Richmond upon Thames College

Policy Name:	Computer Network, Internet & Intranet - Acceptable Use Policy
Policy Number/Version No:	V3
Effective Date:	August 2022
Review Date:	August 2023
Policy Responsibility:	IT Manager
Approved By:	College Management Team
For Action By:	All College staff and students
For Information to:	All College staff, students and parents/carers

Version Control:

1.0 Introduction

1.1 Richmond upon Thames College is dedicated to promoting our values of honesty, integrity, mutual respect and personal accountability to support our students in becoming fully rounded members of society with a strong sense of social and moral responsibility. We prepare our students for life in Modern Britain by developing an understanding of democracy, the rule of law, individual liberty, mutual respect and tolerance of those with different faiths and beliefs and this is reflected in our policies.

1.2 This policy applies to all users of IT facilities owned, leased or hired by Richmond upon Thames College, all users of IT facilities on the College's premises and all users of IT facilities connected to the College's computer networks. Users must also comply with any local instructions or regulations displayed alongside computing facilities or on computer screens. (See Appendix 1 – RuTC Conditions for use of the College Network Systems).

1.3 Use of the IT facilities is subject to the provisions of the Data Protection Act 1998, the Copyright, Designs and Patents Act 1988 and subsequent regulations, and the Computer Misuse Act 1990 and Local College Regulations.

2.0 Monitoring

2.1 The College reserves the right to monitor usage of its computing facilities, in order to ensure optimum performance and proper use in accordance with this policy. The allocation of a user ID and password to access the College's computer network does not imply any right to privacy. Such monitoring may be undertaken randomly or at fixed period's dependent upon the computing facility. All users should be aware that the use of the College's Internet and Intranet provision is monitored and a log of all transactions involving Internet access is available. It is also possible to read incoming and outgoing e-mail, although this is not normal practice in the College.

2.2 Monitoring of computer use does not extend to viewing e-mail messages created by individual users unless the user's consent has first been sought. However, if a user has requested technical assistance from the IT Support Unit (ext 222) to access e-mails, such consent is deemed to have been given. Where obtaining such consent is not practicable or appropriate, (e.g. where misconduct is reasonably suspected), the express written permission of the Principal or Vice Principal must be obtained. If access is granted, the user will be informed of the action which has been taken. Where managers use a computer file, e-mail message or computer log of user actions to investigate a suspected abuse, it will be disclosable if relevant to legal or disciplinary proceedings.

2.3 The systems operator (IT Support Unit) Under *The Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000*, are authorised to monitor and keep a record of communications, for the purpose of preventing or detecting crime, and investigating or detecting the unauthorised use of said systems. By using college systems, you understand and consent to monitoring under these regulations.

3.0 Acceptable Use

3.1 Richmond upon Thames College's computer network Internet and Intranet provision may be used by staff, enrolled students and external guests (where appropriate) for any legal activity that is in furtherance of the aims and policies of the College. However all usage must be carefully managed to ensure that the College's image and reputation is properly protected; its

liability limited; its data security maintained; usage is for legitimate purposes only and is accomplished in a cost effective manner.

3.2 This policy must be read in conjunction with the following:

- RuTC Bring Your Own Device Policy
- RuTC Social Media and E-Safety Policy
- RuTC IT Security Policy

4.0 Unacceptable Use

4.1 Users must not cause any form of damage to the College's computing equipment or software, nor to any of the rooms and their facilities and services which contain that equipment or software. The term "damage" includes modifications to hardware or software which, whilst not permanently harming the hardware or software, incurs time and/or cost in restoring the system to its original state. Costs associated with repairing or replacing damaged equipment or software and/or in providing temporary replacements may be charged to the person or persons causing the damage. The costs will be determined by the designated authority.

4.2 The College network Internet and Intranet services may **not** be used for any of the following:

- The creation or transmission (other than for properly supervised and lawful research purposes) of any offensive, obscene or indecent images, data or other material, or any data capable of being resolved into obscene or indecent images or material;
- The creation or transmission of material which is designed or likely to cause harassment, annoyance, inconvenience or needless anxiety;
- The creation or transmission of defamatory material;
- The connection of any device into the College's computer network without prior agreement from an appropriate designated authority;
- The unauthorised purchase of "goods" and/or "services" through the Colleges network and/or Internet services;
- The transmission of material such that this infringes the copyright of another person;
- The sharing or documenting of Logins and/or passwords;
- The transmission of unsolicited commercial or advertising material either to other User Organisations, or to organisations connected to other networks, save where that material is embedded within, or is otherwise part of, a service to which the member of the User Organisation has chosen to subscribe;
- Deliberate unauthorised access to facilities or services accessible via the college's computer network or Internet provision;

4.3 Deliberate activities with any of the following characteristics are **not** permitted:

- Wasting staff effort or networked resources, including time on end systems accessible via the Colleges' computer network, Internet and/or Intranet facilities and the effort of staff involved in the support of those systems;
- Corrupting or destroying other users' data;
- Violating the privacy of other users;
- Disrupting the work of other users;
- Using the College's computer network, Internet and/or Intranet service in a way that denies service to other users (for example, deliberate or reckless overloading of access links or of network equipment);

- Continuing to use an item of networking software or hardware after an appropriate designated authority has requested that use cease because it is causing disruption to the correct functioning of the College's computer network, Internet or Intranet provision;
- Other misuse of the College's computer network and/or networked resources, such as the introduction of "Viruses", "Worms", "Trojan Horses" or other programs which have a 'harmful' or nuisance affect.
- The taking of deliberate action to circumvent any precautions taken by the College to safeguard the security of its computer systems.

4.4 Where the College's network, Internet or Intranet facility is being used to access another network, any abuse of the acceptable use policy of that network will be regarded as unacceptable use of the College's computer network, Internet and/or Intranet services.

4.5 The use of any of the College's computing facilities for commercial gain, for work on behalf of others or for private or personal use (unconnected with a student's course of study at the College or a member of staff's legitimate activities) is not permitted, unless prior agreement has been made with the designated authority for the facilities and an appropriate charge for that use has been determined.

5.0 Security & Confidentiality

5.1 User passwords must be kept confidential and are not to be disclosed except to the IT Support Unit to enable work to be carried out. With this one exception, it is not acceptable to share passwords with colleagues.

5.2 All users are responsible for ensuring that they do not introduce viruses into the College's computer network. Initial protection must be secured by ensuring that virus check software is installed and upgrades run as available. In particular, the source of all e-mail attachments must be verified prior to opening the attachment. The advice of the IT Support Unit (ext 222) must be obtained and followed with reference to any e-mail attachment of uncertain origin or content.

5.3 Data which is of a highly sensitive or confidential nature should not be sent by e-mail as there is a high risk that it will reach or be accessed by inappropriate recipients.

5.4 Users should be aware that data is not normally deleted from a computer's hard disk when an instruction to delete a file, e-mail or other record is executed. The assistance of the IT Support Unit (ext 222) should be sought if any machine, which has been used for storing highly sensitive data, is to be relocated or decommissioned.

6.0 Personal Responsibility

6.1 It is essential that the provisions of this policy are understood and observed by the whole College Community. If anyone is not clear about any of the rules it is their responsibility to seek advice and ask for further guidance. If anyone is aware of actions which do not comply with this policy or they are affected by actions which are not permitted, they should retain any evidence (e.g. copy of an e-mail message, document) and report the matter to a member of staff or line manager as appropriate.

6.2 Remote Access

6.2.1 Personal Remote Access to RuTC Systems for completion of work duties is only permitted after explicit permission has been granted from both the staff member's line manager, and the IT Department. Personal remote access is a privilege, not a right, and can be revoked and any time, without warning in the event of a broken policy or security breach.

6.2.2 External Remote Access for support purposes must be pre-booked via the IT Department, and the third party involved must have signed the RuTC IT Interconnection Agreement.

7.0 Enforcement

7.1 Failure to comply with this policy may result in withdrawal of access to IT facilities, local, College-wide or external, at the discretion of the Head(s) of the Department(s) concerned. It may also result in further investigation and invoking of the College's formal disciplinary procedures. Infringement of certain regulations may be subject to penalties under civil or criminal law and such law may be invoked by the College.