A guide to Shadow IT at Bournemouth University

Please read the following guidance

It's your responsibility to read through and adhere to the guidance regarding the usage of Shadow IT at BU. Doing so can help to protect the university and the data it holds from cyber threats and data breaches.

Overview of your responsibilities

Your responsibilities

1. Only conduct university activities, which require the use of BU IT systems, via authorised IT Services. This includes hardware, software, enterprise solutions and cloud services.
2. The use of personal cloud services such as a non-BU OneDrive, Google Drive, Google Docs and Dropbox for university business is **prohibited.**
3. If you are already using Shadow IT to conduct university business and activities, please reach out to the IT Service Desk for advice.
4. Take a moment to familiarise yourself with and **follow the guidance provided in the relevant policies below.**

Guidance and policies

Using information technology provided by, or through BU

- **Policy: Acceptable Use Policy**
- This policy defines the way staff, students and other authorised users are required to use information and information technology which is provided by, or through BU. This includes, but is not limited to software, computer equipment and network connectivity.

Connecting mobile devices to the BU network

- **Policy: Network Code of Connection**
- This policy contains guidance on connecting managed and non-BU managed devices to the university's computer network and the security requirements these devices must meet. This includes guidance for staff, students, BU guests and visitor access.

Handling, saving, and sharing different types of information

- **Information Classification**
- This guidance explains how to handle, save, and share a range of data inlcuding public, non-sensitive, restricted and confidential. This concerns secure practices regarding collaborative tools, cloud storage, email, file transfer systems and hard copies.

Other related policies:

BU Information Security Policy Overarching Security Policy Data Protection Policy

Shadow IT - what's the problem?

Shadow IT - what's the problem?

Unauthorized software can lack the necessary security measures to protect sensitive information. Employees using unapproved systems, software, devices or applications may expose sensitive data to security vulnerabilities. These are the cracks in security where cybercriminals can sneak in and take advantage of our data.

Possible consequences of using Shadow IT

Breaches of sensitive information, however small, could lead to an inability to deliver education to our students. In some cases, **complete campus closure** may ensue to protect our computer network and the integrity of our human protective systems including fire alarms, door entry systems and CCTV.

This could undermine our competitive advantage leading **to loss of trust from our students, third parties, and research partners.** Financial losses and fines could also be imposed depending upon the severity and scope of a data breach.

What to do if you are already using Shadow IT?

If you are already using a form of Shadow IT to conduct university business, you

do not have to cease using it immediately, but you should contact the IT Service Desk to seek advice.

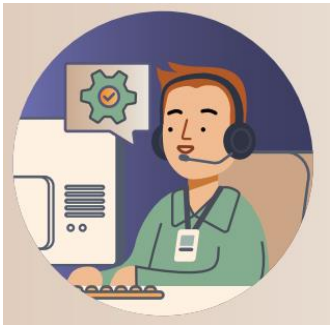
Please keep in mind: The use of personal cloud services such as a non-BU OneDrive, Google Drive, Google Docs & Dropbox for university business is prohibited.

Your responsibility to read our policies

The following policies are available to view on the staff intranet.

Please take a moment to read these; compliance with these policies enables us to keep our people safe and secure our networks, systems, information and equipment.

BU Information Security Policy
Acceptable Use Policy
Overarching Security Policy
Network Code of Connection
Classifying Information
Data Protection Policy



Questions and support

If you have any queries about these policies, please contact the IT Service Desk on (01202 9)65515, or freephone 0808 196 2332.

Thank you for helping to secure the universities future

A copy of this guidance is available from the IT SharePoint Hub