IT Acceptable Use Policy

Policy Owner	University Secretary and VP Corporate Operations	**Policy Author**	Director of IT and Digital
Approved By	The Executive	**Date Approved**	June 2023
Status	Approved	**Impact Assessment**	Yes
Version	5	**Date of Next Review**	June 2026
Endorsed By	Quality Assurance Enhancement Committee and Staff Governance Committee		

Version Number	Purpose/Change	Date
4	Replaces Policy for the Use of IT Facilities, with additions reflecting modern IT usage including a more detailed responsibilities section and in new policy format.	July 2020
4.1	Updated to meet accessibility requirements; 1.5 line spacing, tidying up of links and amending introduction into body of the policy.	February 2021
5	Policy reviewed and updated to reflect Prevent Duty explicitly in sections 5.4 and 6.1, added section 4.5 to cover RGU system usage for non RGU business and minor formatting. Additional updates carried out in sections 1.2, 4.2.1, 4.3.6, 4.6.2, 4.7.3 & 5.4 to reflect current status and additional cyber security controls now available to RGU.	May 2023

IT Acceptable Use Policy

1. Policy Statement

1.1 The aim of this policy is to ensure that the IT Facilities at Robert Gordon University are used safely, lawfully, and equitably and that individuals understand that they have personal responsibilities for ensuring information security.

1.2 This policy should be read in conjunction with the Information Governance Policy.

2. Scope

2.1 This policy applies throughout the University, its IT infrastructure, its IT equipment (including mobile phones and devices) and its IT networks. It applies to all users of the University's IT on or off campus including staff, students and any third parties who use the University IT facilities.

2.2 The University IT facilities includes hardware, software, data, network access, third party services, online services or IT credentials provided or arranged by the University.

2.3 The IT facilities are provided to support the University's core business activities, primarily learning, teaching and research, plus all administrative, business development and support functions to support these core activities.

3. Governance

3.1 When using the RGU IT facilities, you remain subject to the same laws and regulations as in the physical world. When accessing services from another country, you must abide by all relevant local laws, as well as those applicable in the UK. Breach of any applicable law or third-party regulation will be regarded as a breach of this IT policy (see Annex 1).

3.2 You must abide by the regulations applicable to any other organisation whose services you access such as Janet, Eduserv and JISC Collections. When using services via Eduroam (University Wi-Fi), you are subject to both the regulations of RGU and the institution where you are accessing services. Some software licences procured by RGU will set out obligations for the user - these should be adhered to.

3.3 Limited use of IT facilities for personal activities (provided that it does not infringe on any other aspect of this policy and does not interfere with others' valid use) is permitted. Use of IT facilities for non-institutional commercial purposes, is not permitted.

3.4 All messages distributed through the University's e-mail system, even those of a personal nature can be subject to release under Data Protection and Freedom of Information legislation.

4. Responsibility

4.1 IT Credentials

4.1.1 You must not use the IT facilities unless you have been provided with IT credentials (for example, a username and password, email address, smart card, or other identity hardware).

4.1.2 You must take all reasonable precautions to safeguard any IT credentials issued to you.

4.1.3 You must not allow anyone else to use your IT credentials. Nobody has the authority to ask you for your password and you must not disclose it to anyone.

4.1.4 You must not attempt to obtain or use anyone else's credentials.

4.1.5 You must not impersonate someone else or otherwise disguise your identity when using the IT facilities.

4.2 Data Storage

4.2.1 Files should be stored on the University provided Network Drives, Moodle, or Office 365 (0neDrive, Teams, SharePoint). These facilities are provided to support a user's work and study activities, please be aware that personal data in relation to non-RGU activities should not be stored in these facilities (please read section 4.5 of this document).

4.2.2 The University's supported method of sharing data with external organisations is through Office365 (OneDrive, Teams).

4.2.3 You must not create, download, store or transmit unlawful material, or material that is indecent, offensive, threatening, or discriminatory.

4.3 Security

4.3.1 You must not subvert, circumvent, or attempt to subvert or circumvent University security safeguards such as firewalls or antivirus software.

4.3.2 You must not leave your computer logged on when unattended - either lock it with a password or log off.

4.3.3 When using the IT facilities, you must comply with all other relevant University policies and procedures.

4.3.4 You must not use unauthorised software, interfere with hardware, or introduce malware to the IT facilities.

4.3.5 You must not infringe copyright or break the terms of licences for software or other material.

4.3.6 Users are responsible for acting in a timely manner on any security instruction, guidance, or advice provided by the University.

4.4 Information Governance

4.4.1 If you are using the IT facilities in order to process personal data, you must ensure this is done in line with the Information Governance Policy and supporting guidance.

4.5 Non-RGU Business on RGU Systems and Services

4.5.1 The University understands that staff and students have interests and commitments with third-party organisations outside of their day-to-day University work. E.g., a lecturer from the Law School may be a Board Member for a local charity, or a student could be a member of a drama group. In these situations, staff and students should refrain from using RGU licensed software, systems and services, this includes software such as Zoom and Microsoft Office (including Teams, OneDrive, Outlook, SharePoint etc.) to interact with and store information, but remember no RGU licensed software, systems and services should be used. This is because personal data will be retained on RGU systems that the University, under GDPR, has no lawful basis to process and the third-party organisation would be the data controller. For example, by participating in an online Zoom or Microsoft Teams meeting personal data can be captured by the systems, and this can include information contained in documents shared during such an online meeting.

4.5.2 There will be circumstances in which staff and students work with third-party organisations due to their role in the University, e.g., a nursing lecturer could be working on a project with the Nursing and Midwifery Council, or the University Secretary is part of the Scottish University Secretary Group, in these situations staff and students can continue to use RGU licensed software, systems and services as the lawful basis for engagement with these categories of third-parties would be legitimate business interest. Caution must be exercised at all times in relation to third-party files or documents being stored on RGU systems and the intention of the third-party circulating files or documents must be respected, e.g., a third-party may circulate

documents prior to or during an online meeting for the purposes of that meeting only with an expectation that the files or documents would not be stored at RGU for any considerable period of time. Equally RGU staff and students must exercise caution when sharing RGU files and documents with third parties as personal information may be included that the third-party has no rights to process.

4.5.3 The above examples are not inclusive and for further information or guidance please contact the Data Protection Officer at dp@rgu.ac.uk.

4.6 Using your own Device

4.6.1 RGU accepts the use of user owned devices such as Smart Phones, Tablets, Laptops and PCs for work/course activity and this Acceptable Use Policy applies when these devices are logged in or connected to the RGU Network or systems.

4.6.2 Users are responsible for the upkeep of their devices including actioning software updates and running antivirus software. If a user device is seen as posing a threat to University systems or services, i.e., it contains known malware, that device could be blocked from, or have limited access to the RGU network and University systems and services until appropriate updates are carried out.

4.6.3 The user of owned devices should ensure there are adequate access controls enabled (password, PIN etc.).

4.6.4 No personal University data must be stored on the memory of your device (care should be exercised when making recordings of audio, video, or photographs).

4.6.5 For security purposes all user owned devices on campus are only allowed to connect to the University's campus network through Wi-Fi. User owned devices must not be directly connected to the University's campus network via a physical connection.

4.6.6 To access applications, course software, email and network drives users must use the secure RGU MyApps environment.

4.7 Off Campus Working

4.7.1 When travelling, equipment (and media) must not be left unattended in public places. Portable computers should be carried as hand luggage when travelling.

4.7.2 You must not process sensitive information in public places (e.g., on public transport) where it might be viewed by others.

4.7.3 Public Wi-Fi hotspots (e.g., coffee shops and hotels) are not secure as there is no easy way to ascertain who controls or owns the hotspot. This can put your data at risk, so where possible opt for a trusted Wi-Fi connection or mobile 3G/4G/5G network to ensure a secure connection. Use of a Virtual Private Network (VPN)is also possible, however when using a VPN access to certain parts of RGU managed systems might be prevented, this is due to underlying cyber security concerns and mitigations put in place by the University.

4.7.4 Passwords for access to the University's systems should never be stored on mobile devices where they may be stolen or permit unauthorised access to information assets.

4.7.5 Security risks (e.g., of damage, theft) may vary considerably between locations and this should be considered when determining the most appropriate security measures.

4.8 Working Overseas

4.8.1 If you work outside the UK as part of your role at RGU you must consider the access restrictions and other difficulties that you may encounter when using IT equipment in other countries.

4.8.2 In order to ensure you are given the most relevant advice relating to the country, users should contact the IT Services Helpdesk to discuss requirements in more detail.

5. Monitoring

5.1.1 In order to ensure compliance with this policy, RGU monitors and records the overall use of its IT facilities for the purposes of:

5.1.2 The effective and efficient planning and operation of the IT facilities.

5.1.3 Detection and prevention of infringement of these regulations.

5.1.4 Investigation of alleged misconduct.

5.2 Monitoring of individual use, and accessing data in individual user accounts, will only be undertaken by specific members of staff as a recognised part of their normal duties. Any such activity will be approved by the Director of HR and the relevant portfolio holder from the University Executive and be:

5.3 for legitimate business reasons; justifiable; fair; proportionate; not unnecessarily intrusive; and compliant with all applicable legislation including the General Data Protection Regulation, the Data Protection Act 2018 and the Human Rights Act 1998.

5.4 RGU will comply with lawful requests for information from government and law enforcement agencies.

5.5 Under Section 26 of the Counter-Terrorism and Security Act 2015, the University has a duty when discharging its functions to have due regard to the need to prevent people from being drawn into terrorism. To support this duty the University may filter web content in certain situations, this is a generic filtering process and is not targeted at individuals. Additional filtering may also take place at device level for RGU owned devices, at the University Firewall and through our Jisc/Janet Services.

6. Compliance

6.1 Under this Policy it is forbidden to create, download, store, or circulate any materials or digital assets which are illegal, that may cause offence, are discriminatory in nature or that promote terrorism. Should a staff or student users require access to these categories of content for research purposes they must obtain the necessary permissions from their School and Executive member, as a well as successfully seeking the appropriate research permissions.

6.2 Infringing this Policy may result in sanctions under the RGU's disciplinary processes. For staff this would be dealt with through the disciplinary procedure and for students this would result in student misconduct proceedings.

6.3 If the disciplinary process finds that you have breached this policy, sanctions may be imposed.

6.4 For contractors or third-party organisations, breach of this policy will lead to remedies for RGU as detailed within the relevant contract.

6.5 Information about infringement may be passed to appropriate law enforcement agencies, and any other organisations whose regulations you have breached. You must abide by the law when accessing RGU's IT facilities.

6.6 If you become aware of any infringement of this policy, you must raise a call with the ITS Helpdesk.

7. Review

7.1 This policy will be reviewed every three years or as required.

Annex 1:

Laws and Regulations

Computer Misuse Act 1990 - creates offences of unauthorised access and interference with computers and data.

Counter Terrorism and Security Act 2015 – places a duty that a specified authority must, in the exercise of its functions, have due regard to the need to prevent people from being drawn into terrorism.

Communications Act 2003 - creates offences of improper use of a public communications service (s.127) and dishonestly obtaining electronic communications services (s.125).

Investigatory Powers Act 2016 - controls the interception of traffic on networks. It also creates powers for the police and other investigating authorities to require networks to provide information about their users and their use of networks.

The Investigatory Powers (Interception by Businesses etc. for Monitoring and Record Keeping Purposes) Regulations 2018 - covers interception for business purposes, for example the enforcement of acceptable use policies.

Data Protection Act 2018 and General Data Protection Regulation - establish requirements on anyone holding personal data on a computer or any other organised filing system.

Privacy and Electronic Comm1mications (EC Directive) Reg11lations 2003 - contains detailed restrictions on the use of personal data in electronic communications (for example sending unsolicited e-mails), amended by the Privacy and Electronic Communications (EC Directive)(Amendment) Regulations 2011.