Policy Document

I.T. Security, Acceptable Use & Online Safety

Reed Business School

Introduction

Reed Business School values the safety and security of all staff, students, contractors and visitors to the Manor and other related facilities. It is the responsibility of all staff, students, visitors, and other users of Reed Business School facilities to be familiar and comply with our Information Technology Security and Acceptable Use Policy.

We recognise that information is fundamental to our successful operation and must be protected against breaches of confidentiality, failures of integrity and interruptions to availability. Effective information security is a combination of physical and technical security, together with appropriate policies which define the requirements which must be adhered to safeguard information.

Document Control

Version:	#01	Approved:	Stella Shaw
Date of review:	02.08.2023	Title:	Operations Manager
Next review:	01.08.2024	Signed:	
Author(s):	Desiree Rooker Jane Hyde-Walsh		

Purpose

Reed Business School 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 Reed Business School and may be used for any legal activity that further the aims and policies of Reed Business School. This requires the responsible and legal use of the technologies and facilities made available to apprentices, learners, visitors, and co-members of Reed Business School.

This IT Security and Acceptable Use Policy is intended to provide a framework governing the use of all IT resources across Reed Business School. It should be interpreted such that it has the widest application and 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 Reed Business School IT facilities are aware of Reed Business School policies relating to their use.

The objectives of this policy are to:

- Ensure that all information and information systems within Reed Business School are protected to the appropriate level.
- Ensure that all users are aware of and comply with this policy and all current and relevant UK legislation.
- Provide a safe and secure information systems environment for staff, apprentices, students, and any other authorised users.
- Ensure that all users understand their own responsibilities for protecting the confidentiality and integrity of the data that they handle.
- Protect Reed Business School from liability or damage through the misuse of information or information systems.
- Ensure that information is disposed of in an appropriately secure manner when it is no longer relevant or required.

For the purposes of this document, information security is defined as the preservation of:

- Confidentiality: protecting information from unauthorised access and disclosure.
- Integrity: safeguarding the accuracy and completeness of information and processing methods.
- Availability: ensuring that information and associated services are available to authorised users when required.

Scope

This policy applies to all users, (including apprentices, learners, visitors, co-members, and others), of the IT facilities provided by Reed Business School. It also addresses the use of Reed Business School IT facilities accessed via resources not fully owned by Reed Business School, 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.

Legal responsibility

Reed Business School seeks to promote and facilitate the positive and extensive use of Information Technology in the interests of supporting the delivery of learning, teaching, innovation, and research to the highest possible standards. This also requires appropriate and legal use of the technologies and facilities made available to students, apprentices, staff, and partners of Reed Business School.

All users of Reed Business School IT resources must comply with all applicable laws, regulations, and policies, including but not limited to the Data Protection Act 2018, and General Data Protection Regulation (GDPR).

Information exists in many forms. It may be printed or written on paper, stored electronically, transmitted by post, or using electronic means, shown on films, or spoken in conversation. Appropriate protection is required for all forms of information to ensure business continuity and to avoid breaches of the law and statutory, regulatory, or contractual obligations.

Effective and proper use of information technology is fundamental to the successful and efficient running of Reed Business School. However, misuse of IT - in particular misuse of e-mail, social media, and access to the Internet - exposes Reed Business School to liability and is a drain on time and money. It is the responsibility of all users of Reed Business School IT facilities to be aware of and follow all Reed Business School IT policies and guidelines and to seek advice in case of doubt.

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 Reed Business School or a third party or which promotes discrimination on any of the protected characteristics as laid out in the Equality, Diversity, and Inclusion 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 Reed Business School into disrepute.
- Deliberate unauthorised access to networked facilities or services or attempts to circumvent Reed Business School 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 Reed Business School Network.

Acceptable use during remote learning and using Microsoft Teams

At Reed Business School we have a blended learning approach to delivering courses. Blended learning is an approach to training and education that combines face-to-face, classroom-based learning with distance learning, or eLearning via Microsoft Teams. All courses are recorded via Microsoft Teams. We offer remote learning to students and apprentices with prior arrangements in place. All apprentices, students and tutors will have access to Microsoft Teams with individual log in details.

- Reed Business School will clearly communicate expectations to students when working online.
- A reminder to students to dress as they would at college when using webcams.
- Students are unable or may not attempt to call, chat, or set up private groups between each other on Microsoft Teams.
- Students are unable or may not attempt to start or record a meeting or lesson.
- Students are not permitted to share recorded videos and lessons made by tutors within or outside of the Reed Business School Teams Account.
- Students should blur their background if in a lesson which involves a camera or use neutral or plain backgrounds.
- Students should think carefully about what acceptable language with regards is to what they type and post.
- Students must hang up at the end of the lesson once instructed to do so. The tutor is responsible for ensuring the meeting is closed.
- Ensure tutors understand and know how to set up and apply controls relating to student interactions, including microphones and cameras.
- Ensure two factor authenticator is set up for all students, apprentices, and tutors to access Microsoft Teams with password protection and ensure passwords are kept securely and not shared.
- Ensure all tutors, apprentices, and students have a clear understanding of expectations around behaviour and participation.
- Interaction: Both for students, apprentices and tutors it is important to be able to see each other's faces while taking morning attendance registers.
- Engagement: If the cameras are off, it is difficult to ensure students are fully engaged in lessons. Constant engagement with questions and interactions and discussions are encouraged with cameras being switched on and off.
- Wellbeing: To ensure a that learners and apprentices, including tutors are in a safe learning environment as part of safeguarding it is good to check up on wellbeing and that includes socialising and not feeling isolated.

Inappropriate or illegal online activity

Illegally downloading software, music, films, images, or publications can be a crime and if convicted can lead to a prison sentence. In 2016, the government moved to introduce harsher punishments for 'pirates' who illegally download music and videos with the Digital Economy Bill.

Hacking

The Computer Misuse Act 1990 makes it illegal to gain:

- unauthorised access to computer material
- unauthorised access with intent to commit or facilitate commission of further offences
- unauthorised acts with intent to impair, or with recklessness as to impairing, operation of a computer

Gambling online

Online gambling is the largest gambling sector in the UK. The consequences of gambling can be catastrophic and include:

- losing vast sums of money
- becoming addicted
- bankruptcy
- losing possessions, family, and friends
- losing employment

Terrorism and terror-related grooming

Under the Terrorism Act 2006, the following rules apply to online activity:

- it is a criminal offence to encourage terrorism by directly or indirectly inciting or encouraging others to commit acts of terrorism. This includes "glorification" of terror by people who "praise or celebrate" terrorism in a manner that encourages others to commit terrorist acts.
- It is an offence to sell, loan, distribute or transmit terrorist publications, e.g., a bomb-making manual.
- Proscribed terrorist groups or organisations that glorify terrorism that are banned by UK law.

Proscribed terrorist groups or organisations - GOV.UK (www.gov.uk)

Financial scams

Financial scams have been happening for hundreds of years, but the Internet has provided a faster, more sophisticated way for criminals to cheat unsuspecting individuals out of their hard-earned money. Examples include:

- Fake websites – criminals have become adept at copying legitimate banking websites to trick customers into providing their login information.
- Fake emails – criminals also create legitimate-looking emails from banks and credit card companies that tell customers their account has been hacked, and ask them to provide security information so that their identity can be verified.

- Selling something online that doesn't exist – this scam happens so often that there is a Banking Protocol system, which alerts police to unusual activity.
- Fake text messages – criminals send people a message via text or WhatsApp telling them there has been suspicious activity on their account and they must reply with their account number and PIN code.

Bullying or harassing others

Online bullying has proliferated with the anonymity provided by the Internet, but the distress caused by this type of bullying can be long lasting and devastating. While cyberbullying itself is not a crime, if an individual engages in bullying online, they may be prosecuted under a range of acts, including:

- Protection from Harassment Act 1997 – makes it a criminal offence to harass another person, e.g., sending abusive emails.
- Communications Act 2003 – makes it a criminal offence to send via any electronic communication network a message or other content deemed to be offensive, indecent, obscene, or menacing.

Creating and uploading inappropriate material

The content of inappropriate material varies by audience; what is inappropriate for a child may very well not be inappropriate for an adult. However, there is content that is inappropriate for everyone, no matter what age they are. This includes:

- photographs and videos that show child abuse, violence, or cruelty
- photographs and videos that glorify and promote terrorist acts
- material that includes sexual content
- material that encourages criminal activity

Providing misleading information

Providing false or misleading information amounts to fraud, which is governed by the Fraud Act 2006. The maximum penalty for fraud is 10 years' imprisonment.

Harvesting personal information

Some people deliberately seek others out so that they can steal valuable information from them, by posing as someone of a similar age to the person they are stealing the information from, or as someone who has a shared interest.

Bullying, harassment or stalking

Bullying and harassment can be prosecuted under the Protection from Harassment Act 1997 and for victims, it can lead to depression, anxiety, self-harm, and withdrawal from social interactions. Cyberstalking is where a person inundates another person with unwanted messages or unwanted attention. It is illegal under the Protection of Freedoms Act 2012 and became a crime in 2012. There is a National Stalking Helpline for victims: 0808 802 0300.

Grooming

Victims are identified because they are young and/or vulnerable and the perpetrators use a mixture of flattery, threats, and gifts to encourage individuals to send indecent images of themselves or to meet up in person, where they may be sexually or physically abused. Online content includes blog posts, social media posts, publications, photographs, and videos.

Consequences of breach

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

- Restrict or terminate a user's right to use Reed Business School 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.
- If Reed Business School suspects criminal offences have occurred, the police will be informed.

Any disciplinary action, arising from breach of this policy, shall be taken in accordance with Reed Business School's Disciplinary Policy. Disciplinary action may ultimately lead to dismissal.

Protection of personal data

Reed Business School holds and processes information about employees, students, and other data subjects for academic, administrative, and commercial purposes. When handling such information, Reed Business School, and all staff or others who process or use any personal information, must comply with the Data Protection Principles which are set out in the Data Protection Act 2018 (the 2018 Act). Responsibilities under the 2018 Act are set out in the Data Protection Policy.

When managing personal data, Reed Business School will consider:

- taking care not to share contact details when emailing multiple people
- being careful when sharing usernames and other personal data for access to online resources
- providing access to Reed Business School data systems safely
- providing or making available sufficient information about the personal data captured during lesson recordings, particularly where cameras are switched on.

Staying safe online

The increasing use of the internet and digital technology has presented huge opportunities, for apprentices and students. However, apprentices and students can access and engage with online content in many ways, so they need to have the skills to be able to use the internet safely and develop appropriate online behaviours.

It is paramount that apprentices, students, and staff are aware of ways in which they can protect themselves online and ensure the security of their personal data. Dangers can include bullying and abuse, revenge porn, grooming, identity theft, and viruses. Students, Apprentices, and staff need to examine and appraise the validity and authenticity of information online.

The role of Reed Business School

- Assess how apprentices may be at risk of harm using the internet or technology.
- Provide relevant training for apprentices so that they can work safely and effectively online.
- Help apprentices to develop an objective attitude to online information and evaluate its authenticity.
- Make sure staff are trained to identify and deal with concerns about online safety.
- Provide clear guidance on what is and is not an acceptable use of the internet.
- Ensure effective filtering and monitoring systems are in place.
- Exploring online safety principles as part of an embedded and progressive curriculum and reinforcing safe behaviour whenever technology is used.
- Creating a safe environment where learners feel comfortable to report concerns and say what they feel, without fear of getting into trouble and/or be judged for talking about something which happened to them online.
- Involving the Designated Safeguarding Lead (DSL) when needed.
- Report any filtering breaches (such as access to illegal, inappropriate, or harmful material) to the DSL in line with Reed Business School Safeguarding and Prevent Policy.
- Respect copyright and intellectual property rights; and students and staff will obtain appropriate permission to use content, and if videos, images, text, or music are protected.

Wi-Fi acceptable use policy

As a professional organisation with responsibility for safeguarding it is important that all apprentices, learners, visitors, co-members, and others are fully aware of the school boundaries and requirements when using Reed Business School's Wi-Fi systems and take all possible and necessary measures to protect data and information systems from infection, unauthorised access, damage, loss, abuse and theft.

Reed Business School provides Wi-Fi for the business school community and allows access for educational purposes. Reed Business School will not be liable for any damages or claims of any kind arising from the use of the wireless service. Reed Business School takes no responsibility for the security, safety, theft, insurance, and ownership of any device used within the premises that is not the property of Reed Business School. All apprentices, learners, visitors, co-members, and others will take all practical steps necessary to make sure that any equipment connected to the Wi-Fi service is adequately secure, such as up-to-date anti-virus software, systems updates.

Reed Business School owned information systems, including Wi-Fi, must be used lawfully. The Computer Misuse Act 1990 makes the following criminal offences:

- to gain unauthorised access to computer material
- to gain unauthorised access to computer material with intent to commit or facilitate commission of further offences or to modify computer material without authorisation

Filtering and monitoring

Reed Business School has filtering and monitoring in place through ScoutDNS that is appropriate for our apprentices, students, and staff to use. Technology exists to block illegal content (e.g., Internet Watch Foundation blacklist) and other 'harmful' content including but is not limited to:

- Protection of access to terrorist material or materials that might lead into terrorism (as defined in the Counter Terrorism and Securities Act 2015). Also, directly, and actively participate in the CITRU list program, with regular updates.
- Protection of access to Adult content
- Protection of access to Child Sexual Abuse content

The main online safety risks in 2022/2023

Online-safety risks are traditionally categorised as one of the 4 Cs:

- Content
- Contact
- Conduct
- Commerce (section 135 of KCSIE 2022)

They do not stand in isolation, and it is important to understand the interplay between all categories. This is evident in Ofcom's Media and Attitudes Report 2022 which suggests 36% of children aged 8-17 had seen something 'worrying or nasty' online in the past 12 months, with 84% experiencing bullying via text or messaging, on social media, in online games, through phone or video calls, or via other apps and sites.

Potential signs that may be cause for concern include:

- being withdrawn
- being secretive
- depression
- taking dangerous risks
- abusing alcohol or drugs
- spending a lot of time, or much more or less time, online, texting, gaming, or using social media
- not doing well at work or school/ college
- in children, soiled clothes, or bed-wetting
- unexplained physical injuries
- being nervous
- losing confidence

Behavioural changes that may be cause for concern include:

- an inability to sleep
- regularly having nightmares
- self-harm
- missing work or school or showing an unwillingness to go
- aggressive behaviour
- obsessive behaviour
- suddenly being "ill" every day before school/college or work

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