1. Introduction

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 toerop 72 8i9-8a)-3ti)8cu)-3ar)11l 2 8riort na58n1

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.

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 ser

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