STAFF RELATED POLICY: ACCESS TO GUEST WIFI USING NON-COLLEGE OWNED DEVICES

This policy is biannually reviewed to ensure compliance with current regulations

Approved/reviewed by	
Director of Business Services	
Date of next review	February 2022

This policy and procedure is subject to The Equality Act 2010 which recognises the following categories of individual as Protected Characteristics: Age, Gender Reassignment, Marriage and Civil Partnership, Pregnancy and Maternity, Race, Religion and Belief, Sex (gender), Sexual orientation, Disability, Socio-Economic Disadvantage

1. Introduction

The aim of this policy is to address the use in College by staff of non-college owned devices, outline the terms, conditions and implications of use and to help mitigate the data security risks associated with this.

This policy is intended to address the use in the workplace by staff of non-college owned electronic devices such as smart phones, tablets and other such devices to access the internet and web based resources.

It is the policy of Boston College to place as few technical restrictions as possible on the development and use of new applications and services. However the use of non-college owned devices to access the internet creates issues that need to be addressed particularly in respect of e-safety and data security.

As data controller Boston College must remain in control of personal data for which it is responsible, regardless of the ownership of the device used to carry out any processing. College information and data must be kept secure - please refer to Data Protection and Data Security Policies.

Employees of the College are required to assist and support the College in carrying out its legal and operational obligations with regard to College data and internet use, co-operating with officers of the College if it is necessary to access or inspect an individual's device that may have been used to access College information.

Employees are advised where ever possible not to use their own devices to access the college network and process College data and information. The College 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.

2. Security of Systems and Technical Infrastructure

The College takes security very seriously and invests significant resources to protect data and information in its care. The College is contractually required to comply with the Janet Security Policy, to protect the security of Janet and of its own internal networks.

Where employees use their own devices as a work tool to access internet services, they are expected to be mindful of maintaining the security of the College network and any information that is transferred between the personal device and the College system. Refer to Data Protection and Data Security Policies.

Where a staff member uses their own device to access internet services it is their responsibility to familiarise themselves with the device sufficiently in order to keep themselves and any data processed secure.

In practice this means: -

- preventing theft and loss of data
- keeping information confidential
- maintaining the integrity of data and information
- deleting sensitive or commercial emails once actioned
- deleting copies of attachments to emails such as spread sheets and data sets on mobile devices as soon as actioned
- limiting the number of emails and other information that are synced to own device

In the event of a loss or theft of a device, staff members should change their password to any college service accessed from that devices. 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.

In the event of loss or theft of a device you should report the matter promptly to the ICT Manager to enable access to College systems by a device or user to be revoked if possible.

Certain data should never be stored on a personal device, this includes personal data and data that is covered under the Data Protection Act. Any College data that is kept must be stored with the appropriate level of security. If there are any doubts as to the level of security that should be attached to particular data please refer to the appropriate manager, ICT Manager, HR, Funding and Registry Manager.

Failure to comply with this policy could be considered a disciplinary offence.

3. Security and e-Safety of Staff IT Users

Boston College is committed to providing a safe environment for learners and staff including the online environment.

College staff are required to play their part in maintaining a safe working environment and in terms of College provided internet services this means keeping software up to date and avoiding content that threatens the integrity and security of their own device, the College systems and the devices of learners and others. This includes ensuring that the device automatically locks if inactive for a period of time.

The College Social Media Policy provides standards expected on appropriate online behaviour between staff and learners. It is particularly important to maintain a distinction between personal content and work related content especially where interaction takes place between individuals (staff and learners) and where images and content are shared and published.

4. Monitoring of User Owned Devices

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

In exceptional circumstances the College may require access to information stored on personal devices where breaches to College data occur or under Freedom of Information requests. In those circumstances every effort will be made to ensure that the College does not access the private information of the individual. It is advised therefore that College data and information should not be stored and processed on personally owned devices.

5. Compliance with Data Protection Obligations

The College is committed, as 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

College staff are required to comply with the College data protection policy and requirements. Please refer to the Data Protection and Data Security Policies.

6. Acceptable Use of User Owned Devices

The College requires that staff conduct their online activities appropriately and in compliance with the terms of the Acceptable Use Policy (AUP) through the Joint Academic Network (JANET).

Failure to comply with the Acceptable Use Policy could be considered a disciplinary matter.

7. Support

The College takes no responsibility for supporting staff owned devices.

8. Theft, loss, damage and fees

The College is not liable or responsible for any theft, damage or loss for any staff or learner owned devices or for the personal information on any such device. It is the responsibility of the owner of the device to ensure that the device is safe and secure.

The College is not responsible for any fees associated with using any personal technology devices. All fees and charges related to texting or internet use on any staff or learner owned device remains the sole responsibility of the owner.

9. Incidents and Response

Where a security incident, involving staff using their own devices, arises at the College this matter will be dealt with very seriously. The College will act immediately to prevent, as far as reasonably possible, any harm or further harm occurring. The ICT Manager will review what has happened and decide on the

most appropriate and proportionate course of action. Sanctions may be put in place, external agencies may be involved or the matter may be resolved internally depending on the seriousness of the incident. This is in line with the College Data Security Policies and the Janet Acceptable Use Policy. Serious incidents will be dealt with by senior management, in consultation with appropriate external agencies if necessary.

10. 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 College's disciplinary policy.

EQUALITY IMPACT ASSESSMENT

1. What is the name of the policy?

Staff Related: Access to WiFi – using non-College owned devices.

2. What is the aim of the policy?

To address the use in College by staff of non-college owned devices and to mitigate the data security risks associated with this.

3. Who does the policy impact on? (Staff, learners, partners etc.)

College staff – academic and non-academic, learners and visitors to the College.

4. Who implements the policy?

IT Manager/CSU Manager, HR Managers, Registry Manager, ILT Team for training and development.

5. What information is currently available on the impact of this policy?
(This could include data that is routinely collected for this policy and/or minutes from management or team meetings. It could also include conversations with students and/or staff who have used this policy in their day to day role).

None within the college however case studies and information from the educational community supports the use and development of ILT within teaching and learning – opening up the use of WiFi and widening access to individuals is seen to support TL&A.

6. Do you need more information before you can make an assessment about this policy?
(If yes, please put down what information you need and identify in the action plan, how you intend to collect it)
No

7. Do you have any examples that show this policy is having a positive impact on any of the equality characteristics shown in Table.1?

The opening up of College WiFi should have a positive impact on teaching, learning and assessment regardless of equality characteristic – in some cases it could even support and enhance delivery methods and techniques to support individuals within the protected characteristics..

8. Are there any concerns that this policy could have a negative impact on any of the equality characteristics shown in Table.1?

Table. 1

Category	No	Yes	Please supply any additional comments
Race	✓		
Disability	✓	✓	In most cases the increased use of ILT should support learners and staff with disabilities however training and awareness of applications/devices should always consider accessibility.
Gender	✓		
Gender re-assignment	✓		
Age	✓		
Sexual orientation	✓		
Religion/belief	✓		
Pregnancy/maternity	✓		
Marriage/Civil Partnership	✓		
Socio-economic		✓	As the College are within an area of high levels of deprivation access to learners/staff having their own device may result in the positive outcomes for TL&A being reduced.
Rurality	✓		

Actions are to be taken as a result of the Equality Impact Assessment			
Action Required (clearly state where within existing management structures these actions will be performance monitored)	Person responsible	Comp date	Review details - impact and outcome
To monitor and review impact or issues relating to the widening use of non-college owned devices	P Macpherson/Julie Hebdige	January 2016	No significant negative effect on network services by the implementation of guest wireless.
Signed:	**Position:**	**Date:** 22 September 2015	
		Date EIA reviewed: October 2017	