Edinburgh Napier University - Electronic Information Security Policy

Bring Your Own Device Policy

1.0 Introduction

Information Services Network and Security Services team identified early in the BYOD hype cycle that a critical enabling feature was the implementation of pervasive accessible Wi-Fi. The Team having successfully delivered an ever-improving Wi-Fi network simplified network access removing older implementations of 'NapAir' and standardising on the sector wide Eduroam service. An 'active' user portal enabled users to register and access the Wi-Fi service with-out the need for IT intervention, demonstrating Information Services move toward delivering IT as a Service.

Highly available robust Wi-Fi services represents excellent customer service that supports the myriad of devices our staff and students routinely use to engage for learning, work and socially. The consumerisation of IT has seen many large-scale applications broken down into streamlined, simple to use 'App's that deliver service in an attractive user focused on demand format. The University therefore wishes to encourage widespread adoption of user led services regardless of device, location or time.

This policy therefore actively encourages the use of user owned devices tablets, hybrid tablets, smart phones and devices, and commits to the widening of access and the development of IT as a Service.

2.0 Scope

This policy is intended to address the use in the workplace by staff and students of non-University owned electronic devices such as smart phones, tablets and other such devices to access and store University information, as well as their own. This is commonly known as 'bring your own device' or BYOD.

Using mobile and hybrid tablet and smartphone devices safely, requires all users to adhere to all aspects of the Information Security Policies. User owned devices are no exception and connecting, using or accessing University electronic systems, services and information commits, You, the user to the policies and playing your part in securing the University. All devices accessing University Wi-Fi must register with Information Services and adhere to the mobile computing policy. To ensure you are compliant with University policies you should ensure the following.

As data controller Edinburgh Napier must remain in control of the personal data for which it is responsible, regardless of the ownership of the device used to carry out the processing. As an employee you are required to keep secure University information and data. This applies equally to information held on the University systems and to information held on an employee's own device.

As an employee you are required to assist and support the University in carrying out its legal and operational obligations with regard to University data and information stored on your device. You

are required to co-operate with officers of the University when they consider it necessary to access or inspect University data stored on your device.

The University reserves the right to refuse to allow access to particular devices or software where it considers that there is a security or other risk to its systems and infrastructure.

- University information, identity details such as usernames and password and any information classed as confidential should not be saved or synchronised to third party storage providers. This includes,
    - Research data
    - Personal data belonging to you or other members of the University
    - Note that many commercially funded research projects expressly forbid the storage of research data on unsecured third-party storage and
    - Where that data may be stored in countries out with the reach of European law
- Your device should be registered with 'locate me' style services
- Your device should be registered with a recognised supplier or Information Services for device wipe functionality
- Device lock code should always be in place and where available a complex password implemented that has a combination of letters and numbers. See University password policy
- Your devices should automatically lock on a maximum of 30 minutes non-use device lock on idle
- In all instances where University confidential data may be stored on your device encryption software must be used and appropriate authentication and password access in place.

2.1 Mobile Device Management

The University will shortly implement a Mobile Device Management service and all University owned or supplied devices must be registered with this service. Users who own their devices are encouraged to register with the service to receive its many benefits. However, should you not wish to do so users who access the University electronic, systems and services are bound by this policy and all related information security policies.

2.2 Informing the University of the loss or theft of your device

In order to protect you and the University should you lose your device you must immediately inform Information Services via its Helpdesk on extension 3000 or by emailing ISServiceDesk@napier.ac.uk, informing the University of any potential data or user identity loss and whether you have contacted the authorities.

In the event of a loss or theft, you should change the password to all University services accessed from the devices (and it is recommended this is done for any other services that have been accessed via that device, e.g. social networking sites, online banks, online shops.

2.3 The University Virtual Desktop Service.

To access University electronic systems, services and data the University provides a Virtual Desktop Service. This service provides secure access to these systems and services, delivers access to complex systems and software services and computing power associated with PC's or workstations on a wide range of simple tablet or smart devices. This is particularly useful for those devices not running standard business software and applications.

2.4 Monitoring & Logging

The University will not monitor the content of user owned devices for threats to the technical infrastructure of the Institution. However, the University reserves the right to prevent access to the University network by any device that is considered a risk to the network.

In exceptional circumstances the University will require to access University owned data and information stored on your personal device. In those circumstances every effort will be made to ensure that the University does not access the private information of the individual. University data and information can only be stored and processed on personally owned devices under acceptance of these conditions.
You should note the separate University Monitoring & Logging Policy which regulates the monitoring of devices used by staff and students for work and learning purposes.

If certain secure or confidential categories of data and information are required to be accessed or stored on your own device then Edinburgh Napier University would be obliged to monitor the device at a level that may harm your privacy and that of anyone you lend your device to. You should consult with the senior responsible officer for Information Security when secure or confidential categories of data are to be handled in this way.

3.5 Compliance with data protection

The University is committed, as a data controller, to treating all personal data fairly and lawfully in line with the Data Protection Act 1998 (DPA). This includes the requirement to keep personal data up-to-date, and to handle it securely and to keep it for no longer than is necessary.

As an employee you are required to comply with the University Data Protection Policy and requirements. Your personal responsibility is expected to align with these University obligations.

Your attention is drawn to the separate Edinburgh Napier Data Protection Policy which requires you as an individual to process data in compliance with all aspects of the DPA and this applies equally to processing of data which takes place in the context of BYOD.

As an employee, researcher or student you have a responsibility to ensure that data is stored, transferred, handled and destroyed in accordance with the University Information Security policies for information originating from your own device. Further you are also required to assist the university in complying with subject access and Freedom of Information requests for information and you may be required to search your device and to provide the information requested to the University.

3.6 Support for BYOD

The University intends to support all devices however this may not always be possible and the IS Service Desk should be contacted in the first instance for device advice and help.

Information Services take no responsibility for supporting user owned devices but are committed to assisting users connect their devices to University Wi-Fi systems and services. The IS Service Desk will further support users in implementing Virtual Desktop and VPN services where applicable and will assist with securing your device.