I.T. Security & Acceptable Use

Reed Business
● ● ●
School

Introduction

Reed Business School Ltd (RBS), a separate entity within the Reed Group, outsources its IT management to the Reed Group central IT team. All RBS staff are considered as co-members of Reed Group. The Group is owned by the Reed family and it is committed to the following values:

- We are Fair, Open and Honest
- We Take Ownership
- We Work Together

These values are the cornerstones of the Reed Group policies.

Purpose

RBS seeks to promote and facilitate the proper and extensive use of Information Technology (IT) for the sole purpose of supporting the teaching, learning and business activities of RBS and may be used for any legal activity that further the aims and policies of RBS. This requires the responsible and legal use of the technologies and facilities made available to apprentices, learners, visitors and co-members of RBS.

It is the responsibility of all users of RBS IT services to read and understand this policy. This policy may be updated from time to time, in order to comply with legal and policy requirements.

This Acceptable Use Policy is intended to provide a framework governing the use of all IT resources across RBS. It should be interpreted such that it has the widest application and so as to include new and developing technologies and uses, which may not be explicitly referred to. This policy is additional to and does not replace the Reed Group IT policy which sets out guidelines for all co-members that is available on the Intranet.

The purpose of this document is to ensure that all users (apprentices, learners, visitors, co-members and associates etc.) of RBS IT facilities are aware of RBS policies relating to their use. Effective and proper use of information technology is fundamental to the successful and efficient running of RBS. However, misuse of IT - in particular misuse of e-mail, social media, and access to the Internet - exposes RBS to liability and is a drain on time and money. It is the responsibility of all users of RBS IT facilities to be aware of and follow all RBS IT policies and guidelines and to seek advice in case of doubt.

Scope

This policy applies to all users, including apprentices, learners, visitors, co-members and others, of the IT facilities provided by RBS. It also addresses the use of RBS IT facilities accessed via resources not fully owned by RBS, such as partner resources and the use of personal BYOD ('bring your own device') equipment.

The IT facilities include hardware, software, data, storage, network access, telephony, printing, back-office systems and services and service provided by third parties including online, Cloud and hosted services.

Definitions of Unacceptable Use

Unacceptable use includes, but is not limited to:

- Creation or transmission, or causing the transmission, 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.

- Creation or transmission of material which is subsequently used to facilitate harassment, bullying and/or victimisation of a member of RBS or a third party or which promotes discrimination on any of the protected characteristics as laid out in the Equality, Diversity and Access Policy.

- Creation or transmission of material with the intent to defraud or which is likely to deceive a third party or which advocates or promotes any unlawful act.

- Unlawful material, or material that is defamatory, threatening, discriminatory, extremist or which has the potential to radicalise themselves or others.

- Material that infringes the intellectual property rights or privacy rights of a third party, or that is in breach of a legal duty owed to another party.

- Material that brings RBS into disrepute.

- Deliberate unauthorised access to networked facilities or services or attempts to circumvent RBS security systems.

- Deliberate activities having, with reasonable likelihood, any of the following characteristics:

  - Wasting staff effort or time unnecessarily on IT management.

  - Corrupting or destroying other users' data.

  - Violating the privacy of other users.

  - Disrupting the work of other users.

  - Denying service to other users (for example, by deliberate or reckless overloading of access links or switching equipment).

  - Continuing to use an item of networking software or hardware after a request that use should cease because it is causing disruption to the correct functioning of the network.

  - Other misuse of network resources, such as the introduction of computer viruses, malware, or other harmful software.

  - Introduce data-interception, password-detecting or similar software or devices to the RBS Network.

Consequences of Breach

In the event of any failure to comply with the conditions of this Acceptable Use Policy by a user, RBS may in its sole discretion:

- Restrict or terminate a user's right to use RBS IT facilities.

- Withdraw or remove any material uploaded by that user in contravention of this Policy.

- Where appropriate, disclose information to law enforcement agencies and take any legal action against a user for breach of this Policy, including but not limited to claiming all costs, fees and disbursements (including but not limited to legal fees) connected therewith.

- Investigate disciplinary action, arising from the breach of this policy, and in accordance with RBS's Disciplinary Policy. Disciplinary action may ultimately lead to dismissal or learners/apprentices being disciplined in line with the published Code of Conduct.

Terms & Conditions
www.reedbusinessschool.co.uk/terms-and-conditions

Reed Business School
The Manor, Little Compton
Moreton-in-Marsh
Gloucestershire GL56 ORZ

01608 674224
rbs.reed@reedbusinessschool.co.uk
www.reedbusinessschool.co.uk