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 the proper use of them. This policy sets out the standards which apply to the use 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 Adult Community College is committed to bringing the maximum benefits of ICT possible to its learners and staff, and equipping them with the knowledge, skills and attitudes enabling 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. This can be by accessing or transmitting offensive or unacceptable material or simply spending a disproportionate amount of time using ICT for personal, non educational or non-work related use. There are risks involved in the use of the IT Systems. Examples of such risks include:
1.3.1 Claims brought against RACC because the reputation of other individuals or organisations has been damaged;
1.3.2 Unauthorised disclosure of information which is confidential to RACC or its staff and/or learners;
1.3.3 Infringement of copyright, licenses and other rights in RACC's and other parties 'material (which includes infringement arising from the use of material without the permission of the author);
1.3.4 Harassment and discrimination claims being brought against RACC (caused by offensive or other inappropriate material);
1.3.5 Entering into contracts on behalf of RACC by mistake;
1.3.6 Inadvertent breach of contract by RACC; 1.3.7
The introduction of viruses to RACC'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 and comply with the contents of this policy. You should speak to the IT Helpdesk if you are unsure about whether anything you propose to do might breach this policy.

1.5 In order to ensure that the ICT facilities are not being misused, the College reserves the right to monitor the use of email and internet activity in terms of this policy. If you are a member of staff or a learner at RACC, failure to adhere to this policy may result in disciplinary action.

2. General Principles

2.1 All staff and learners accessing the College ICT facilities must only do so using their own unique login name or 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 The primary role of ICT, as with other resources within the College, is to support the learning and development of our learners, and to aid our staff to be able to work more effectively and productively. ICT within the college must therefore be used for the primary purpose of the curriculum and business support use. The College ICT facilities must not be used for commercial purposes such as running a business or the selling of goods or services.

2.3 Limited personal use of ICT is acceptable, as long as the facilities afforded to our staff and learners are not abused. Personal use of available electronic resources must not be permitted to 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 constituting misconduct and may lead to disciplinary action being taken.

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 notice to you.

3. Use of the Internet

3.1 The Internet can be accessed at the College as:

- For staff and Student 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 apply
- For visitors, partners and other members of the community through "The Cloud" network provided by Sky and you must adhere to the terms below 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	*Don'ts*
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.	Users must not 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	Use College ICT facilities to defame, bully, offend or hinder another person, by the
Use for topics related to the business of the college	Creation, transmission, storage, download or display of materials, or by any other means.

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, capable of constituting any form of discrimination on the grounds of gender, race, disability, sexual orientation, religion, belief or age, obscene, pornographic or paedophiliac.

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, or use College's ICT facilities to gain unauthorised access to other ICT facilities.

3.10 Users are prohibited from using College ICT facilities to create, access, or transmit material in a way which infringes a copyright, trade mark, or other intellectual property right.

3.11 Users must not alter computer material 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 are prohibited from copying software which is installed or otherwise available on the College's ICT network.

3.13 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.

3.14 Users are prohibited from installing or running programs other than College authorised software.

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

3.16 Users may not directly connect personal laptops or other equipment to any college owned networks without contacting IT helpdesk. Guest Wi-Fi access has been made available for those requiring internet accesses using their own devices.

3.17 Users may not attempt to set-up or use any proxy by-pass software, in order to bypass the college Internet filtering systems.

3.18 Users are prohibited from the use of any Peer-to-Peer file sharing software, such as bit torrent and other related applications.

3.19 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 You should keep your password secure at all times and must not reveal your password 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 Your password must conform to the following password policy

4.2.1 Passwords must be at least 6 characters long

4.2.2 Your password must contain characters from at least 3 of the following:

i. Upper case letters ii.
Lower case letters iii.
Numbers
iv. Non-alphanumeric characters

4.3 Further advice and guidance on selecting and maintaining your password can be requested from the help desk

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 time 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.

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

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

6.4 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.

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

6.6 Used for the creation or transmission of material which brings the College into disrepute, or which could be in any way potentially libellous.

6.7 Used to send or forward 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.

6.8 Knowingly distribute viruses or other malicious applications via email. Any concerns over the contents of an email should be bought to the attention of IT Services.

6.9 Exceed your authority to make representations, enter into binding agreements or place orders.

7. Monitoring Usage

7.1 The College will randomly monitor email and internet usage by staff and learners, adhering to its obligations under the legislation relevant to the use and monitoring of electronic communications and *PREVENT* statutory duty. *Refer to Related Legislation – 16.1*

7.2 Misuse of College ICT facilities, including unacceptable use as defined in this policy and the accessing of inappropriate materials, will be seen as constituting misconduct. Disciplinary action up to and including dismissal may be taken against a member of staff who has been found to have been misusing College ICT facilities in terms of this policy. Disciplinary action may also be taken against any learner found in breach of this policy.

7.3 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.

7.4 We 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 RACC and neither staff nor learners should have any expectation of privacy in any such messages.

7.5 We reserve the right to intercept e-mail messages and monitor access to the Internet in the following circumstances:
7.5.1 to detect the unauthorised use of the IT Systems;
7.5.2 to protect the IT Systems against viruses or hackers;
7.5.3 to find lost messages or retrieve messages due to computer failure; 7.5.4 to prevent or detect crime and terrorism

7.6 We reserve 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 RACC where this is necessary for any purpose in connection with your employment, your study, or with the services you have been engaged to provide to RACC and in the following circumstances:
7.6.1 to detect the unauthorised use of the IT Systems;
7.6.2 to protect the IT Systems against viruses or hackers;
7.6.3 to find lost messages or retrieve messages due to computer failure;

7.6.4 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);
7.6.5 to combat or investigate fraud, corruption, extremism and terrorism;
7.6.6 to prevent or detect crime or to comply with any legal obligation.
7.6.7 to prevent the receipt of unsolicited communications that do not relate to the operation, business or academic activities of RACC.
7.6.8 We will take all reasonable steps to avoid opening or otherwise viewing the contents of e-mails which are marked “personal” in the subject heading unless we believe that such action is required in the circumstances set out in paragraphs 6.6.1 to 6.6.6. 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.
7.6.9 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 we reserve the right to restrict access to individual or groups of website should it be deemed appropriate to do so. Where possible automated monitoring will be used.

8. Web Filtering

8.1 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.

8.2 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.

8.3 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

8.4 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.

9. Email quotas/limits

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

9.2 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.

9.3 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

9.3.1 Staff mailbox - 1GB

9.3.2 Staff personal archive - 1GB

System Limits

9.3.4 Maximum size of any email (including attachments) that can be sent or received will be 15MB.

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

9.3.6 For staff, messages in your Junk and Deleted E-mail folder will automatically be deleted when they are 14 days old.

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 drive (operational) - 5GB

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

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

11. Internet Safety

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. Unlike seeing someone face to face, online, people aren't always what they first seem.

11.3 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 you would normally want to avoid.

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/

12. Security and Safeguarding the Network

12.1 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.

12.2 You must ensure any computer you use to access our IT Systems is protected with anti-virus software which is kept up to date. This is provided automatically for RACC Desktop

computers however laptops and home computers users should refer to the advice provided on the IT help pages http://www.racc.ac.uk/it or contact the IT Service Desk.

12.3 If you have cause to be away from your work station for any period and wish to avoid any risk of abuse of your equipment, you should log out or lock your 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 you.

12.4 Avoid overloading the system by sending messages to a wide group, particularly with attachments. Do not try to send long and complex documents by e-mail without checking with the IT Service Desk that the system has the necessary capacity. 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.

13. Leavers

13.1 On leaving RACC, staff and learners' e-mail accounts will be disabled and IT Services will be notified of leavers on a monthly basis.

14. Discipline

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

14.2 Breaches of this policy which have serious or potentially serious adverse consequences for the operation, business or academic activities or reputation of RACC or the security and integrity of the IT Systems will constitute gross misconduct .

14.3 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 update themselves regularly with this policy. In the event of a conflict between this policy and the law, the law will prevail.

15. Interpretation

15.1 This policy cannot cover every eventuality, particularly as the technology and its application is changing so rapidly. You 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.

15.2 "IT Systems" means our 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 RACC laptops or personal computers and from equipment not belonging to RACC when access is pursuant to RACC's operation, business or equipment not belonging to RACC when access is pursuant to RACC's operation, business or academic activities or on our behalf but also the use of other equipment such as telephones, personal digital assistants, USB drives, mobile phones and fax machines.

15.3 This policy will be reviewed and updated annually.

16. Appendix

a. Related policies and procedures

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

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

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

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

17. Related Legislation

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

17.1.1 Copyright, Designs & Patents Act (1988)

17.1.2 Computer Misuse Act (1990)

17.1.3 Criminal Justice & Public Order Act (1994)

17.1.4 Data Protection Act (1998)

17.1.5 Human Rights Act (1998)

17.1.6 Regulation of Investigatory Powers Act (2000)

17.1.7 Lawful Business Practice Regulations (2000)

17.1.8 Communications Act (2003)

17.1.9 Counter terrorism and Security Act (2015)

17.1.10 Police & Justice Act (2006)

18. 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.

Approved: November 2016
Review date: November 2017