IT Services

ICT Acceptable Use Policy (Overview)
Staff and Temporary Staff
(Revised May 2014)

Introduction

The purpose of this document is to provide a brief overview to ensure that all Staff (including contractors, secondments, visitors etc. - 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 person's work as a user of the college, 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. General Points

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.

2. User Account Security & Data Protection

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. Staff users will be created upon receipt of a New User request from the HR Department.

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, except to trusted members of IT services. (The member of IT services will then show you how to re-set your password so that they no longer know it.) Attempts to access, or use, any username, which is not authorised to the user are prohibited.

2.4. You must only access information held on the College's computer systems if you have been properly authorised to do so and you need the information to carry out your work.

2.5. It is college policy to store data on a network drive where it is regularly backed up. Valued documents and files should not be stored on Desktop PCs or laptops. Files stored on Desktop PCs are at risk of loss through hardware/software failure or automated administrative activity

2.6. The College maintains a notification with the Information Commissioner's Office in compliance with the Data Protection Act 1998. It is the responsibility of all College staff to ensure that personal data held and processed is within the terms of the College's data protection policy.

2.7. Under no circumstances should you disclose personal or other confidential information held on computer to unauthorised persons. The unauthorised access to and/or unauthorised modification of data is a criminal offence under the Computers' Misuse Act 1990.

3. Use of E-Mail, Internet & Telephone Services

3.1. The College's electronic mail system is provided for the College's business purposes and academic support. Limited personal use of the email system is permitted, but not to a level that would influence the primary business purpose.

3.2. Email messages must be treated like any other formal written communication. Improper statements in email can give rise to personal liability and liability for the College and can constitute a serious disciplinary matter. Email messages to or from you cannot be considered to be private or confidential.

3.3. Reasonable private use of the Internet is permitted but should be kept to a minimum and should not interfere with your work. Excessive private accessing of the Internet during working hours may lead to disciplinary action.

3.4. All Internet usage from the College network is monitored and logged. Reporting on aggregate usage is performed on a regular basis. When specific circumstances of abuse warrant it, individual web sessions will be investigated and linked to the relevant user account. Such an investigation may result in action via the College's Disciplinary Procedure and possibly criminal investigation.

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

3.6. The College appreciates that there may be occasions where employees need to use the College telephone system during working hours. Reasonable use of the College telephone system for private use is permitted but this should not interfere with your work.

3.7. Telephone conversation are not monitored (but can be via call recording software built into the phone system). A comprehensive call logging system is in place to record all incoming and outgoing numbers. The Senior Management reserve the right to monitor and investigate the use of the College telephone system, including any numbers dialled.

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. Non-College software or data files intended to be run on college equipment by external people such as engineers or trainers must be checked for viruses before use. 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 an external device (such as a USB), IT Services are immediately emailed (and an automatic clean-up is attempted).

4.3. Files received by or sent by e-mail are checked for viruses automatically.

4.4. Remote users are responsible for maintaining up to date virus definitions on their own computers and can contact IT Services for help as required.

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

5. Social Media

5.1. Users are strongly advised that they should:

- Be highly circumspect about the information that is posted in public view; criticising the College, colleagues and students will be considered a serious disciplinary offence
- ensure that there is restricted access to their individual sites
- ensure that they do not invite students to be a 'friend' or visit their site

5.2. Think carefully about posting anything which you would not want a third party such as a future employer, institution or professional body to read.

6. Implementation & Updates of the Policy

6.1. 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.

6.2. Training is available to familiarise employees with the College ICT system and its uses.

6.3. 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.

Further Information
The following documents relate to this Policy;

BSFC – IT Services Full ICT Acceptable Use Policy
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)