IT Systems Acceptable Use Policy

B&FC
BLACKPOOL AND THE FYLDE COLLEGE

IT Systems Acceptable Use Policy

Date approved:	17/05/2019
Approved by:	SMT
Responsible Manager (s):	Head of IT
Executive Lead:	Chief Operating Officer

Applicable to Students:	Yes / ~~No~~ *
Accessible to Students:	Yes / ~~No~~ *
Accessible to general public: (including clients)	Yes / ~~No~~ *

Consultation

Consultation undertaken with:		Date:
• SMT	Yes / ~~No / NA~~ *	……17/05/19
• AMT	Yes / ~~No / NA~~ *	14/03/19
• CCMT	Yes / ~~No / NA~~ *	20/02/19
• Students	Yes / ~~No / NA~~ *	10/05/19
• Employee representatives ***(HR policies only)***	~~Yes / No /~~ NA *	……
• Other	~~Yes / No /~~ NA *	……

**** please delete as appropriate***

Policy review frequency, normally: Once every three years

CONTENTS **PAGE**

1. Scope and Purpose of the Policy

This policy applies to users (employees, students and third parties) who are authorised by B&FC to access its IT systems* and data.

The purpose of this policy and associated agreement is to ensure that users are aware of what constitutes acceptable use of IT systems and data so that the risks (both security and reputational) to B&FC through the mis-use of IT systems* and data is minimised.

* For the purpose of this policy, 'IT systems' includes, but is not limited to telephone systems (landlines and mobiles), fax devices, print/copier devices, personal computers (PCs, desktop, laptops, hybrid devices), tablets, terminals, email, the Internet, any locally installed software, and any internet based software accessible from within B&FC's network.

2. Policy Statement

IT systems and data provide the backbone on which B&FC provides an excellent learning and working environment. This policy and associated agreement is part of a set of risk management controls that B&FC puts in place so that users can rely on the availability and security of those systems.

"Acceptable use" is defined in detail within the Acceptable Use Agreement. In summary, a user should not perform any activity using B&FC IT systems and data that is illegal, inappropriate or that would result in risk of, or actual damage to, B&FC IT systems and data or to B&FC's reputation. Where conduct by a user is considered illegal, the matter will be reported to the police.

3. Accountability

3.1 The Head of Information Technology is responsible for:

- Ensuring that the policy is implemented, regularly reviewed and updated.
- Ensuring that IT systems, networks and applications are available to agreed service levels.
- Ensuring that this policy and associated agreement are readily available
- Supporting the investigations into incidents where the Acceptable Use Agreement may have been breached.
- Ensuring that measures are in place to restrict one's ability to breach the acceptable use agreement.

3.2 Users are responsible for:

- Adhering to the terms of this policy and the associated acceptable use agreement.
- Reporting known or suspected breaches of the acceptable use policy.

4. Student Involvement

4.1 Students will be made aware of the Acceptable Use Policy and associated agreement via induction and are available to view through the virtual learning environment (VLE).

5. Linked Policies

None

6. Linked Procedures

Acceptable Use Agreement
Professional Boundaries

7. Equality Impact Assessment attached

Equality Impact Assessment

Impact Assessment for IT Security Policy	
Initial Form to be completed with Risk Assessments or as part of a proposal or change to a policy, plan or new way of working	
Title of Activity: Policy draft, as no equivalent exists. Author Head of IT Date: May 2019	☒ New or ☐ Revision Please tick as appropriate Expected Implementation Date: May 2019 What is the review date? May 2022
Equality and Diversity. Which of the characteristics maybe impacted upon? And, if yes, how has this been considered? What are the risks? What are the benefits?	None N/A N/A
Safeguarding: Are there any aspects of this proposal which could cause a learner/member of staff/visitor to feel unsafe? If yes, how has this been considered? What are the risks? What are the benefits?	☐ Yes ☒ No
Health and Safety: Have any risks been identified? If yes, how has this been considered? What are the risks? What are the benefits?	☐ Yes ☒ No
Sustainability: Are there expected benefits or impacts on sustainability issues?	☐ Yes ☒ No

If yes, how have these been considered?	
Evidence: What evidence do you have for your conclusions and expectations for these conclusions? How will this impact be monitored for all these considerations?	
Is this policy of a high/medium or low risk? :	☐ High ☐ Medium ☒ Low

Full Assessment Screening (if required)

IT Systems Acceptable Use Policy

Date approved:	TBC
Approved by:	
Responsible Manager (s):	Head of IT
Executive Lead:	Chief Operating Officer

Applicable to Students:	Yes / ~~No~~ *
Accessible to Students:	Yes / ~~No~~ *
Accessible to general public: (including clients)	Yes / ~~No~~ *

Consultation

Consultation undertaken with:		Date:
• SMT	Yes / No / NA *	……
• AMT	Yes / No / NA *	14/03/19
• CCMT	Yes / No / NA *	20/02/19
• Students	~~Yes~~ / No / NA *	……
• Employee representatives ***(HR policies only)***	~~Yes / No / NA~~ *	……
• Other	~~Yes / No / NA~~ *	……

**** please delete as appropriate***

Policy review frequency, normally: annually.

CONTENTS **PAGE**

1. Scope and Purpose of the Policy

This policy applies to users (employees, students and third parties) who are authorised by B&FC to access its IT systems* and data.

The purpose of this policy and associated agreement is to ensure that users are aware of what constitutes acceptable use of IT systems and data so that the risks (both security and reputational) to B&FC through the mis-use of IT systems* and data is minimised.

* For the purpose of this policy, 'IT systems' includes, but is not limited to telephone systems (landlines and mobiles), fax devices, print/copier devices, personal computers (PCs, desktop, laptops, hybrid devices), tablets, terminals, email, the Internet, any locally installed software, and any internet based software accessible from within B&FC's network.

~~This Acceptable Use Policy forms part of the College's risk management controls and outlines the responsibilities of all who access IT systems at Blackpool and The Fylde College (B&FC).~~

~~1.1 For the purpose of this policy, 'IT systems' includes, but is not limited to telephone systems (landlines and mobiles), fax devices, print/copier devices, personal computers (PCs, desktop, laptops, hybrid devices), tablets, terminals, email, the Internet, any locally installed software, and any web-based software accessible within B&FC's network and beyond.~~

~~1.2 The Acceptable Use Policy and associated Agreement apply to staff, students and third parties (users) authorised by B&FC to access its systems or data.~~

~~1.3 The purpose of this policy is to inform users of IT systems that their use of IT systems is monitored and that there is a requirement that their usage will be within acceptable professional boundaries, with due respect to others and to be compliant with relevant legislation.~~

2. Policy Statement

~~2.1 IT systems are critical to the success of B&FC. B&FC is committed to ensuring the integrity, security and availability of IT systems required for its operation and compliance with relevant legislation, related policies and procedures.~~

~~2.2 IT systems and resources are made available to B&FC staff and students for use in relation to their work. Any such use of B&FC IT and information systems must be made with due respect to others at all times.~~

~~2.3 It is accepted and acknowledged that reasonable personal use of these systems and resources may be made outside of working periods, however~~

~~this use should not be to the detriment of others and shall abide by the terms outlined in the Acceptable Use Agreement.~~

IT systems and data provide the backbone on which B&FC provides an excellent learning and working environment. This policy and associated agreement is part of a set of risk management controls that B&FC puts in place so that users can rely on the availability and security of those systems.

"Acceptable use" is defined in detail within the Acceptable Use Agreement. In summary, a user should not perform any activity using B&FC IT systems and data that is illegal or that would result in risk of, or actual damage to, B&FC IT systems and data or to B&FC's reputation. Where conduct by a user is considered illegal, the matter will be reported to the police.

~~2.1 B&FC seeks to provide an excellent learning and working environment through the use of and access to IT systems.~~

~~2.2 B&FC is committed to ensuring the availability, integrity and security of IT systems.~~

~~2.3 B&FC requires that all users accessing B&FC IT Systems comply with relevant legislation and, related policies and procedures.~~

~~2.4 B&FC requires that usage of IT systems must be made with due respect to others at all times.~~

~~2.5 B&FC recognise that IT systems provided can be used for personal use outside of a persons working hours, however this use should not be to the detriment of others, bring B&FC into dis-repute and shall abide by the terms outlined in the Acceptable Use Agreement.~~

3. Accountability

3.1 The Head of Information Technology is responsible for:

- Ensuring that the policy is implemented, regularly reviewed and updated.
- Ensuring that IT systems, networks and applications are available to agreed service levels.
- Ensuring that this policy and associated agreement are readily available
- Supporting the investigations into incidents where the Acceptable Use Agreement may have been breached.
- Ensuring that measures are in place to restrict one's ability to breach the acceptable use agreement.

3.2 Employees are responsible for:

- Adhering to the terms of this policy and the associated acceptable use agreement
- Reporting known or suspected breaches of the acceptable use policy

3.3 Students are responsible for:

- Adhering to the terms of this policy and the associated acceptable use agreement
- Reporting known or suspected breaches of the acceptable use policy

~~3.4 Heads of Curriculum/Service are responsible for:~~

- ~~Ensuring that their team is aware of this policy.~~

~~3.5 The Head of Information Technology is responsible for:~~

- ~~Ensuring that IT systems, networks and applications are available when needed~~
- ~~Ensuring that this Policy and associated Framework are readily available~~
- ~~Ensuring that users of B&FC IT Systems comply with this Policy.~~
- ~~Investigating breaches of the Acceptable Use Policy~~
- ~~Ensuring that measures are in place to restrict one's ability to breach the Acceptable Use Policy~~

~~3.4 Where conduct by either staff, students or third parties is considered illegal, the matter will be reported to the police.~~

4. Student Involvement

4.1 Students will be made aware of the Acceptable Use Policy and associated agreement via induction and are available to view through the virtual learning environment (VLE).

5. Linked Policies

~~This policy links into other B&FC policies. These include:~~

~~5.1 Disciplinary Policy~~

None

6. Linked Procedures

Acceptable Use Agreement
Professional Boundaries

7. Equality Impact Assessment attached

Equality Impact Assessment

Impact Assessment for IT Security Policy	
Initial Form to be completed with Risk Assessments or as part of a proposal or change to a policy, plan or new way of working	
Title of Activity: Policy draft, as no equivalent exists. Author Head of IT Date: March 2019	☒ New or ☐ Revision Please tick as appropriate Expected Implementation Date: March 2019 What is the review date? March 2022
Equality and Diversity. Which of the characteristics maybe impacted upon? And, if yes, how has this been considered? What are the risks? What are the benefits?	None N/A N/A
Safeguarding: Are there any aspects of this proposal which could cause a learner/member of staff/visitor to feel unsafe? If yes, how has this been considered? What are the risks? What are the benefits?	☐ Yes ☒ No
Health and Safety: Have any risks been identified? If yes, how has this been considered? What are the risks? What are the benefits?	☐ Yes ☒ No
Sustainability: Are there expected benefits or impacts on sustainability issues?	☐ Yes ☒ No

If yes, how have these been considered?	
Evidence: What evidence do you have for your conclusions and expectations for these conclusions? How will this impact be monitored for all these considerations?	
Is this policy of a high/medium or low risk? :	☐ High ☐ Medium ☒ Low

Full Assessment Screening (if required)