Policy for Acceptable Use of College ICT Facilities

RHACC
Richmond and Hillcroft Adult Community College

1. Introduction

1.1 In today's rapidly evolving digital environment, with the increasing use of cloud-based services, mobile devices, and collaborative tools, it is crucial that learning institutions play an active role in educating people not only on safe and effective use of ICT but also on cybersecurity awareness and digital responsibility. Richmond and Hillcroft Adult and Community College (**RHACC**) is committed to empowering our learners and staff, giving them the ICT knowledge, skills and behaviours that will help them succeed in this new digital age.

1.2 This requires defining appropriate and legal use of the technologies and services made available to employees, students and other authorised users. (**Users**)

2. Purpose

2.1 This policy provides a framework for the use of College ICT Facilities in a way which allows those resources to be shared and minimises the risk of harm to staff, learners, the wider community and the College itself.

2.2 It should be interpreted such that it has the widest application so as to include new and developing technologies and uses, which may not be explicitly referred to.

3. Scope

3.1 This policy applies to all users of RHACC's ICT facilities, including remote access through personal devices (BYOD) and cloud-based services used for College-related work.

3.1.1 Devices provided by the college, such as PCs, laptops, iPads and phones.

3.1.2 Networks provided by the College including the networks provided on campus, networks provided by other parties such as eduroam and internet access provided using dongles or mobile phones provided by the College.

3.1.3 Systems and applications provided by the College, such as Moodle, the student information system REMS and Adobe Acrobat

3.1.4 Information and Communication Services provided the College, such as Microsoft Teams, other Microsoft 365 services and Zoom.

3.1.5 Online services used by RHACC employees to conduct RHACC business.

3.2 This policy applies to all employees of the College, learners studying at the college and visitors using the facilities such as the Learning Centre or public wifi. Employees are defined as all persons working at the College or on our behalf in any capacity, including employees at all levels, officers, agency workers, seconded workers, volunteers, interns, agents, contractors, external consultants, third-party representatives and business partners, sponsors, or any other person associated with the College, wherever located.

3.3 In accessing RHACC's ICT network or services or using devices to study or work on behalf of RHACC all users will be deemed to have accepted the terms of this policy. This policy may be updated from time to time, in order to comply with legal and College requirements.

3.4 The use of RHACC's ICT facilities is subject to the JANET Acceptable Use policy[1], and to the terms and conditions of other suppliers and partners. Users should ensure that they are aware of these terms and abide by them whenever using the relevant services.

[1] https://community.jisc.ac.uk/library/acceptable-use-policy

Owner:	Head of IT	Approved by:	F&R Committee
Review Interval:	2 years	Approved on:	13th November 2024
Date of next review:	November 2026	Post to website:	Yes

4. General Principles

Any use of ICT facilities will generally be considered acceptable unless it violates College data privacy policies, compromises GDPR compliance, or subverts security and system integrity.

4.1 Attempts, deliberately or otherwise, to subvert the security, integrity, availability or performance of College ICT facilities or data.

4.2 Disrupts acceptable use by other users.

4.3 Causes harm to others, with particular regard to our obligations to safeguard vulnerable members of the RHACC community, and to provide a safe working and learning environment for all.

4.4 Affects personal data in a way which is contrary to the provisions of the Data Protection Act 2018 and associated regulations and guidance.

4.5 Is otherwise illegal.

4.6 Is otherwise detrimental to the interests of the College, learners, staff or the wider community.

5. Unacceptable activities

This is a list of activities that are unacceptable for any user at any time. This list is not exhaustive:

5.1 Unauthorised use of another user's logon credentials.

5.2 Disclosure of your own logon credentials to any other person.

5.3 Creation, transmission or other use of material which is:

- 5.3.1 indecent
- 5.3.2 obscene
- 5.3.3 discriminatory against someone based on any of the protected characteristics of the Equalities Act 2010 – age, disability, gender reassignment, marriage and civil partnership, pregnancy and maternity, race, religion or belief, sex, sexual orientation.
- 5.3.4 hateful
- 5.3.5 violent
- 5.3.6 extremist[2].
- 5.3.7 threatening
- 5.3.8 abusive
- 5.3.9 defamatory
- 5.3.10 harassment, bullying and/or victimisation.

5.4 Profit or gain-making activities not sanctioned by RHACC

5.5 Private or personal interests or business, where such use is excessive or unreasonable.

5.6 Compromising the security of our ICT facilities.

5.7 Seeking to gain unauthorised access to data.

5.8 Disrupting the work of other users or the correct functioning of the network.

5.9 Denying access to the network and its services to other users.

5.10 Wasting resources (e.g., people, capacity, computer, consumables).

[2] As defined by the Preventing radicalisation policy

5.11 Compromising the privacy of users or confidentiality of data.

5.12 Propagating unsolicited commercial or advertising material, chain or junk emails.

5.13 Customisation of IT equipment provided for shared use, such as in classrooms, unless specifically required for a course.

5.14 Infringing copyright.

5.15 Creating or transmitting material with the intention to defraud.

5.16 Introducing computer viruses, Trojans or other malicious software.

5.17 Downloading, installing or removing software without authority.

5.18 Deliberately or recklessly corrupting or destroying another user's data.

5.19 Any illegal activities

5.20 Using unlicenced software or services or using software or services in a way which contravenes their licences.

5.21 Installing any unauthorised software onto any College-owned device.

5.22 Introducing data-interception, password-detecting or similar software or devices to the network.

5.23 Seeking to gain unauthorised access to restricted areas of the network.

5.24 Accessing or trying to access data where the user knows or ought to know that they should have no access.

5.25 Carrying out any hacking activities; or

5.26 Introducing or propagating ransomware, engaging in phishing, or attempting social engineering to compromise other users' credentials or sensitive information.

6. Microsoft 365 accounts for Learners

6.1 Learners will be provided with a Microsoft 365 account, including an email account and access to Microsoft applications from shortly before their course starts until 31 December of the end of the academic year in which their course finishes. This means that if, for instance, a learner is enrolled in a course during the 2024/25 academic year their Microsoft 365 account will be available to them until 31 December 2025

6.2 While learners are provided with Microsoft 365 accounts, they should be aware that these accounts are subject to the College's monitoring policy and may be revoked if deemed necessary. Furthermore, learners must ensure adherence to cybersecurity best practices while using these services.

6.3 This account is provided at the College's sole discretion and may be withdrawn by the College at any time, and for any reason.

7. Passwords

7.1 College employees and learners are issued with a username, password and email address to use to access college services. These are unique to you and may not be shared with anyone else.

7.2 You must:

7.2.1 Reset passwords regularly, and at least every 90 days.

7.2.2 Ensure that your password is not obvious and is not one you use elsewhere. It should contain at least 20 characters and include 3 different words.

7.2.3 Not write your password down or save it in a password store such as a browser or spreadsheet.

7.2.4 All users should utilize MFA wherever possible, and employees are encouraged to use a password manager approved by the College, such as LastPass or Keeper, to ensure secure password management.

7.2.5 College Employees must use Multi Factor Authentication where it is provided for a College ICT Facility. Where possible, we will secure staff access to College ICT Facilities under Microsoft Azure Active Directory MFA (eg when staff members access RHACC Connect), but if that is not possible, and another form of MFA is available, it must be used.

7.3 Most College ICT Facilities which require a password use your main 'domain' password. If using a service which requires a different password, users:

7.3.1 Must not repeat their main password.

7.3.2 Must use 20 characters where possible, or the maximum allowable otherwise.

7.3.3 Must either use 3 distinct words or, if that is not possible, a mix of CAPITALS, small letters, numbers and symbols.

8. Internet

8.1 The Internet can be accessed at the College in the following ways:

8.1.1 For staff, learners and members of other academic communities visting RHACC, through the Joint Academic Network (JANET). All staff and learners must adhere to the JANET Acceptable Use Policy: https://community.jisc.ac.uk/library/janet-services-documentation/janet-policies-and-legal-requirements

8.1.2 For visitors, partners and other members of the community through "The Cloud" network provided by Sky. Users must agree and adhere to the following terms and conditions: https://service.thecloud.net/service-platform/terms-and-conditions/

8.2 RHACC applies filters to limit access to websites that contain inappropriate, offensive or illegal content e.g. obscene or pornographic, sexist, racist, terrorist, discriminatory or other offensive material. This is to protect users from inadvertently carrying out an unacceptable activity.

8.3 If you consider that, for legitimate work or learning purposes, you need to undertake any activity that may be misunderstood or considered an unacceptable activity you should:

8.3.1 Carefully consider whether your activity or research is appropriate.

8.3.2 Agree your activity with your manager or tutor before undertaking the activity.

8.3.3 If agreed, apply to IT Services to have access restrictions removed

8.4 Employees may use the internet for reasonable personal use, this must be undertaken in a user's own time, normally before or after work or whilst on a break. Any such use must not interfere with individual work responsibilities or affect the quality of service.

9. Email, Teams and other messaging services

9.1 When using College ICT facilities which include messaging services, such as email and MS Teams, users must ensure that the language used is appropriate and in particular is not:

9.1.1 indecent

9.1.2 obscene

9.1.3 hateful

9.1.4 discriminatory against someone based on any of the protected characteristics of the Equalities Act 2010 – age, disability, gender reassignment, marriage and civil partnership, pregnancy and maternity, race, religion or belief, sex, sexual orientation.

9.1.5 violent
9.1.6 extremist[3].
9.1.7 threatening
9.1.8 abusive
9.1.9 defamatory
9.1.10 harassment, bullying and/or victimisation

9.2 Discussion of individuals in email and messaging services may create personal data which is subject to the provisions of GDPR and the laws of libel. Messages may be discoverable in legal proceedings and through subject access requests. Users must ensure that any discussion of individuals is accurate and appropriate.

9.3 The college will treat all messages sent, received or stored using College ICT Facilities as messages which relate to the operation, business or academic activities of RHACC and neither staff nor learners should have any expectation of privacy in any such messages.

9.4 While the College will take reasonable steps to avoid opening or viewing messages which are marked as 'personal', the College reserves the right to access, review, copy, process, delete or otherwise process any messages sent, received or stored on College ICT Facilities and to disclose any such email messages (or information contained in them) to any person outside RHACC where this is necessary for the reasonable operation, business or academic activities of RHACC.

9.5 Employees must not use personal email accounts to conduct RHACC business, including contacting learners and external contacts.

9.6 Users must be vigilant for spam and malicious messages and be aware of opening attachments and clicking links, even if they appear to come from a recognised address. If you are in any doubt as to the safety of an email you should contact the IT Helpdesk.

10. Employee use of personal devices

10.1 Full time employees working from home regularly may request a college laptop to use for all work requirements.

10.2 Employees may use personal devices, such as laptops or smartphones to work from home or elsewhere provided the device is:

10.2.1 Not shared with others, including other members of the employee's household.
10.2.2 Protected by a password or PIN
10.2.3 Running a currently supported version of its operating system (Windows, MacOS, Android, iOS, Linux)
10.2.4 Up to date with all Windows or MacOS updates applied within 14 days of their release.
10.2.5 Running well-regarded anti-virus and malware protection software. For Windows machines, RHACC accepts Windows Security as sufficient protection provided Virus and Threat Protection, Account Protection and App & Browser control are all enabled and up to date.
10.2.6 Kept safely when not in use
10.2.7 Where possible, encrypted to protect data if the device is stolen. This is not easily done with Windows Home devices, and some older versions of Windows. It may be possible for the college to upgrade your Windows to allow encryption if you use it regularly for work purposes. Contact the IT Helpdesk for assistance with this.

[3] As defined by the Preventing radicalisation policy

10.3 Employees who are unwilling, or unable, to comply with these conditions should only access email and documents using web versions of Microsoft 365 tools and may not download any documents. They may not access Remote Desktop Server.

10.4 ITS provide support for employees using personal devices for college work. Please note that they may not be able to support software which has not been provided by the college.

10.5 Employees using personal devices must ensure that the device is regularly updated with security patches, is connected to a secure network, and uses VPN services when accessing College systems remotely.

11. Authorisation of online services, software and applications

11.1 Users may only use software on College devices where that software has been authorised by IT Services.

11.2 Employees using online services for College business which allow the uploading of learner or college data or documents or carry out significant processing may only use services which have been authorised by IT Services.

11.3 Requests to use other services, software or applications, even if free, must be submitted to the Head of IT and Digital Transformation for approval via your tutor or manager.

11.4 Approval will be granted if the service, software or application is:

11.4.1 Secure

11.4.2 Supported by the vendor or an active open-source community.

11.4.3 Complies with our Data Protection policy

11.4.4 Does not impose an unreasonable burden on IT Services for installation, maintenance and support.

11.4.5 Able to be licenced in a cost-effective manner

11.5 IT Services may provide advice on the suitability of the item for the need proposed and the potential use of alternatives.

12. Monitoring

12.1 The College will undertake routine monitoring of network activity, including the use of external email and Internet access, to detect security threats or abuse. Monitoring will be conducted transparently and in compliance with data protection laws.

13. Breaches of this policy

13.1 Breaches that compromise cybersecurity or involve data theft may result in immediate suspension, potential legal action, or reporting to relevant authorities.

13.2 Deliberate breaches of any of the provisions of this policy by any employee or learner will constitute misconduct and RHACC may commence disciplinary proceedings.

13.3 Deliberate breaches of this policy that have serious or potentially serious adverse consequences for the operation, business or academic activities or reputation of RHACC or the security and integrity of the ICT Systems will constitute gross misconduct.

Version tracking

Versions	Date	Author	Reason for changes
1.0	30 Oct 2024	Dayo Ogunjobi	Update for review

Policy for Acceptable Use of College ICT Facilities

Equality Impact Assessment: Initial Screening (Stage 1)

Name of Policy or Practice: ICT Systems Acceptable Use
Person/ Team/ Department Responsible: Director of Technology and Digital Transformation
Date of Assessment: 18 October 2024

Consider the three aims of the public equality duty:

- To eliminate discrimination
- To advance equality of opportunity
- To foster good relations

Protected Characteristics:

Age, Disability, Gender Reassignment , Race, Religion or Belief, Sex, Sexual Orientation, Marriage & Civil Partnership, Pregnancy & Maternity

Q1) What is the purpose of the policy, decision or practice	This policy provides a framework for the use of College ICT Facilities in a way which allows those resources to be shared and minimises the risk of harm to staff, learners, the wider community and the College itself.

2) Who is affected by the initiative? Does the initiative make a positive contribution to equality and diversity in the College? Or is it equality neutral i.e. no particular effect on anyone group? ***All people using RHACC computing equipment. Neutral***
3) Is there the potential for there to be a negative impact on one or more of the Equality groups as a result of this initiative? If so what groups may be effected and why? Or is it equality neutral? ***Equality neutral***
4) Has anyone complained about the policy or initiative? ***No***
5) Is the impact of the initiative significant enough to warrant a more detailed assessment? ~~Yes~~ ***No*** If yes please circle priority rating for assessment: High Medium Low