The
Sixth Form
College
Birkenhead

IT Services

ICT Acceptable Use Policy (Overview)
Students
(Revised May 2014)

Introduction

The purpose of this document is to provide a brief overview to ensure that all Students (referred to as ‘users’) of Birkenhead Sixth Form College’s (referred to as ‘the College’) computing facilities are aware of the college’s policies relating to their use.

The College has a comprehensive ICT Acceptable Use Policy (BSFC – IT Services Full ICT Acceptable Use Policy) which is far more detailed than this document and users are required to be familiar with it. This is available on the IT Services website (http://itservices.bsfc.ac.uk).

The college encourages the use of computing (and other technologies) for the benefit of its users. The computing resources are provided to facilitate a student’s work, specifically for educational, training, administrative or research purposes.

In addition to the main ICT Acceptable use policy, the college also has a number of other policies that relate to the use of technology in the college;

BSFC – Bring Your Own Device (BYOD) Policy
BSFC – E-Safety Policy
BSFC – Social Media Policy
Janet Acceptable Use Policy (https://community.jisc.ac.uk/library/acceptable-use-policy)

Users are asked to familiarise themselves with the above policies.

1. <u>General Points</u>

1.1. The phrase ‘ICT Facilities’ as used in College policies are interpreted as including any computer hardware, printers, telephones, or software owned or operated by the College, including any allocation of memory/disk space on any of the College systems.

1.2. Users may only use those systems listed in 1.1.at the College or any of its centres if they have signed this Acceptable Use Policy.

1.3. The College has the right to monitor any and all aspects of its computer and telephone system that are made available to users and to monitor and/or document any communications made by users, including those by telephone, email and other internet communication. The college also wishes to make users aware that Closed Circuit (CCTV) cameras are in operation for the protection of our users and assets.

1.4. Computers and email accounts are the property of the College and are designed to assist in the performance of your studies. You should, therefore, have no expectation of privacy in any communications sent or received, whether it is of a college or personal nature.

2. User Account Security

2.1. In order to use the ICT facilities of the College a person must first be provided with their own user name by IT services. Registration to use the computer facilities implies, and is conditional upon, acceptance of this Acceptable Use Policy.

2.2. All individually allocated usernames and passwords are for the exclusive use of the individual to whom they are allocated. Passwords protect the College's systems from access by unauthorised people; they protect your work and the College's information. The user is personally responsible and accountable for all activities carried out under their username.

2.3. The password associated with a particular personal username must not be divulged to another person. Attempts to access, or use, any username or other data, which is not authorised to the user are prohibited.

3. Use of E-Mail, Internet & Social Media

3.1. The College's email system is provided to aid users with their studies. Personal use of the email system is permitted, but the account is only valid whilst you are a student at the college.

3.2. All use of the Internet can be tracked and users should be aware that all sites accessed are automatically recorded. It is important to note that if you connect your device to our Wireless BYOD (Bring Your Own Device) system then again all traffic is monitored and logged.

3.3. Extensive filtering and firewalls are in place to protect our users, in addition users should not attempt to download, transmit or store any material that might reasonably be considered to be obscene, abusive, sexist, racist or defamatory.

3.4. Copyright and licensing conditions must be observed when downloading from the internet.

3.5. Social media is not anonymous, and the internet remembers everything. Postings of all types can typically be traced back to their authors, and information posted through social media is backed up, stored, replicated, linked and reposted continuously.

3.6. Inappropriate or inaccurate comments which are damaging to a person's reputation should be avoided. Bullying remains bullying even if it is not conducted in a public sphere. The same is true for cyber-bullying. Think carefully about posting anything which you would not want a third party such as a future employer, institution or professional body to read.

4. Security & Anti-Virus

4.1. Anti-virus software is loaded on all computers as standard and is updated regularly via the network. There are security protocols in place to prevent users from attempting to remove or de-active the Anti-Virus software, so please do not attempt to do so.

4.2. If you suspect that a virus has infected a computer then stop using the computer and contact IT Services immediately. As soon as a Virus is detected on a device (including external media such as a USB drive), IT Services are immediately emailed (and an automatic clean-up is attempted).

5. Implementation & Updates of the Policy

5.1. The Head of IT Services is responsible for the management of all College ICT systems. The IT Services department are available to give advice on the practical implications of this policy.

5.2. Training is available to familiarise students with the College ICT system and its uses.

5.3. In the light of changes in the business, technology, legislation or relevant standards it may be necessary to update this policy from time to time. Notification to all users will be made when updates are available.