huish | POLICIES

Author | Richard Anderson
Contributors | SMT
Version | 4.0
Publication Date | 10/12/2015
Last Review Date | 01/11/2019
Next Review Date | 01/11/2022

Acceptable Use Policy

CONTENTS

1. AIMS

1.1 To ensure security of College IT Systems.

1.2 To safeguard Richard Huish College's reputation.

1.3 To inform all users (staff and users) of all relevant legislation relating to IT.

1.4 To provide an appropriate teaching and learning environment for all College IT Users.

1.5 To safeguard and protect users of the College IT Systems.

1.6 To ensure all users of College IT Systems are aware of the Terms and Conditions laid down by JISC (Joint Information Systems Committee).

2. GENERAL COMPUTER USAGE

2.1 Your ability to connect to other computer systems through the network does not imply a right to connect to those systems or to make use of those systems unless authorised to do so. You should not alter or copy a file belonging to another user without first obtaining permission from the creator of the file.

2.2 For reasons of network security you are not permitted to download/import/install any application/program which has not previously been approved of by the IT Services team. Attempting such actions may lead to disciplinary action.

2.3 You are not permitted to play computer games both run locally or from the Internet, as this wastes computer time and generally causes a disturbance. Attempting such actions may lead to disciplinary action.

2.4 You are responsible for the security of any data that you take offsite. This could be on a mobile device, external storage device or cloud service platform. Further information is available in the Information Security Policy, Mobile Device Policy and at the IT Helpdesk.

2.5 There shall be no expectation of privacy when using College owned devices and services. Accordingly, users shall not have an expectation of privacy in anything that they create, place on, store, send, or receive on any College owned devices and services.

3. PASSWORDS

3.1 You are responsible for safeguarding your network or email accounts and associated passwords. Never allow anyone else to know your password or allow them to use your accounts at any time. User password rights given to users should not give rise to an expectation of privacy.

3.2 For reasons of security, when changing your password please follow the guidance below.

- Avoid choosing obvious passwords, such as those based on easily-discoverable information like the name of a pet or family member.
- Do not use common passwords such as, password, password1, p@55w0rd.
- Do not use the same password anywhere else, such as personal accounts like social media accounts or online shopping.
- Your password should not be printed, stored online or given to others.
- Avoid using a similar password to a previous one e.g. adding a ! or number on the end.
- Avoid using simple sequences such as 123 or abc.
- Try to use either completely random characters or long word phrases such as jydi834CSi0 or ilikeshopping.

4. MONITORING AND INTERCEPTION OF DATA

4.1 The College reserves the right to monitor the usage of all College IT facilities in order to:

- ensure the security of its systems and compliance to this policy
- to safeguard those systems from virus infection and spam invasion.
- to monitor and prevent access to inappropriate internet sites in order to provide as secure an environment for users as possible.
- to ensure compliance with the JANET (Joint Academic Network) AUP and Security Policies

4.2 College telephone and computer equipment, applications and services, email and the Internet are provided primarily for work related purposes. No users may use College telephone equipment without prior approval from a member of staff.

4.3 The College has the right to monitor any and all aspects of its telephone and computer systems and networks that are made available to users and to monitor, intercept and/or record any communications made by users, including but not just restricted to telephones, e-mail or Internet communications. This also includes decrypting and inspecting HTTPS data. To ensure compliance with this policy or for any other purpose authorised under the Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000, users expressly consent to the College doing so by agreeing to this policy. In addition, it should be noted that every time a user logs on they are agreeing to this policy.

4.4 Close Circuit Television (CCTV) is in operation on the College site for the protection of employees, users and College property. Images are automatically deleted a short period after recording, unless they have been manually saved due to the recording of an incident in progress.

4.5 Computer and telephone networks and user's network and e-mail accounts are the property of the College and are designed to assist in the performance of their work. Users should, therefore, have no expectation of privacy in any communication sent or received, whether it is of a business or personal nature. The IT Services department ensures the automatic monitoring of web and email traffic is working correctly and efficiently. Manual checking of quarantined email and logs is carried out authorised staff.

4.6 It is an inappropriate use of e-mail, the Internet or the network for users to access, download or transmit any material which might reasonably be considered to be unacceptable i.e. obscene, abusive, sexist, racist or defamatory. You should be aware that such material may also be contained in jokes sent by e-mail. Such misuse of electronic systems will be regarded as a disciplinary matter. Inappropriate material also includes chat, chain mail or global mailings unless for academic purposes.

4.7 The College reserves the right to use the content of any user's e-mail in any disciplinary process.

5. USE OF THE INTERNET

5.1 The College's Internet access is provided by JISC. They operate the Joint Academic Network (JANET).

5.2 JANET requires The College to agree to abide by and adhere to various terms and conditions when using the service. Details of which can be found at www.ja.net

5.3 This AUP applies to all users of College computer facilities, i.e., all staff (academic, support and other), students, and any other visitors.

5.4 The sites accessed by you must comply with the restrictions set out in these guidelines. You must not access or attempt to access unsuitable or inappropriate sites by searching. Accessing inappropriate sites may lead to disciplinary action.

5.5 The College reserves the right to filter all Internet content electronically to ensure it meets the requirements of this policy. Whilst every effort is made to remove such content, it is not technically possible to ensure that such filtering will stop 100% of such content.

6. USE OF E-MAIL

6.1 E-mails should be drafted with care. Due to the informal nature of these forms of communication, it is easy to forget that it is a permanent form of written communication and that material can be recovered even when it is deleted from your computer.

6.2 Users should not make derogatory remarks in e-mails about employees, users or any other person. Any written derogatory remark may constitute libel.

6.3 By sending e-mails on the College's system, you are consenting to the processing of any personal data contained in that e-mail and are explicitly consenting to the processing of any sensitive personal data contained in that e-mail. If you do not wish the College to process such data you should communicate it by other means.

6.4 Any emails sent outside the College are accompanied by the College's standard user notice.

7. COPYRIGHT AND DOWNLOADING

7.1 Copyright applies to all text, pictures, video and sound, including those sent by e-mail or on the Internet. Files containing such copyright protected material may be downloaded, but not printed, forwarded or transmitted to third parties without the permission of the author of the material or an acknowledgement of the original source of the material, as appropriate.

7.2 Software or Internet applications must never be downloaded without the agreement of the Head of Information Technology as it may break copyright agreements and could pose a serious risk to network security.

7.3 Users should note that all files or emails are scanned electronically for viruses, SPAM and other unwanted content. These files may be opened and interrogated should a virus or suspicious content be found.

8. LEGAL

8.1 The use of the College computer and telephone network and systems are covered by UK National legislation, including:

- **Data Protection Act 2018**
  Computer facilities shall not be used to hold or process personal data except in accordance with the provisions of the Data Protection Act 2018. Most processing of personal data is subject to the General Data Protection Regulations (GDPR). Any person wishing to use facilities for such a purpose are required to inform the Head of Information Technology and Head of College Information Systems & Exams in advance and comply with any restrictions that the College or the UK Data Protection Commissioner may impose concerning the manner in which data may be held or processed.

- **Copyright Designs & Patents Act**
  Copyright is infringed if a person acquires an unauthorised copy of a computer program. Mere acquisition, without regard to the actual, or intended use, constitutes an infringement of the author's copyright. "Acquisition" includes loading a copy of a program into the random access memory or other temporary storage device of a computer or onto any form of permanent data storage medium.

- **Computer Misuse Act 1990**
  Under the Act hacking and the introduction of viruses are criminal offences. The Act identifies three specific offences:
  - Unauthorised access to computer material (that is, a program or data). e.g. accessing another person's area without permission, trying to steal a password, outputting data to screen or printer
  - Unauthorised access to a computer system with intent to commit or facilitate the commission of a serious crime e.g. trying to access financial or administrative records with intent.
  - Unauthorised modification of computer material. e.g. modifying records, creation or introduction of a local or network virus, deliberately generating information to make a system malfunction

  Offensive material legislation includes: Regulations regarding the transmission, storage or display of obscene material are enforceable by law under the Criminal Justice and Public Order Act 1984, which amends the Obscene Publications Act 1956, the Protection of Children Act 1978 and the Telecommunications Act 1984 to extend their provisions to transmission over a data communications network.

Prevent Duty: From 1 July 2015 all schools registered early years childcare providers and registered later years childcare providers are subject to a duty under section 26 of the Counter-Terrorism and Security Act 2015, in the exercise of their functions, to have "due regard to the need to prevent people from being drawn into terrorism". This duty is known as the Prevent duty.

9. SAFEGUARDING AND PREVENT DUTY

9.1 Access to personal webmail is blocked on the College network. All official College communication is via College supplied email addresses and College systems.

9.2 Web browsing reports are regularly reviewed to help keep staff and students safe from terrorist and extremist material.

10. E-SAFETY

10.1 Students and staff must not take, use, share, publish or distribute images or videos of others without their permission.

10.1.1 Care should be taken when taking digital or video images that students and staff are appropriately dressed and are not participating in activities that might bring the individuals or the college into disrepute.

10.2 Personal communications are those made via a personal social media account (including personal messaging accounts, e.g. email, SMS, Skype, WhatsApp etc). In all cases, where a personal account is used which associates itself with the college or impacts on the college, it must be made clear that the member of staff or student is not communicating on behalf of the college with an appropriate disclaimer.

10.2.2 All communications between staff and students should only be made using official college systems and approved methods of communication.

10.3 Cyber bullying is any form of bullying which takes place online or through smartphones and tablets. Social networking sites, messaging apps, gaming sites and chat rooms such as Facebook, XBox Live, Instagram, YouTube, Snapchat and other chat rooms. Where appropriate, cyber bullying will be investigated and could lead to disciplinary action.

10.4 Some internet activity e.g. accessing child abuse images or distributing racist material is illegal and would obviously be banned from college and all other technical systems and would lead to criminal prosecution. Other activities e.g. cyber-bullying could lead to criminal prosecution.

10.5 To report any misuse please contact the Designated Safeguarding Lead (DSL) or Deputy Designated Safeguarding Lead (DDSL). They will decide if any further action is required.

11. RELATED POLICIES AND DOCUMENTS

Data Protection and Information Security
Huish Privacy Notices
Mobile Device Policy
Safeguarding and Child Protection Policy
Staff Code of Conduct
Student Behaviour Policy
Social Media Guidance