Network Code of Connection

A guide to connecting devices to the universities wireless or wired network.

As part of the ongoing cybersecurity program at Bournemouth University (BU), we have introduced a comprehensive set of controls and principles governing the types of devices authorised to connect to BU's networks. This includes a set of security requirements that must be met before access is granted.

These controls and principles are a key part of our commitment to strengthen the protection of our services and data assets and enhance the online security of the wider university community.

What devices do these rules and regulations apply to?
The controls and principles within this document are applicable to the following categories of device connecting to and using a BU owned and managed network resource:

- **Unmanaged devices** – such as personal devices, faculty owned and managed devices. (Smart phones, tablets, servers, laptops, routers, switches, network bridges and other network connectable devices).
- **Managed devices** - BU IT Services provided and supported devices.

These controls and principles **do not** apply to networks not owned or managed by IT Services, such as third party managed networks and resources.

Related policies/standards
Controls within this document are aligned to existing requirements as outlined in BU's wider policies and standards, including:

- Information Security policy
- BU Acceptable Use policy
- JISC Acceptable Use policy
- BU Threat and Vulnerability security standard
- BU End User Computing security standard
- BU Network Management security standard
- Logical Access Security Standard
- Information Security policies and technical standards

Security Requirements
All connecting devices must meet and comply with the **cyber and information security requirements** as detailed within this document and accompanying relevant BU Policy.

Terms of use
By connecting a device, as defined, to the BU owned and managed network means you:

- Accept and will abide by the controls and principles detailed below.
- Accept and abide by other relevant terms of use such as those detailed within the BU Acceptable Use policy and the wider BU Security Policies and standards.

Access provisions

Unmanaged Devices

- **Wireless connectivity -** devices used by staff, students, registered guests, or visitors may use the **BU WiFi or Eduroam** services. To utilise these services, you will be required to login using your BU credentials.
  The Cloud is an alternative internet access solution, and this will require registration prior to use (Registration instructions are available upon connection).
- **Physical wired connectivity** - Will only provide access to **Wepresent™**, there is no provision to access the network.

<table>
<tr><th colspan="3">Unmanaged device access provisions</th></tr>
<tr><td>Staff and students</td><td colspan="2">Access is limited to authenticated users only and provides access to the internet and the following additional BU services.
✓ Microsoft 365: Email, Word, Excel, PowerPoint, OneDrive, Teams and other Microsoft office applications (Installing Office365 for Students and Staff)
✓ AppsAnywhere™: Some applications are available remotely via the internet, meaning they can also be used on personal devices via the BU Wi-Fi. However due to software licensing constraints there may be some software applications that are only available via an IT managed device. (™).
✓ Horizon virtual desktop: Access to core university services and infrastructure can be obtained using the Horizon virtual desktop service (How to use Horizon).
✓ Wepresent™: Access to the digital presentation infrastructure is provided via Wepresent™.</td></tr>
<tr><td>BU guests and BU visitor access</td><td colspan="2">BU Wi-Fi: Access is only provided to those with valid temporary or visitor BU Credentials and access is limited to the internet and the digital presentation infrastructure (Wepresent™) only.

The Cloud: Is an alternative internet access provider and the use is limited to providing access to internet resources only.

When you connect to this network, a website will appear asking you to create a Sky Cloud account (this should only take a minute or two). Once you're signed up, you can access this WiFi network across both campuses.</td></tr>
<tr><td rowspan="4">Limitations and constraints</td><td>Access to core university services</td><td>No provision to access any BU core services, if access to internal services is required, please use the virtual desktop solution through the Horizon service.</td></tr>
<tr><td>Printing</td><td>No provision for direct network-based printing.
If printing is required, please use the BU email to print service.</td></tr>
<tr><td>Digital Presentations
Access to digital display and presentation solutions.</td><td>If presentation facilities are required, please use the audio/visual input cabling provided.</td></tr>
<tr><td>Alternative access solutions</td><td>BU Remote Access VPN.
A Remote Access Request can be made but will require relevant justification.</td></tr>
<tr><td>Exceptions</td><td colspan="2">All exceptions must be approved by IT Services
Raise an IT Service request via Hornbill.</td></tr>
</table>

IT Services provided and supported devices

This classification of device has a standard set of security solutions built in such as anti-malware, host-based firewall and vulnerability scanning mechanisms applied by IT Services before they are issued. Therefore, such devices are permitted to connect to and utilise the core network without significant restriction.

Limitations

- No existing device must be reconfigured, moved, or connected to an alternative physical network port without approval from IT Services.
- Where a static IP address is required, a formal service request must be raised with supporting business justification.

Cyber and information security requirements

All individuals using a device to connect to the Core BU network must...

- ✓ Have an active anti-malware solution enabled on the device configured to check for daily updates as a minimum
- ✓ Ensure the device has the latest security updates applied/installed
- ✓ Comply with the BU Acceptable Use Policy
- ✓ Only use IT approved remote access solutions
- ✓ Accept that any connecting device may be subject to security scanning
- ✓ Ensure the software firewall on the device is not bypassed or turned off
- ✓ Where unsupported server infrastructure is being introduced, these hosts must comply with Information Security policies and technical standards.

All individuals using a device to connect to the BU network must not...

- χ Connect a device that does not have the latest security updates applied/installed
- χ Knowingly connect a device to a BU network if there is evidence or suspicion that the device may be infected with malware
- χ Use hacking, enumeration or packet capture tools unless approved or supplied by IT Services.
- χ Add too or alter existing network infrastructure
- χ Joining two or more separate networks so they can share information, bypassing any restrictions or security measures in place
- χ Introduce or use any unauthorised VPN or remote access solutions that allow internet originating remote
- χ Connect any “unknown” device such a device that has been found to any BU owned network
- χ Change or render inoperative any pre-existing security solutions or network configurations
- χ Remove any device from the network or move a device to another location or network port unless specifically approved by IT Services
- χ Circumvent or utilise unapproved non university Domian Name Services (DNS) or registries (connection of a device to a BU network will not allow unintended connections to malicious destinations, you must not override this automatic DNS setting).

Security monitoring and threat response measures

- By connecting a device to a BU network, you accept that the device may be scanned and assessed by BU’s security solutions. This is to ensure devices have an antivirus solution installed which is up to date and has the latest operating system security patches applied. these measures may also be applied to ensure devices connecting to the network comply with the controls outlined here in and or in accordance with BU policies and standards.
- A device may be removed from the network without notice if an immediate security threat is identified or suspected.