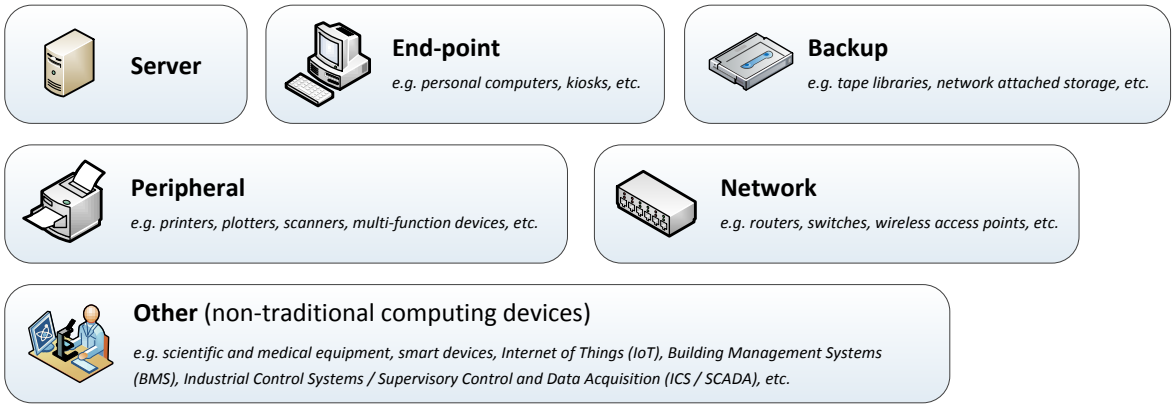
# Code of Connection Overview and Check List

## What is the Code of Connection?

The Code of Connection provides guidance on how to protect the following types of devices if they are connected to the University's network:




If a device is not kept secure, then it may be possible for an attacker to take control of that device, attack other devices on the network, and access protected information. We (Newcastle University's IT Service) will disconnect a device from the network if we believe it poses a risk to ICT security.

## Who is the Code of Connection aimed at?

The Code of Connection is for everyone who installs, manages or maintains ICT equipment connected to Newcastle University's ICT network. This includes central and local ICT support, administrative and academic staff, and students who are involved in these activities.

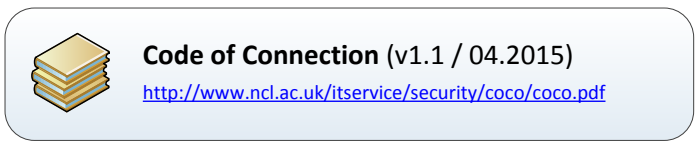
## Does the Code of Connection cover BYOD (Bring Your Own Device?)

No. The Code of Connection does not cover BYOD or encryption for mobile devices. You can access separate guidance on BYOD and mobile device encryption at the following location:


Remember - confidential and sensitive information must be encrypted if stored on a portable computing device or portable storage device.

## Where can I download the full Code of Connection?

You can download the full Code of Connection from the following location:




## What if I have problems with understanding and complying with the Code of Connection?

If this is the case then you need to contact the Information Security Team for further advice. We can be contacted through the IT Service Desk by telephone **(0191 208) 5999** and by email at **it.servicedesk@ncl.ac.uk**

# Code of Connection Overview and Check List

## Check List

Please use this check list to assess the security of the devices that you are responsible for.

For more information on each high-level requirement, please refer to the relevant section of the full Code of Connection that is referenced through the CoCo Security Controls.

| Ref | High-Level Requirement | CoCo Security Controls | Compliant? | | |
|---|---|---|---|---|---|
| | | | Y | N | N/A |
| 1.0 | Have you correctly registered your devices in the Network Inventory? | 1.1, 1.2, 1.3 | | | |
| 2.0 | Have you provided us with a valid business reason for allowing your device to be accessed over the internet? | 2.1 | | | |
| 3.0 | Have you disconnected devices from the network that are no longer needed? | 3.1 | | | |
| 4.0 | Are you able to fix security vulnerabilities within 5 working days of being notified? | 4.1, 4.2 | | | |
| 5.0 | Have you installed anti-malware software on all devices that are vulnerable to malicious software; such as viruses, worms, bots, Trojans, adware, spyware, ransomware and scareware? | 5.1 | | | |
| 6.0 | Are your devices still in receipt of vendor security updates and are the latest security updates installed? | 6.1, 6.2 | | | |
| 7.0 | Have you turned off all unnecessary and non-secure network services and are all other services running with non-administrative privileges? | 7.1, 7.2 | | | |
| 8.0 | If software firewalls are available, are they securely configured and running on all devices that are accessed over the Internet? | 8.1 | | | |
| 9.0 | Are your devices running secure access controls? | 9.1, 9.2, 9.3, 9.4, 9.5, 9.6, 9.7, 9.8 | | | |
| 10.0 | Are your devices hardened in accordance with vendor recommendations? | 10.1 | | | |
| 11.0 | Have you reduced the amount of technical information that is publicly advertised by your devices? | 11.1 | | | |
| 12.0 | Are you using only software that has been obtained from a trusted source? | 12.1 | | | |
| 13.0 | Do you check security settings for misconfigurations after system changes and at least annually if no changes have been made? | 13.1 | | | |
| 14.0 | Have you secured your web applications? | 14.1, 14.2, 14.3, 14.4 | | | |
| 15.0 | If you collect, store or process other people's personal information, is that information kept secure in compliance with the Data Protection Act? | 15.1, 15.2 | | | |
| 16.0 | Are you using only secure wireless access points? | 16.1 | | | |
| 17.0 | If system and/or application logging is available, is it enabled and are logs kept for at least three months, or as required? | 17.1 | | | |
| 18.0 | Will you report all suspected information security incidents to the IT Service Desk?<br><br>Tel: **(0191 208) 5999** Email: **it.servicedesk@ncl.ac.uk** | 18.1 | | | |