems Service Desk.

Monitoring of User Owned Devices

The University will not monitor the content of your personal devices, however the University reserves the right to monitor and log data traffic transferred between your device and University systems, both over internal networks and entering the University via the Internet.

In exceptional circumstances, for instance where the only copy of a University document resides on a personal device, or where the University requires access in order to comply with its legal obligations (e.g. under the Data Protection Act 1998, the Freedom of Information Act 2000, or where obliged to do so by a Court of law or other law enforcement authority) the University will require access to University data and information stored on your personal device. Under these circumstances all reasonable efforts will be made to ensure that the University does not access your private information.

Under some circumstances, for example where you legitimately need to access or store certain types of information, such as student or financial records on your own device, you must seek authority from your Line Manager. The University may then need to monitor the device at a level which may impact your privacy by logging all activity on the machine. This is in order to ensure the privacy, integrity and confidentiality of that data.

You are required to conduct work-related, online activities in line with the University's Computer Use Regulations. This requirement applies equally to BYO.

Support

Where possible the University supports all devices, but you have a responsibility to learn how to use and manage your device effectively in the context of this policy.

Help and advice is available on a reasonable endeavours basis, via the Information Systems Service Desk, including help installing and configuring apps and other software.

Support forums are maintained at https://support.ntu.ac.uk/forums

[1] See http://en.wikipedia.org/wiki/IOS_jailbreaking and http://en.wikipedia.org/wiki/Android_rooting

Bring Your Own Policy

The University takes no responsibility for supporting, maintaining, repairing, insuring or otherwise funding employee-owned devices, or for any loss or damage resulting from support and advice provided.

Use of Personal Cloud Services

Personal data as defined by the Data Protection Act (1998) and University confidential information may not be stored on personal cloud services[2] and you should use the University provided OneDrive as part of Office365 which you login to using your normal University logon.

Compliance Sanctions and Disciplinary Matters

Compliance with this policy forms part of the employee's contract of employment and failure to comply may constitute grounds for action, under the University's disciplinary policy.

Equality and Diversity

This Policy has been reviewed for accessibility and inclusion purposes and has positive benefits, allowing the use of a broad range of devices to meet individual needs.

Feedback and Further Information

The University welcomes feedback on this Policy.

If you would like to comment or need further information on BYO please contact the Information Systems Service Desk.

Other Supporting Documents

NTU Computer Use Regulations – Regulations accepted by Users when granted access to the University Computer Network.

Information Systems Security Manual – Regulates the manner in which Information Systems are managed to ensure the security of information assets.

Process Owner

The Head of Infrastructure and Operations 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 throughout the University.

[2] Such as Apple iCloud, Dropbox, Google Drive, Microsoft Personal OneDrive, Box, etc. Also note products such as Evernote and OneNote should be considered cloud services.