IT Acceptable Use Policy

RHACC
Richmond and Hillcroft Adult Community College

1. Purpose and Scope

1.1 Information and communication technologies (ICT) such as the Internet and email are continually evolving in today's technological world in which we live and work. With this in mind learning institutions have an important role to educate and train people in their proper use. This policy sets out the standards which apply to the use of technology by our staff members, learners, visitors and other individuals as part of their equipment for work and/or study, namely for learning, training, research, development and administrative purposes

1.2 Richmond and Hillcroft Adult and Community College (RHACC) is committed to bringing the maximum possible benefits of ICT to its learners and staff, giving them the knowledge, skills and attitudes that will enable them to succeed in the digital age.

1.3 However, the College recognises that the misuse of ICT by members of staff or learners can occur. There are risks involved in the use of the IT Systems.
Examples of such risks include:

- 1.3.1 Claims brought against RHACC because the reputation of other individuals or organisations has been damaged;
- 1.3.2 Unauthorised disclosure of information or breach of the data protection regulations
- 1.3.3 Infringement of copyright, licenses and other rights in RHACC's and other parties material (which includes use of material without the permission of the author);
- 1.3.4 Harassment and discrimination claims being brought against RHACC (caused by offensive or other inappropriate material);
- 1.3.5 Entering into contracts on behalf of RHACC by mistake;
- 1.3.6 Inadvertent breach of contract by RHACC;
- 1.3.7 The introduction of viruses to RHACC's network;
- 1.3.8 Usage of IT systems for terrorism and extremist action;

1.4 This policy is designed to prevent these and other problems and therefore you are expected to be familiar with it and comply with its contents. You should speak to the IT Helpdesk if you are unsure about whether anything you propose to do might breach this policy.

2. General Principles

2.1 All staff and learners accessing the College ICT facilities must only do so using their own unique login name and password. Under no circumstances should they use someone else's login name or password. Access to ICT facilities is subject to all staff and learners accepting the terms of the Acceptable Use Policy, each and every time they log in.

2.2 Limited personal use of ICT is acceptable, as long as the facilities provided to our staff and learners are not abused. Personal use of available electronic resources must not conflict with the educational aims of the College. Any misuse, including unacceptable use as defined in this policy, and the accessing of inappropriate material, will be seen as misconduct and may lead to disciplinary action being taken.

2.3 Staff should note that the rules contained in this policy also apply to the use of the College's ICT facilities when working on College business away from the College's premises, i.e. when working remotely and using the College webmail system.

2.4 In the event that it is deemed necessary to disable a staff member or learner's e-mail account immediately, we reserve the right to action this without prior notification.

3. Use of the Internet

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

- For staff and students through JANET, which is provided via the Joint Academic Network (JANET), and must adhere to the JANET Acceptable Use Policy. https://community.ja.net/library/acceptable-use-policy
- For members of other academic communities signed up to Eduroam through JANET – Eduroam. The JANET Acceptable Use Policy applies.
- For visitors, partners and other members of the community through "The Cloud" network provided by Sky. The terms below must be adhered to: https://service.thecloud.net/service-platform/terms-and-conditions/

3.2 Staff should note that personal use is a privilege and must not be excessive or in any way interfere with the proper performance of their duties.

Examples of Do's and Don'ts of acceptable use include, but are not limited to, the following:

Do's	*Dont's*
Use for College business, administrative, academic and research based work	Use for unreasonable personal business
Access and use of library, information resources, databases, people and news from a variety of research institutions, commercial, and non-commercial sources.	Use College ICT facilities to engage in any unlawful activity. E.g racism, sexism, homophobia, religious intolerance, terrorism, or political violence.
Administrative, academic, and research related discussion groups on a wide variety of topics.	Use College ICT facilities to defame, bully, offend or hinder another person, by the creation, transmission, storage, download or display of materials, or by any other means.
Process data for the purpose in which permission was giving in line with the fulfilment of your job at the college during the data retention period	Collect data or process data without permission from the data subject or approval from the Data Protection officer

Further examples of unacceptable use include, but are not limited to, the following:

3.3 Users must not display, download, distribute, store, edit or record any material, including images, that are offensive or, capable of constituting any form of discrimination (including on the grounds of gender, race, disability, sexual orientation, religion, belief or age, obscene, pornographic or paedophilia).

3.4 Users must not use College ICT facilities in order to promote or engage in racism, sexism, homophobia, religious intolerance, terrorism, or political violence.

3.5 Users must not use College ICT facilities for downloading and playing computer games or accessing online gambling sites.

3.6 Any deliberate attempt to bypass the College IT systems policy/procedure or ICT security systems.

3.7 Any action that intentionally jeopardises the availability or integrity of any computing, communication, or information resource.

3.8 Users must not knowingly download, transmit, store, generate or use any program, tool or virus designed to damage or disrupt or in any other way interfere with the functioning of the College ICT facilities.

3.9 Users must not attempt to gain or grant unauthorised access to any of the College's ICT facilities/Data, or use College's ICT facilities to gain unauthorised access to other ICT facilities.

3.10 Users must not use College ICT facilities to collect, create, access, process or transmit material in a way which infringes a copyright, trade mark, data protection or other rights of an individual or organization.

3.11 Users must not alter computer materials or data on the College's ICT facilities without permission of the owner or license holder. This includes systems software, other software, configurations, databases, messages, data files, web pages or web sites.

3.12 Users must treat as confidential any information to which they are given access to in using the College's ICT facilities and which is not on the face of it intended for unrestricted dissemination. Users must not copy, modify or disseminate such information without explicit permission from an authorised person.

3.13 Users must not install or run programs other than College authorised software.

3.14 Accessing or trying to access information that belongs to another person or for which no authorisation has been granted.

3.15 Users must not attempt to set-up or use any proxy by-pass software, in order to bypass the College Internet filtering systems.

3.16 Users must not use any Peer-to-Peer file sharing software, such as bit torrent and other related applications.

3.17 Users must not use the College ICT facilities in any way, which may damage, overload or affect the performance of the systems or the internal or external networks.

4. Usernames and passwords

4.1 Users must keep passwords secure at all times and must not reveal them to anyone else. The use of another person's username and/or password, with or without their permission will be dealt with under the Staff Disciplinary Procedures or the Learner Disciplinary Procedures as appropriate.

4.2 Passwords must conform to the following password policy:

4.2.1 Include a phrase of at least 3 unrelated words and must be at least 10 characters in length.

4.2.2 Passwords must only be used with college provided services and must never be reused or be similar to ones used elsewhere.

4.2.3 The College may audit password strength and require users to change their password where a weak or compromised password is found.

5. Use of Social Media

5.1 Social media has considerable potential in collaborative learning and working. At the same time the recreational use of these systems can be very time consuming and, therefore, wasteful of College resources.

5.2 Where use of social media is excessive, is in conflict with other use of resources or is infringing on work and study time, it will be regarded as unacceptable. Also, where the content is inappropriate, this will clearly be an unacceptable use of College ICT facilities. The College reserves the right to block any social media sites identified as inappropriate for an educational environment.

6. Use of Email

6.1 Personal use of email, provided that it does not impinge in any way on class, or study time in the case of learners, and on working hours in the case of staff, or involve unacceptable content, is an acceptable use of the College ICT facilities.

6.2 Misuse of the College email systems will be regarded as a disciplinary matter and disciplinary action up to and including dismissal may be taken against staff or learners found to have misused this facility.

6.3 The college will treat all messages sent, received or stored using the IT Systems as e-mails 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.

6.4 The College reserves the right to intercept e-mail messages and monitor access to the Internet in the following circumstances:

6.4.1 to detect the unauthorised use of the IT Systems;
6.4.2 to protect the IT Systems against viruses or hackers;
6.4.3 to find lost messages or retrieve messages due to computer failure;
6.4.4 to prevent or detect crime and terrorism.

6.5 The College reserves the right to access, review, copy, process, delete or otherwise process any messages sent, received or stored on the IT Systems and to disclose any such e-mail messages (or information contained in them) to any person outside RHACC where this is necessary for any purpose in connection with employment, study, or with the services users have been engaged to provide to RHACC and in the following circumstances:

6.5.1 to protect the IT Systems against viruses or hackers;
6.5.2 to find lost messages or retrieve and review messages due to computer failure or staff absence;
6.5.3 to assist in the investigations of wrongful acts (including further investigation where a routine audit has revealed a breach of this policy or the breach of any relevant regulatory or self-regulatory practices or procedures);
6.5.4 to combat or investigate fraud, corruption, extremism and terrorism;
6.5.5 to prevent or detect crime or to comply with any legal obligation.
6.5.6 to prevent the receipt of unsolicited communications that do not relate to the operation, business or academic activities of RHACC.
6.5.7 to prevent the unsecure/unauthorised transfer of data within or outside the college.

6.6 The College will take all reasonable steps to avoid opening or otherwise viewing the contents of e-mails that are marked “personal” in the subject heading unless it is believed that such action is required in the circumstances set out in paragraphs 6.4.1 to 6.5.7. E-mails marked "personal" will be subject to traffic monitoring and automated interception to check for viruses in the same way as all other e-mails sent or received using the IT Systems.

6.7 Where possible monitoring of e-mail and Internet traffic will be limited to audits and monitoring traffic data unless routine monitoring or auditing justifies more detailed monitoring. However, the College reserves the right to restrict access to individual or groups of websites should it be deemed appropriate to do so. Where possible automated monitoring will be used.

Email quotas/limits

6.8 An email quota is the amount of email (including attachments) that a user can store on the central email server.

6.9 ITS will limit the number of emails an individual can leave on the mail server to manage available disk space and ensure equitable availability of IT resources. For this reason, a mailbox should be regarded as only a temporary repository for email.

6.10 Messages and attachments should be deleted if no longer needed or can be more permanently stored on a hard drive, archived or saved on other storage media. The following limits will apply to emails:

Mailbox Quotas

6.10.1 Staff mailbox - 50GB - The system will warn users if they go over this limit.

6.10.2 Staff personal archive - 50GB - The system will warn users if they go over this limit.

System Limits

6.10.3 Maximum size of any email (including attachments) that can be sent or received will be 15MB. The system will warn users if they go over this limit.

6.10.4 Number of messages that can be sent per minute will be 30.

6.10.5 Messages in the Junk and Deleted E-mail folder will automatically be deleted when they are 14 days old.

Examples of unacceptable use include, but are not limited to, the following:

6.8 Sending the creation or transmission of material that is illegal.

6.9 Sending an email or message that does not correctly identify the user as the sender, or which appears to originate from another person or otherwise attempt to impersonate another person.

6.10 Sending unsolicited emails to a large number of recipients, without the proper authorisation to do so.

6.11 Creating or transmission of material which brings the College into disrepute, or which could be in any way potentially libellous.

6.12 Sending or forwarding an email containing abusive or threatening language, or any language that could cause offence, constitute harassment or contravene gender, race, age, religion or belief, sexual orientation and transgender or disability discrimination, legislation or related College policies.

6.13 Knowingly distributing viruses or other malicious applications via email. Any concerns over the contents of an email should be bought to the attention of the IT helpdesk.

7. Telephone Equipment Conditions of Use

7.1 Use of (RHACC) voice equipment is intended for business use. Individuals must not use (RHACC) voice facilities for sending or receiving private communications on personal matters, except in exceptional circumstances. All non-urgent personal communications should be made at an individual's own expense using alternative means of communications.

Individuals must not:

7.2 Use (RHACC) voice equipment for conducting private business.

7.3 Make hoax or threatening calls to internal or external destinations.

7.4 Accept reverse charge calls from domestic or International operators, unless it is for business use.

8.0 Ownership & Asset Management of RHACC IT

8.1 All IT services provided by RHACC, directly or via research funding, shall be considered as an IT asset, whether directly owned or leased

8.2 All RHACC IT assets may be tagged and inspected as required

8.3 All RHACC IT assets shall be returned to RHACC upon request, or when a user leaves RHACC

8.4 All RHACC IT assets may be tracked and recorded in RHACC asset systems

9. Monitoring, Filtering & Wireless

9.1 RHACC has a statutory duty, under the Counter Terrorism and Security Act 2015, termed 'PREVENT'. The purpose of this duty is to aid the process of preventing people being drawn into terrorism. Users must not create, download, store or transmit unlawful material, or material that is indecent, offensive, defamatory, threatening, discriminatory or extremist. The College reserves the right to block or monitor access to such material.

9.2 The College assumes no responsibility for guest user equipment or data when connecting to this wireless network;

9.2.1 It is the sole responsibility of the wireless device owner/user to provide antivirus protection and to configure their device settings to provide the appropriate security to control access from other wireless users and the Internet. The College will not take responsibility for damages incurred for incorrect, insufficient or incomplete security settings; or lack of adequate or up-to-date virus protection;

9.2.2. **eduroam** is provided by the college for students and staff with RHACC computer accounts and for External visitors from institutions providing their own eduroam service. The eduroam services are monitored and restricted in line with the RHACC IT Acceptable Use Policy available here: rhacc.ac.uk/q/aup.

WiFi Guest (The Cloud) is provided and supported by Sky WiFi The Cloud on behalf of the College for Visitors who are unable to use the eduroam services. The Cloud services are monitored and restricted in line with Sky WiFi The Cloud Terms and conditions available here: rhacc.ac.uk/q/cloudterms

Other web-based services and programs may not work due to filtering policies in place;

9.2.3 The College may routinely monitor information systems to assure the continued integrity and security of the IT network. You should also note that the College uses filtering software to endeavour to make sure that, wherever possible, unsuitable web sites are blocked, and keeps a record of all internet sites accessed. Guest users shall indemnify the College against all claims, damages and other losses attributable to the guest user's access to the network;

9.2.4 Encrypted SSL (https://...) based internet access will be inspected by decrypting and inspecting the page contents. The only exception to this is internet banking websites and some exam services;

9.2.5 Inappropriate use will be reported to the relevant authorities as required; and

9.2.6 Users should keep the password they have been issued secure and not share it with anyone else;

9.3 The following list is not exhaustive, but is to provide a framework for activities that fall into the category of unacceptable use. The following activities are strictly prohibited:

9.3.1 Accessing inappropriate or offensive Internet sites is strictly forbidden (this will include the accessing of gambling or betting sites). Users must also report any instances of

access to pornography or other offensive sites on the Internet if they become aware of it;

9.3.2 Unauthorised copying of copyrighted material including digitisation and distribution of photographs from magazines, books or other copyrighted sources, copyrighted music, and the installation or distribution of any copyrighted software;

9.3.3 Deliberate introduction of malicious programs into the network, fileservers or workstations (e.g. viruses, scanners, 'hacking' tools, password crackers, etc.); and

9.3.4 Effecting security breaches or disruptions of network communication. This includes accessing data of which you are not an intended recipient, logging into a server or account that you are not expressly authorised to access, using network scanning software to probe other devices connected to the network or carrying out activities that consume excessive amounts of bandwidth. Note this is an unsecured wireless network and is open to interception by other wireless users. Usage of the guest wireless network is entirely at the risk of the user. By connecting to this network, you agree to comply with the terms detailed above.

9.4 The college filters all web access in order to protect our learners and staff from information that is offensive, abusive, discriminatory, illegal to possess, or contravening college policies and regulations.

9.5 The software operates by means of a block list of undesirable web sites, which is automatically updated by the software vendor on a daily basis. Every URL (website) requested is checked against a block list, and if it is found to be on that list, instead of displaying that page, the system returns a replacement page, informing the user what has happened.

9.6 Blocked site categories include but are not limited to:

Adult / Sexually Explicit
Tasteless and Offensive
Criminal Activity
Gambling
Hacking
Illegal Drugs
Intolerance and Hate
Violence
Weapons
Proxies and Translators
Phishing and Fraud
Peer to Peer

9.7 If access to a blocked website *(URL)* is required, then a formal request must be initially made through the ITS department by a member of staff, stating the website in question, and the reason to why access is required.

10 File quotas/limits

10.1 A file quota is the size of documents that a user can store on the file server (H: drive).

10.2 ITS will limit the size of files an individual can leave on this file server. For this reason, document areas should be regarded as only a temporary repository for files and a location to store personal work related files e.g. personal confidential documents. The following limits will apply to files:

File Quotas

10.2.1 Staff document (H:) drive (operational) - 5GB

10.2.2 Staff personal (Downloads) document archive (not backed up) - 5GB

10.2.3 Learners document (H:) drive (Wiped off every summer) – 1GB

11. Internet Safety and College Values

11.1 Most of us use and access the internet via our laptops, mobile phones, tablets or personal computer. The potential for the internet to be a valuable and a fun resource for learning, entertainment, making friends and keeping in touch is unlimited.

11.2 However as we use the internet, we could be at risk of illegal activity or abuse, be it bullying, fraud or something more serious. Some examples include cyber bullying, cyber stalking, sexting, identity theft and online grooming. Online users may not always be whom they first seem. Social networking websites and apps, such as Facebook, Myspace, Tumblr and Twitter have become incredibly popular in recent years. Most users are genuine, but because it is so easy to hide your real identity, it is possible to come into contact with people users would normally want to avoid.

11.3 The college promotes values to ensure learners leave college prepared for life in modern Britain. This includes how technology is used in areas like:

Democracy: Using technology to safely gather and exchange views in learning and understanding political landscape and systems at the college and around the world.
Rule of Law: Ensuring that the use of technology is in line with the Principles of the rule of law.
Individual Liberty: Our use of technology at the college is designed to ensure that rights of individuals are respected while using technology in ways that are safe and secure.
Mutual Respect: Our use of technology supports mutual respect.
Tolerance: Using technology to promote diversity including allowing the use of technology to explore different views and believes as part of academic work or self-improvement.

Some golden rules for keeping safe – Staff & Learners

Don't give out personal information such as your address or phone number
Don't send pictures of yourself to anyone you don't know
Don't open emails or attachments from people you don't know
Don't become online friends with people you don't know
Never arrange to meet someone in person who you've met online
Use the strongest privacy settings when setting up an online profile
Always use a strong password and change it regularly
Don't contact learners using personal email, always use college emails.

11.4 Additional Information regarding Internet Safety

https://www.getsafeonline.org/

https://www.cyberstreetwise.com/

11. Security and Safeguarding the Network

11.1 You are responsible for the security of your laptop or computer terminal and must not allow your equipment to be used by any unauthorised person.

11.2 Users must ensure any computer used to access the Colleges IT Systems is protected with anti-virus software which is kept up to date. This is provided automatically for RHACC Desktop computers however laptops and home computers users should refer to the advice provided on the IT help pages http://www.RHACC.ac.uk/it or contact the IT Service Desk.

11.3 If users have cause to be away from their work station for any period and wish to avoid any risk of abuse of equipment, they should log out or lock equipment while absent. Otherwise we will be entitled to assume in the first instance that any material coming from or via your equipment was generated or passed on by the user.

11.4 Remember that images and audio files use up much more memory than text. You should not overload the system by sending chain mail or other frivolous material. Failure to comply with this requirement may be dealt with under the Staff Disciplinary Procedures or the Learner Disciplinary Procedures as appropriate.

12. Leavers

12.1 On leaving RHACC, staff and learners' e-mail accounts will be disabled, and IT Services will be notified in advance of the leaving date by HR. For staff, all IT equipment must be returned to IT services via HR on the last day. An equipment borrowed from the College by a learner must be returned to the ITS dept.

12.2 Student computer and e-mail accounts will be disabled automatically at the end of the last active course in the current academic year.

13. Discipline

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

13.2 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 IT Systems will constitute gross misconduct.

13.3 The law with regard to IT systems use is still evolving. This policy takes into account the current legal position but staff and learners should be aware that it will continue to change, often at great pace. For this reason, staff and learners must ensure that they regularly re-read this policy. In the event of a conflict between this policy and the law, the law will prevail.

14. Interpretation

14.1 This policy cannot cover every eventuality, particularly as technology and its application is changing so rapidly. Users are required to consider the purpose and objectives of this policy and to acknowledge that there are some uses of the Internet, e-mail facilities and related technology, which, while not expressly forbidden by this policy, may still be regarded as inappropriate.

14.2 "IT Systems" means the College's telecommunications and information technology systems and equipment and all related software. This definition embraces not only the accessing of email and Internet systems (or similar) from RHACC laptops or personal computers, but also from equipment not belonging to RHACC when access is pursuant to RHACC's operation, business or equipment not belonging to RHACC when access is pursuant to RHACC's operation, business or academic activities on our behalf but also the use of other equipment such as telephones, personal digital assistants, USB drives, mobile phones and fax machines.

15. Appendix - Related policies and procedures

Anti-bullying policy
http://www.RHACC.ac.uk/files/pdfs/Anti-Harassment-and-Bullying-Policy-2015.pdf

Equality and Diversity Policy
http://www.RHACC.ac.uk/files/pdfs/Equality-Diversity-Policy-2015.pdf

Social media procedure
http://www.RHACC.ac.uk/files/pdfs/social-media-procedure.pdf

Bring Your Own Device(BYOD) procedure
http://www.RHACC.ac.uk/files/pdfs/B-Y-O-D.pdf

16. Related Legislation

16.1 The use of ICT within the college is subject to various legislation, including the following:

16.1.1 Copyright, Designs & Patents Act (1988)
16.1.2 Computer Misuse Act (1990)
16.1.3 Criminal Justice & Public Order Act (1994)
16.1.4 General Data Protection Regulation (2018)
16.1.5 Human Rights Act (1998)
16.1.6 Regulation of Investigatory Powers Act (2000)
16.1.7 Lawful Business Practice Regulations (2000)
16.1.8 Communications Act (2003)
16.1.9 Counter terrorism and Security Act (2015)
16.1.10 Police & Justice Act (2006)

17. Terminology used throughout this document ICT –

Information and Communication Technology

The College - Richmond Adult Community College

Users – Staff, Learners, Governors, Visitors and Contractors

JANET *Acceptable Use Policy* - Formal HEFCE rules for use of JANET
JANET – Joint Academic Network

PREVENT – 1 of the 4 elements of CONTEST, the government's counter terrorist strategy, which aims to stop people becoming terrorists or supporting terrorism.

Users of RHACC IT Services, information systems and networks	Members of RHACC using the college's information systems and networks will act lawfully and responsibly and in full compliance with all relevant policies and procedures when handling and sharing college data, in whatever format (i.e. digital or physical). Third parties who manage, process, transmit or store information, or information system on behalf of the college will act responsibly and in full compliance with this Policy and all relevant policies and procedures when handling and sharing college data.
IT Services	Responsible for: • administering access to colleges Active Directory environment and many of its systems • hardening end user systems in accordance with research data provider requirements • implementing role based access control upon colleges shared access file systems • creating colleges Active Directory user accounts • maintaining colleges network infrastructure, firewalls and network zoning
Management	The Director of Finance and Resources ensures that security is properly evaluated and managed across the college. The Head of IT is responsible for: • writing and maintaining this policy • investigating security incidents and breaches and recommending remedial actions • assessing information and security risks • identifying and implementing controls to risks
Monitoring & Reporting	This policy is monitored by the prevailing SMT

Owner:	Paul Eleftheriou	**Approved by:**	College Management Team
Review Interval:	1 year	**Approved on:**	17/01/2019
Date of next review:	January 2020	**Post to website:**	Yes