Contents

Amendments:	**Microsoft Teams referenced, email usage advice updated**
Re-authorised By:	**Information Security Group**
Re-authorisation Date:	**June 2020**
Policy Version:	**6.0**
Date of review:	**October 2021**

the creation, collection, storage, downloading or displaying of illegal offensive, obscene, indecent or menacing images, data or material capable of being resolved into such

the downloading, copying and/or re-sale of copyrighted material such as films, music, journal papers etc. in breach of the owner's license terms and the Copyright, Designs and Patent Act

processing personal data in a manner that does not comply with the RVC's Data Protection Policy and all current UK Data Protection legislation

conducting activity that will harass, defame, defraud, intimidate, impersonate or otherwise abuse another person

unencrypted emails, please refer to IT policies on Information Handling (ITPOL002) and Encryption (ITPOL003) for further information.

Only use email signatures that are consistent with the current advice issued by RVC External Relations and also follow the Social Media guidance issued by the College.

Abide by any departmental advice issued on appropriate Subject lines, message content etc which apply to the local operational circumstances, especially where communications with external parties are involved.

Always consider other channels of communications such as the RVC Intranet, Learn and signage systems before proposing 'mass emails' as often the content will not be applicable to many of the recipients within distribution lists used.

If an organisation wide email is agreed for broadcast, the recipients/distribution group names should be included in the (hidden) : field rather than the : field, for both security and avoidance of accidental replies to all.

When creating or requesting new group/team/distribution list names for communication and collaboration purposes, ensure that a similar designation does not already exist or will appear at all misleading or unprofessional.

Remember the use of the College IT facilities and networks is restricted to bona fide purposes only, i.e. teaching, study, research, administration or related activities. When using these systems, you must abide by the Acceptable Use Policy.

7.4. Document Sharing Platforms

Documents must be shared via the RVC's OneDrive platform, rather than via third party platforms such as DropBox.

7.5. Use of the Internet

The primary reason for the provision of Internet access is for the easy retrieval of information in relation to College activities. However, it is legitimate for users of IT services to make use of the Internet in its various forms in the same way as email above as long as it is not used to view or distribute improper material such as text, messages or images which are derogatory, defamatory or obscene. Inappropriate use of the Internet may be treated as misconduct under the appropriate disciplinary procedure. The College reserves the right to audit the use of the Internet from particular computers or accounts where it suspects misuse of the facility.

8. Personally Owned Devices

Personally owned devices must not be used to store or share RVC business information. Where it is necessary for staff to use personally owned devices for RVC work purposes, these must have up

9. Using Social Media

Users of services external to the College such as Facebook/Twitter are expected to abide by the

Personal equipment connected to the RVC domain and network from halls of residence must comply with certain standards (100/1000baseTX, 802.11n/ac) and the only protocol family supported by IT Infrastructure Services is TCP/IP.

Users connected to the College domain from halls of residence must not:

Run Peer to Peer applications that distribute copyright material.
Attempt DDNS dynamic Name Server Updates.
Set up network file shares that are writable without a password.
Re-distribute access to others, nor any college resource made available to them.
Configure any device attached to the domain with any IP address not specifically allocated to them.
Connect any form of Wireless Access point to the domain, nor configure any computer with wireless capability such that the domain can be accessed wirelessly.
Download or distribute copyright material in breach of any licence conditions.

Neither are they permitted to run:

DHCP servers
eaʿ dibute copyr e

IT Infrastructure Services reserves the right to actively scan for vulnerabilities or infections on connected systems and monitor the usage. This is in order to guarantee the integrity of the network service and user compliance with this service. In any case of misuse, RVC reserves the right to suspend students' use of the Halls of Residence connection and associated services if they contravene these regulations in any way.

The use of wireless-based access points, routers or bridges, or the use of NAT-based routing devices,