Bedford College Academies Trust

IT Acceptable Use Policy

Status: Advisory	**Member of staff responsible:** Principal	**Implementation date:** **September 2017**
Issue No: 1A	**Approved by:** BCAT	**Next Review Date:** **June 2018**

Our Vision

“The BCAT vision is to support students to achieve their absolute best whatever their ability or background. We aim to:

1. Work collaboratively to deliver an inclusive and outstanding education to all students, thereby driving up local standards.
2. Maximise social mobility and life chances, through the highest expectations of and aspirations for all students.
3. Encourage and support a range of high performing and distinctive educational establishments for local communities.”

Our Values

Student focus - We will seek to achieve a high quality learning experience for every student

High performance - We will strive for consistently high levels of performance in all aspects of our work

Respect, openness and honesty - We will treat everyone with respect, encourage openness and honesty, and recognise each other’s contribution and achievements.

1. Introduction

Bedford College Academies Trust (BCAT) are committed to making full use of appropriate ICT resources and new technologies to make learning as exciting, interesting and relevant as possible.

It is acknowledged that with new technologies, such as the Internet, there are risks to students of accessing inappropriate content, receiving unwanted attention or being vulnerable to cyber bullying. The Trust believes it is our responsibility to educate students to ensure they are highly aware of the dangers in order to maximise the use of ICT safely.

For reference “user” refers to any authorised user or employee of the Trust.

2. When using ICT at an academy

IT hardware must be treated with care and used only in accordance with the proper operating instructions. No equipment shall be used which is labelled out of order. Any apparent fault with hardware should be reported promptly to IT Services Helpdesk. Equipment must not be used if there is reason to believe that it may not be in safe working order.

Users must not by any deliberate or careless act or omission jeopardise or seek to jeopardise the integrity of any IT equipment, and / or its software and / or any information stored within it and / or accessed through it.

Users must not access and / or attempt to access any IT equipment, software and / or data that they are not properly authorised to access. In particular, the confidentiality of data belonging to other users must be respected.

Users must take all necessary steps to protect and maintain the security of any equipment, software, data, storage area and / or passwords allocated for their use. Users must not access codes that belong to someone else; give out passwords to unauthorised persons; allow others access using their username or aid anyone in entering the system except by authorised means.

Users must not use any IT facility for a purpose other than that for which they are authorised. Users must seek advice if they have any doubt about their authority to use any of the IT facilities.

Users must comply with all their legal obligations affecting their use of IT facilities, including Contempt of Court, Copyright, Defamation, Computer Misuse Act, Data Protection Act, Official Secrets Act, Obscene Publications Act, Protection of Children Act and the Equality Act.

Users must take all reasonable steps to exclude and avoid the spread of malicious software, e.g. viruses, and must co-operate fully with all measures instituted by IT Services to prevent the spread of such software. In particular, users must not install or execute on a BCAT computer any software obtained from a third party source. Under the Computer Misuse Act 1990 it is an offence knowingly to corrupt a computer program or any of the data stored in the computer system.

Computer programs on IT facilities are protected by law of copyright. BCAT has the appropriate licences to use these programs. Users must comply with all their legal obligations concerning copyright, and must not copy any software or other data without the prior authorisation from the copyright owner. Such action would be in breach of copyright law.

User must not connect any unauthorised equipment to BCAT networks without consultation and the prior written approval of a senior member of the IT Services Department. If IT Services has reasonable grounds for believing that any equipment may be the cause of unacceptable degradation of the performance of the network detrimental to other users, then the user must co-operate with the disconnection of the equipment from the network pending resolution of the problem.

The use of any IT equipment for storage and/or transmission of materials which BCAT considers to be obscene and/or offensive are strictly prohibited.

3. When using the Internet

Users must be aware that the Trust cannot accept any responsibility for personally downloaded content or software.

Users must understand that under no circumstances should attempts be made to bypass the Internet filtering system, as it exists to safeguard both staff and students.

Users should understand that the use of the Trust information systems, Internet and email may be monitored and recorded to ensure policy compliance.

Users must not send staff or students personal information via the Internet without authorisation from their line manager.

Users must understand that when using social networking sites for personal use the user will not contact or communicate with students or parents.

Users must ensure that electronic communications with students including email, IM and social networking are compatible with the user professional role and that messages cannot be misunderstood or misinterpreted.

Users must promote e-safety with students in the user care and will help them to develop a responsible attitude to system use, communications and publishing.

Users must not use IT facilities to download pornographic, obscene, excessively violent and/or offensive materials from the Internet.

BCAT may exercise its right to monitor the use of academy information systems and Internet access, to intercept e-mail and to delete inappropriate materials where it believes unauthorised use of the academy's information system may be taking place, or the system may be used for criminal purposes or for storing unauthorised or unlawful text, imagery or sound.