Purpose

To define John Rowan and Partners policy regarding IT & Data Security. This document replaces all previous IT & Data Security Policies.

Scope

The policy covers all aspects of IT & Data Security for John Rowan and Partners.

Responsibility

The Managing Partner has overall responsibility for the effectiveness of this process.

This policy applies to all employees, contractors, consultants and authorised users. Policy breaches may lead to disciplinary and/or legal action.

IT & Data Security Policy

Policy Prepared by: Dilbagh Virdee – IT consultant
Policy Approved by: Gurpal Virdee – Managing Partner
Last Review Date: 29/10/2018

CONTENTS

1.0	Context and Overview	2
2.0	People, Risks and Responsibilities	3
3.0	General Employee Guidelines	4
4.0	Working with Data	5
5.0	Software and Cloud Services	7
6.0	World Wide Web Usage	8
7.0	Email	9
8.0	Personal Use of Business Telephones	10
9.0	Use of Personal Devices for Business	12
10.0	Social Networking	15
11.0	Disposal of Electrical Equipment	16
12.0	Internet Access from Homes, Mobile Devices and Public Wi-Fi	17
13.0	End of Employment	17
14.0	Policy Non-Compliance	17
15.0	Policy Agreement	18

1.0 Context and Overview

1.1 Introduction

As we move more and more into a digital age, so more and more of our personal data is stored and can be accessed electronically. However, much of that data contains confidential and personal information and so there is a responsibility on the part of individuals and organisations to make sure that data is protected and that appropriately diligent processes and procedures are put in place to ensure that access to data is restricted.

As a business, we have a responsibility to ensure that we have appropriate policies, procedures and processes in place to ensure that we are storing and processing data in a responsible manner. Likewise, as an employee of John Rowan and Partners, you will inevitably come into contact with personal data of some form or other as part of your normal duties – whether it is held electronically or on hardcopy (i.e. printed onto paper). As such, you too have a responsibility to ensure that the data you do come into contact with, and the technologies you use to interact with that data, are used in a way that is both secure and for the appropriate reasons.

Having considered our responsibilities as an organisation, this policy is intended to set out how personal data is to be handled, and how to use the equipment which interacts with that data, so as to comply with our legal and security responsibilities and requirements.

This document supersedes any previously published IT and Data Security Policy and should be read in conjunction with John Rowan and Partners' Employee Handbook. If there are any conflicts between this policy and the handbook, this policy will prevail. This policy does not form part of any employee's contract of employment and may be amended by the Company at any time.

1.2 Why this policy exists

This security policy ensures John Rowan and Partners:

- Complies with data protection law and follows good practice
- Protects the rights of our people, customers and business partners
- Is open about how it stores and processes individuals' data
- Protects itself from the risks of a data breach
- Complies with software licensing requirements

1.3 Data Protection Law

A variety of data protection legislation both UK and EU governs how organisations – including John Rowan and Partners – must collect, handle, store and delete personal data whether in an on-line or physical environment. Personal Data means data relating to a living individual who can be identified (directly or indirectly) from that data (or from that data and other information in the Company's possession). Personal data can be factual (for example, a name, address or date of birth) or it can be an opinion about that person, their actions and behaviour.

All automated and computerised personal data (such as IP addresses and mobile phone numbers) are covered as well as data on paper or held on any other media (for example video, pictures), where that personal data is to be processed wholly or partly by automated means, or it forms part of a filing system (or is intended to be).

As a general rule personal information must be collected and used fairly, stored safely and not disclosed unlawfully.

The EU General Data Protection Regulation (GDPR) is the principal legislation governing the collection use and processing of personal data. It applies to all companies controlling or processing personal data of individuals within the EU, irrespective of where in the world that actual control or processing takes place.

The GDPR is underpinned by six important principles. These are that personal data must:

- Be processed transparently, fairly and lawfully;
- Be obtained only for a specified, explicit and, legitimate purpose;
- Be adequate, relevant and limited to only that data that is necessary in relation to the purpose for which it is being processed;
- Be accurate and (as necessary) kept up to date;
- Not be kept for any longer than necessary (to fulfill the purpose for which it was obtained);
- Be kept in a manner that ensures appropriate security of the personal data, including protection against unauthorized or unlawful processing and against accidental loss, destruction or damage.

The company is responsible for a 'seventh` principle – ensuring compliance with the six principles and for being able to demonstrate compliance.

2.0 People, Risks and Responsibilities

2.1 Policy Scope

This policy applies to:

- The Head Office in Ealing and any satellite offices;
- All employees (permanent and casual) and volunteers of John Rowan and Partners located at these various premises or using mobile access points;
- All workers, contractors, suppliers and other people working on behalf of John Rowan and Partners.

It applies to all data that the company holds relating to identifiable individuals, contractors, suppliers, employees, or indeed the company itself, even if that information technically falls outside of the GDPR or other relevant legislation. This typically includes anything that can be used to identify an individual, such as:

- Names of individuals
- Postal addresses
- Email addresses
- Telephone numbers
- Business performance reports
- Supplier purchase orders
- Any other information relating to individuals, contractors, and suppliers to John Rowan and Partners.

2.2 Data Protection Risks

This policy helps to protect John Rowan and Partners from some very real data security risks, including:

- **Breaches of confidentiality: for example where** information is being given out inappropriately.
- **Failing to offer choice: for example,** all customers must be given a choice as to whether they receive marketing information from John Rowan and Partners or not.
- **Reputational damage: for example**, the company may suffer damage to its reputation if hackers successfully gained access to sensitive data.
- **Loss of business with clients –** due to actual or perceived issues with data, particularly to assure their Data Protection requirements.

2.3 Responsibilities

Everyone who works for or with John Rowan and Partners has a responsibility for ensuring data is collected, stored and handled appropriately.

Each person that handles personal data must ensure that it is handled and processed in line with this policy and data protection principles.

All employees have a responsibility to keep the company updated in relation to their own personal data e.g. change of address, marital status, dependents etc.

By accepting employment you are expressly agreeing to comply with this policy when handling personal data during your employment including any personal data relating to any employee, customer, client, supplier or agent of the company.

3.0 General Employee Guidelines

In order to comply with the eight data protection principles, employees should adhere to the following guidelines:-

- Employees should keep all data secure, by taking sensible precautions and following these guidelines and policies;
- You should only access and use personal data where it is necessary to do so for your work; Data **should not be shared informally** (i.e. there must be a valid legal or business reason for sharing the information);
- **Strong passwords must be used.** Your password should be at least 8 characters in length and contain a combination of upper case characters, lower case characters, numbers, and non-alphanumeric characters. **You should not share your password with any person either inside or outside of John Rowan and Partners** (including IT support staff, colleagues, managers, controllers or directors of the business). This includes any passwords for authorisation to any of our systems;
- Personal data **should not be disclosed** to unauthorised people, either within the company or externally;
- Data should be **regularly reviewed and updated** if it is found to be out of date;
- **If data is no longer required, it should be deleted and disposed of;**
- Employees **should request help** from their line manager or the Data Protection Officer if they are unsure about any aspect of data protection;

- **Computers must not be left logged in and unattended.** When you move away from your computer, you must either lock the computer or log out of your account. All John Rowan and Partners' computers are set to lockout after 60 minutes of inactivity and it is your responsibility to ensure all workstation are secure from data leakage (non-authorised access to data).

4.0 Working with Data

4.1 Data Storage

These rules describe how and where data should be safely stored. Questions about storing data safely can be directed to the Office Manager and/or IT service provider (Esteem Services).

When data is stored on paper, it should be kept in a secure place where unauthorised people cannot see it.

These guidelines also apply to data that is usually stored electronically but has been printed out for some reason (such as copies of emails):

- When not required, the paper or files should be kept **in a locked drawer or filing cabinet.**
- Employees should make sure paper and printouts **are not left where unauthorised people could see them**, like on a printer.
- **Data printouts should be shredded** and disposed of securely when no longer required.

When data is **stored electronically**, it must be protected from unauthorised access, accidental deletion and malicious hacking attempts:

- Data should be **protected by strong passwords** that are changed regularly and never shared between employees.
- If data is stored on **removable media (like CD, DVD, USB hard drive or flash drive),** these should be kept locked away securely when not being used. Where possible encrypted removable drives must be used at all times. All employees are entitled to use removal media and have the responsibility to ensure this remains secure.
- Data stored on laptops should be backed up to either an external hard drive (not kept in the same bag as the laptop) or synchronised to the company's network drive.
- Data should only be stored on **designated drives and servers**, and should only be uploaded to **secure company file storage system.**
- **Personal data relating to customers of the business must only be stored in JRP Docs.** Personal data relating to customers is not to be held outside of JRP Docs. This includes emails held in Outlook, data within Microsoft Office documents, data files, scanned documents or photography. Emails must be copied to JRP Docs. Call recordings must remain held within the horizon call recording system unless needed for legal purposes. Printed records from all IT systems must not be taken unless strictly necessary for the fulfilment of a business purpose, retained in a locked facility and securely destroyed when no longer necessary.

4.2 Data Use

Personal data is of no value to any business unless that business can make use of it. However it is when personal data is accessed and used that it can be at the greatest risk of loss, corruption or theft:

- Personal data **must not be shared informally** (i.e. there must be a valid legal or business reason for sharing information).

- Personal data must be **encrypted before being transferred electronically to a third party outside of John Rowan and Partners (e.g. by email)**. Emails are not encrypted by default and therefore, John Rowan and Partners doesn't permit the use of this communication for personal data transfer. The Office Manager or the IT service provider can explain how to send data to authorised external contacts using encryption but the preferred channels is JRP Docs.
- Personal data must not be disclosed to any third party that is not authorised to receive such data and that third party must be made aware of the personal nature of the data and have agreed to maintain the same level of confidentiality and security of the data as John Rowan and Partners. If in doubt, speak to your line manager or contact the Office Manager or the IT Consultant.
- Employees **must not save copies of personal data to their own computers or other electronic devices**. Always access and update the central copy of any data.
- **Data must only be accessed to fulfil a business reason**, and only by employees who need to carry out that reason and have the authority to do so.
- **Employees must ensure that nobody else can see their screens when working with personal data** (especially client sensitive data). Be wary of members of the public using camera phones to take pictures of your screens when working of site.
- **Employees must ensure that nobody else can hear confidential telephone calls or dictations unless authorised to do so using the call recording system when collecting or using personal data. The retention period is set to 30 days and is automatically disposed and not retrievable after**.

4.3 Data Accuracy

The law requires that we take reasonable steps to ensure data is kept accurate and up to date. It is therefore the responsibility of all employees who work with data to take reasonable steps to ensure it is kept as accurate and up to date as possible.

- Data should be held in **as few places as necessary,** so we should not create any unnecessary additional data sets.
- Employees should **take every opportunity to ensure data is being updated.** For example, by asking a client to confirm their details when they call.
- Employees should ensure that they verify the identity of the client and that they do not give out personal data to the client.
- John Rowan and Partners will make it easy for data subjects (individuals who the data is about) to update the information John Rowan and Partners holds about them (e.g. via the company website).
- Data should be **updated if/when inaccuracies are discovered (e.g.** if a client can no longer be reached on their recorded telephone number, it should be removed from the database.

In particular, customer email addresses must be recorded accurately in all systems. Incorrect email addresses will result in personal data being sent to the wrong person, contravening the legislation and regulations and placing the business at risk of prosecution.

The accurate collection of email addresses is very important to us for future cost-effective communication (with the appropriate level of permission) so we should always endeavour to obtain the email address. However, in the event that a customer's email address is not known, simply use the 'None' button to record the fact that the customer has no email address.

4.4 Subject Access Requests

All individuals who are the subject of personal data held by John Rowan and Partners are entitled to:

- Ask what information the company holds about them and why.
- Ask where the data has been, or will be, disclosed;
- Ask how long the data will be stored (or the criteria used to determine the retention period);
- To request rectification, erasure, or to object to its processing or require its restriction;
- To be informed of their right to lodge a complaint with the supervisory authority (the Information Commissioner's Office in the UK);
- The source of the personal data if it wasn't collected directly from them;
- Whether their data is used for automated profiling;
- Request the portability of the data (if obtained relying on consent or contract); and
- Who to contact in relation to the above

If an individual contacts the company requesting this information, this is called a **Subject Access Request.**

Subject Access Requests from individuals should be made in writing and should always be passed to the Data Protection Officer at John Rowan and Partners for administration.

Once we have verified the identity of anyone making a subject access request, the necessary information will be provided in a format that is consistent with our legal obligations.

4.5 Disclosing Data for Any Other Reason

In certain circumstances, the law and regulations allows personal data to be disclosed to law enforcement agencies without the consent of the data subject.

Under these circumstances, we will disclose requested data. However, the John Rowan and Partners Data Protection Officer will ensure the request is legitimate, seeking assistance from the Partners and from the company's legal advisors where necessary.

5.0 Software and Cloud Services

To protect personal and business data, and to comply with software licensing / anti-piracy legislation, the following rules are to be adhered to:

- **The IT service provider will provide all software for all John Rowan and Partners desktop and laptop computers**. As a user of laptops and desktop computers provided by the company, you are not permitted to use any software that has not been provided by the Managed Services Organisation.
- **Only "cloud" services authorised by the IT service provider may be used within the business.** This includes email services, online storage services and team collaboration services. No cloud services may be used without the consent of the IT Consultant.
- If you have been permitted to use mobile devices (phones and tablets) and personal computers for business purposes, **the Office Manager will provide you with authorised software for your devices that have been vetted for data security**. Ownership of these applications and the data stored within them will stay with John Rowan and Partners

regardless of the ownership of the device and the business can rescind the use of this software at any time.

- **Any user accounts created on cloud services must be unique to an individual rather than generic logins and passwords that are used by multiple people.** Account logins and passwords must not be shared.

6.0 World Wide Web Usage

John Rowan and Partners provides World Wide Web access to employees for both business and personal use from within the company's enterprise network and guest Wi-Fi networks. Access is provided at the discretion of the company and is not a contracted benefit associated with employment.

All user activity on the World Wide Web is recorded for management, security and legal purposes. These logs can be interrogated to identify areas of misuse, abuse or illegal activities. Access to these logs are only available directly to the Office Manager and Managing Partner via the IT service provider, extracts of these logs can be made on request by John Rowan and Partners line management, Directors or law enforcement agencies.

Whereas the company takes every measure to ensure access to the World Wide Web is safe and secure through the use of web filters, firewalls and end-point protection software, it is the responsibility of the user accessing the World Wide Web to make every effort to avoid the following activities:

- Accessing web sites or services providing illegal or pornographic materials
- Soliciting or advertising for illegal or pornographic services / materials
- Accessing web sites providing gaming or gambling services
- Downloading any software onto your computer, phone or tablet that may contain viruses, malware, spyware or adware (if in doubt, contact the IT service provider and/or the Office Manager)
- Downloading any software onto your computer, phone or tablet that requires licensing (be aware that a large number of software applications advertised as free are only free for personal use and not with businesses such as John Rowan and Partners)

Access to the World Wide Web for non-business reasons is done so under an understanding of "reasonable use", and we trust you to behave responsibly. The Company monitors all use of its computer systems including use of the World Wide Wed. Examples of unreasonable use are:

- Excessive use of the internet for personal matters (whether you access the internet using our IT systems or via your own personal device). Personal use of the internet which interferes with your ability to properly perform your duties will be considered excessive. In any event, personal use of more than 2 hours a day during office hours is unacceptable;
- Streaming videos or downloading/uploading large files using our Internet access/systems. We will monitor this by looking at bandwidth utilisation;
- Using gaming or gambling services; and
- Accessing Illegal or adult materials (illegal activities will be forwarded to law enforcement agencies).

The above list is not exhaustive. Unreasonable use of the internet may result in disciplinary action being taken against you up to and including dismissal (depending on the severity of your actions).

7.0 Email

Use of email by employees of John Rowan and Partners is permitted and encouraged where such use supports the goals and objectives of the business. **On the whole, our email system should be used for business purposes only**. However, we acknowledge that there may be times where employees use emails for personal reasons, but these should be kept to a minimum and should not interfere with an employee's work.

Employees must ensure that they:

- Comply with current legislation
- Use email in an acceptable way
- Must not forward business emails to personal accounts
- Do not create unnecessary business risk to the company by their misuse of email
- **Do not open files attached to emails if the sender is unknown to the recipient** (the majority of network security breaches are the result of the opening of email attachments containing viruses)

Email messages may be disclosed in legal proceedings in the same way as paper documents. Deletion from a user's inbox or archives does not mean that an email cannot be recovered for the purposes of disclosure. All email messages should be treated as potentially retrievable, either from the main server or using specialist software.

7.1 Unacceptable behaviour

The following behaviour by an employee is considered unacceptable:

- Use of company emails systems to send chain letters
- Forwarding of company confidential messages to external recipients or personal mailboxes
- Distributing, disseminating or storing images, text or materials that might be considered indecent, pornographic, obscene or illegal or which could contravene our Code of Conduct
- Distributing, disseminating or storing images, text or materials that might be considered discriminatory, offensive or abusive, in that the context is a personal attack, sexist, rude or racist, or might be considered as harassment
- Accessing copyrighted information in a way that violates the copyright
- Accessing unauthorised mailboxes without the owner's consent
- Impersonating another individual, or amending messages received to change what the original sender has said
- Transmitting unsolicited commercial or advertising material
- Undertaking deliberate activities that waste staff effort or networked resources
- Introducing any form of computer virus or malware into the corporate network

This list is not exhaustive and the company will review individuals behaviour in the specific and relevant circumstances to determine the acceptability or otherwise of an individual's use of company technology, equipment, network or data and its acts (or omissions) related thereto.

7.2 Monitoring

John Rowan and Partners accepts that the use of email is a valuable business tool. However, misuse of this facility can have a negative impact upon employee productivity and the reputation of the business.

In addition, all of the company's email resources are provided for business purposes. Therefore, the company maintains the right to examine any systems and inspect any data recorded in those systems.

To ensure compliance with this policy, the company also reserves the right to use monitoring software in order to check upon the use and content of emails.

Employees should not have any expectation of privacy when using the company's emails for personal use or when using the company's computer systems to access personal email accounts.

8.0 Personal Use of Business Telephones

Mobile phones also are provided to all employees deemed to require them based on demonstrated need and job function or to enhance company efficiency and provide safety and/or security.

Mobile phones issued to staff remain the property of John Rowan and Partners unless otherwise advised by the business.

John Rowan and Partners supplied mobile phones, like other means of communication, are to be used to support company business. Employees may use John Rowan and Partners supplied mobile phones to communicate with others inside and outside of the company when such communications are related to legitimate company activities and are within their job assignments or responsibilities. All communications using John Rowan and Partners supplied mobile phones – verbal, written or other – must meet professional standards of conduct. Employees may use John Rowan and Partners supplied mobile phones for any legitimate safety, security or emergency purposes. Employees shall not use John Rowan and Partners supplied mobile phones for illegal, disruptive, unethical or unprofessional activities, or for personal gain, or for any purpose that would jeopardize the legitimate interests of the company.

Mobile phones can be a distraction in the workplace. To ensure the effectiveness of meetings, employees are asked to turn their phones off, or at a minimum to 'vibrate' mode. Typically, each call from a mobile phone incurs a cost, while land-line calls do not. Employees are encouraged to use land-line phones when they are available. Employees should be aware that mobile phone conversations are not secure and can on occasions be picked up on radio receivers or conversations more easily overheard if used in communal or public areas. Employees should use discretion in discussing highly sensitive or confidential matters on the cell phone. No employee may use another employee's cell phone without that person's prior permission.

When installing applications on mobile phones, only official stores are used e.g. App Store, Google Play, etc once approved by the business. Installing free applications for business purposes is allowed with consent from the Office Manager or the IT Service Provider. Apps that incur additional costs to the monthly rental will be passed to the end user. Use of unlicensed software is illegal and puts John Rowan and Partners at significant legal risk. Users are specifically prohibited from changing security settings or amending configuration files on mobile phone issued to them. This includes disabling passwords, pin codes and any installed security programs.

John Rowan and Partners mobile phone contract allows for unlimited UK minutes (01,02 and 03 numbers) and unlimited UK text messages without any additional cost. Call to 08 numbers are chargeable therefore, should be made through the desk phone to reduce additional cost to the business. Data roaming charges from abroad can result in very high-level charges, and if it is found from the monthly billing that these have been incurred due to personal use or negligence on the part

of the user, then the charges may be passed onto the user. Consequently, users should ensure their mobile phone is connected to a Wi-Fi network whenever possible and then to use application in the like of WhatsApp or Skype to make phone calls abroad.

John Rowan and Partners receives itemised billing for all company mobile phones and this is monitored monthly. If it is found the mobile has been misused, or additional costs have incurred, John Rowan and Partners may, after investigation, act to recover the costs.

Employees are responsible for the safekeeping and condition of the mobile phone always, and will be responsible for the cost of any repair or replacement (other than fair wear and tear). Apart from the financial cost associated with replacing a stolen mobile phone there may be other associated hidden costs. These include loss of productivity, data replacement, increased insurance premiums and so on. To prevent the theft of mobile phones and confidential information or personal data, all John Rowan and Partners mobile phone users must ensure mobile phones are not be left in full view even for a short period of time and never be left unattended.

Mobile devices contain confidential information and the personal data in multiple applications, including diaries, contacts and email. Employees, contractors and third parties using a John Rowan and Partners mobile device shall not disclose, share, transfer (by any means) or allow the unauthorized access, sharing, disclosure or transfer (by any means) of that information or data without the prior permission of John Rowan and Partners.

If a mobile phone is stolen, the user must notify the police and / or any other appropriate authority. It is the user's responsibility to obtain a crime incident/ reference number and to inform both their line manager and the IT Service Provider, as soon as possible after the event.

Employees whose job responsibilities include driving and who must use a mobile phone for business use, are expected to refrain from using their phone while driving. Allow voice mail or your passenger to handle calls when possible. Safety must come before all other concerns. Regardless of the circumstances, including slow or stopped traffic, employees are strongly encouraged to pull off to the side of the road and safely stop the vehicle before placing or accepting a call.

In situations where employees drive and accept phone calls, UK law, as well as this policy, require the use of "hands-free" equipment. Under no circumstances are employees allowed to place themselves at risk to fulfil business needs. Employees who are charged with traffic violations resulting from the use of their phone while driving will be solely responsible for all liabilities that result from such actions. Violations of this policy will be subject to discipline, including dismissal. Employees are encouraged to check and return calls at safe opportunities (during a rest stop, before leaving, upon arrival).

Employees, contractor or third party are prohibited from using any of their personal mobile devices including laptops, mobiles, tablets, watches to access any of John Rowan and Partners' data without written consent granting appropriate access from the Office Manager or the IT Consultant.

Upon leaving employment or changing to a new role where the mobile phone is no longer required, the member of staff must return the mobile phone or devices to their Line Manager including all accessories.

VIOLATIONS AND PENALTIES

You are liable for any misappropriation of your John Rowan and Partners supplied mobile device or devices.
Violation of this policy may result in disciplinary action and potential dismissal.

John Rowan and Partners makes extensive use of telephony equipment as part of the day to day running of the business. You are permitted to use these facilities for **essential** personal calls, but on the explicit understanding that any calls you make from a business phone regardless of whether the call is of a business or personal nature, can be traced back to John Rowan and Partners and as such you must ensure that the nature, content and language used in a personal telephone call is in keeping with that used in a business call.

You should be aware that personal use of our telephone systems may be monitored and disciplinary action may be taken where there are breaches of any of our policies (including for example our policies relating to Equal Opportunities and Dignity at Work), not just this policy. John Rowan and Partners reserves the right to prevent or restrict access to certain telephone numbers if we consider personal use to be excessive.

In using the company's telephone systems for personal calls, you must adhere to the following:

- **No international calls**
- **No premium rate telephone** numbers (telephone numbers beginning with 09, 070, 0871, 0872, 0873)
- **No calls to directory enquiries** (telephone numbers beginning with 118) – Use web sites such as www.yell.co.uk to find numbers
- **Don't use business telephones for social calls** (e.g. having a catch-up with friends or family). Ensure that if you need to use a business telephone, it's for an explicit reason (e.g. booking a doctor's appointment, calling your child's school).

9.0 Use of Personal Devices for Business

John Rowan and Partners will provide their staff with business devices but often under agreement will allow the use of personal devices including (home computers, mobile phones and tablet devices) for users who have obtained explicit authorisation from the Office Manager or the IT Consultant to do so.

When you access our systems you may be able to access data about us, our customers, clients, distributors, suppliers and other business connections, including information which is confidential, proprietary or private (company data).

Therefore, we are exposed to a number of risks, including from the loss or theft of the device (which could result in unauthorised access to our systems or company data), the threat of malware (such as viruses, worms, spyware, Trojans or other threats that could be introduced into our systems via a device) and the loss or unauthorised alteration of company data (including personal and confidential information which could expose us to the risk of non-compliance with legal obligations of confidentiality, data protection and privacy). Such risks could result in damage to our systems, our business and our reputation.

John Rowan and Partners must protect its systems and company data, and prevent company data from being deliberately or inadvertently lost, disclosed or altered, while enabling you to access our systems using a device for the purposes of your employment and the business.

Breach of this policy may lead to us revoking your access to our systems, whether through a device or otherwise. It may also result in disciplinary action up to and including dismissal and in the case of a breach of this policy by a contractor, consultant, casual or agency worker, the termination of the engagement. It may also lead in some cases to possible criminal charges. Disciplinary action may be

taken whether the breach is committed during or outside office hours and whether or not the use of the device takes place at your normal place of work. You are required to co-operate with any investigation into suspected breach, which may involve providing us with access to the device and any relevant passwords and login details.

9.1 Acceptable Use

- The company defines acceptable business use as activities that directly or indirectly support the business of John Rowan and Partners.
- **Personal Devices are not to be connected to the John Rowan and Partners corporate network** (including enterprise Wi-Fi). You must use your own Internet connectivity (3G / 4G / GPRS / Home Wi-Fi) with Cato VPN software to connect your device to the company network.
- You may not use your personal devices' camera to take photos or video either on business premises or when participating in activities on behalf of the business (most mobile devices use cloud backups of pictures and videos which cannot be secured by John Rowan and Partners).
- Devices may not be used at any time to:
  - Store or transmit illicit materials
  - Store or transmit proprietary information belonging to another company
  - Harass others
  - Engage in outside business activities
  - Engage in illegal activities
- **Users may only store business data on Microsoft OneDrive, JRP Docs and Network Drives as appropriate**. Business data is not to be saved to your personal device's storage, or any other storage facility / service (including Dropbox, Google Drive, Apple iCloud or personal Microsoft OneDrive account)
- **John Rowan and Partners has a zero-tolerance policy for texting or emailing while driving, and only hands-free talking while driving is permitted in line with current legislation.**

9.2 Security

If you are authorised to use your personal device to connect to our computer systems, you must:-

- Use your best efforts to physically secure the device against loss, theft or use by persons who we have not authorised to use the device. This includes, but is not limited to, setting passwords, making sure that the device is not left in the possession of a third party, etc;
- Protect the device with a pin number or password, and keep that pin number or password secure at all times. The pin number or password should be changed regularly. If the confidentiality of a pin number or password is compromised, you must change it immediately. The use of pin numbers and passwords should not create an expectation of privacy by you in the device;
- **Ensure that you have appropriate anti-virus and firewall protection for your personal devices** (excluding Apple iPads and iPhones). For paid anti-virus and firewall software, you must ensure your subscription is active and that you are receiving regular updates for this software;
- Not use an Android, Apple iOS or Windows Phone device that has been "jail broken" or "rooted" (where the security restrictions have been removed to allow apps to run that would otherwise be blocked as a security risk);
- **Set the device to automatically lock after 5 minutes of inactivity;**

- Ensure that any apps loaded on your mobile device (Android, Apple iOS or Windows Phone) are not "side loaded" onto the device (i.e. using a personal computer to load software onto the device). Any apps installed on your devices must be downloaded from the Apple App Store, Android Play or Windows Store.

9.3 Devices and Support

- Whereas the IT service provider will assist you with connectivity issues with your personal device, **you will need to arrange your own support for any other problem in regards to hardware, operating system or software.**
- Devices must be presented to IT service provider for proper provisioning and configuration of standard apps, such as browsers, office productivity software and security tools, before they can be used for business purposes.
- In connecting your device to the company's systems, John Rowan and Partners will take control of elements of your device (e.g. forcing a 4 digit unlock code onto your device).
- Employees, contractor or third party are prohibited from using any of their personal mobile devices including laptops, mobiles, tablets, watches, etc to access any of John Rowan and Partners' data without consent from the business in writing.
- **Your personal device may be remotely wiped or rendered inoperable** if 1) the device is lost, 2) the employee terminates his or her employment and we have a reasonable belief that the Employee has retained Confidential Information or company data and fails to present the device to the IT service provider promptly when requested, 3) IT detects a data or policy breach, a virus or similar threat to the security of the company's data and technology infrastructure.
- **John Rowan and Partners does not accept any liability or responsibility for your own personal data stored on your device, or the repair of any personal device**. It is your responsibility to ensure your personal data is backed up. Personal devices are used at your own risk.
- John Rowan and Partners reserves the right to disconnect devices or services without notification.
- Lost or stolen devices must be reported to your line manager and the IT service provider within 24 hours.
- Owing to their heightened risk of data interception, personal devices used for business purposes must not be connected to public Wi-Fi hotspots.

9.4 Monitoring

The contents of our systems and company data are our property. All materials, data, communications and information, including but not limited to e-mail (both outgoing and incoming), telephone conversations and voicemail recordings, instant messages and internet and social media postings and activities, created on, transmitted to, received or printed from, or stored or recorded on a device (collectively referred to as content in this policy) during the course of business or on our behalf is our property, regardless of who owns the device.

We reserve the right to monitor, intercept, review and erase, without further notice, all content on the device that has been created for us or on our behalf. This might include, without limitation, the monitoring, interception, accessing, recording, disclosing, inspecting, reviewing, retrieving and printing of transactions, messages, communications, postings, log-ins, recordings and other uses of the device as well as keystroke capturing and other network monitoring technologies, whether or not the device is in your possession.

It is possible that personal data may be inadvertently monitored, intercepted, reviewed or erased. Therefore you should have no expectation of privacy in any data on the device. Staff are advised not to use our systems for any matter intended to be kept private or confidential.

Monitoring, intercepting, reviewing or erasing of content will only be carried out to the extent permitted by law, for legitimate business purposes, including, without limitation, in order to:

a) prevent misuse of the device and protect company data;
b) ensure compliance with our rules, standards of conduct and policies in force from time to time (including this policy);
c) legal compliance;
d) monitor performance at work; and
e) ensure that staff members do not use our facilities or systems for any unlawful purposes or activities that may damage our business or reputation.

We may also store copies of any content for a period of time after they are created and may delete such copies from time to time without notice. We may obtain and disclose copies of such content or of the entire device (including personal content) for litigation or investigations.

By opting to use your personal device to connect to our business systems and by signing the declaration at the end of this policy, you confirm your agreement (without further notice or permission) to such monitoring and to our right to copy, erase or remotely wipe the entire device (including any personal data stored on the device). You also agree that you use the device at your own risk and that we will not be responsible for any losses, damages or liability arising out of its use, including any loss, corruption or misuse of any content or loss of access to or misuse of any device, its software or its functionality.

10.0 Social Networking

The purpose of John Rowan and Partners social networking policy is to allow the company to take advantage of social media's business benefits and promote its products/services, contribute to the relevant online dialog, and better engage with customers and prospects, while avoiding the significant risks involved.

John Rowan and Partners provides a private social network using Microsoft Teams. This network may be used to engage with team members on business and social matters as the network is not open to public access. The IT service provider can provide users of Microsoft Office access to this network upon request.

Outside of John Rowan and Partners' Teams network, you may not use any other social media to collaborate with colleagues for business reasons (e.g. arranging meetings through Facebook, discussing services).

Occasional use of social media during work hours is permitted so long as it does not involve unprofessional or inappropriate content, does not interfere with your employment duties and productivity, and complies with this policy.

When using any social media, be it under business accounts or personal accounts, Employees must abide by the following:

- Employees are forbidden from using social networks to post or display comments about co-workers, managers, controllers, directors or John Rowan and Partners that may be considered to be offensive, vulgar, obscene, threatening, harassing, rude, or a violation of John Rowan and Partners policies on equality at work, discrimination or harassment.

- Employees must not disclose any confidential or proprietary information about John Rowan and Partners, our business, employees, customers or business partners.
- Unless specifically authorised to do so, employees are not permitted to express opinions on behalf of John Rowan and Partners via social media. You should ensure that when making social media posts you state, or make it clear in your personal profile, that you are speaking on your own behalf and you use your personal email address to set up any social media account.
- Employees must be respectful to others when making any statement on social media. You should be aware that you are responsible for all communications which will be published on the internet for anyone to see.
- If you see any social media content that disparages or reflects poorly on John Rowan and Partners, you should contact the Marketing department.
- You may be required to remove any social media content that we consider to constitute a breach of this policy. Failure to comply with such a request may in itself result in disciplinary action.

Please also be aware of the following:

- John Rowan and Partners employees should keep in mind that they are personally responsible for what they post online and be mindful that what they say will be available publicly for a long time.
- Social media use is subject to the same workplace policies employees must follow in other situations, including but not limited to John Rowan and Partners policies regarding harassment, discrimination, defamation, confidentiality, non-competition and general Internet use.

Further guidance is available in the Employee Handbook which should be read in conjunction with this policy.

A breach of this policy may result in disciplinary action up to and including dismissal.

10.1 Monitoring

We reserve the right to monitor, intercept and review, without further notice, staff activities using our IT resources and communications systems, including but not limited to social media postings and activities, to ensure that our rules are being complied with and for legitimate business purposes and you consent to such monitoring by your use of such resources and systems.

11.0 Disposal of Electrical Equipment

The Waste Electrical and Electronic Equipment (WEEE) 2006 regulations dictate the organisations must dispose of electrical equipment in a way that maximises the recovery, reuse and recycling. Aside of the WEEE regulations, there is a large security consideration that needs to be taken into account of when disposing of equipment that holds or processes data.

As such, all IT electrical equipment must be disposed of through the Office Manager who works with professional organisations that securely delete data from devices and recycles equipment in accordance with WEEE 2006.

Do not dispose of any IT equipment yourselves directly. All electrical equipment for disposal needs to be transported to a central location where it will be collected and disposed of legally and securely.

Please contact the office management team whenever you have IT equipment to dispose of.

12.0 Internet Access from Homes, Mobile Devices and Public Wi-Fi

The IT service provider will support all Internet connections which have been provided to employees by John Rowan and Partners (including home broadband connections and 3G / 4G / GPRS mobile network connections).

Owing to the varying levels of performance and service from different providers of Internet access both in the UK and worldwide, **IT service provider cannot support any Internet connections not supplied by the business** (including home broadband connections not supplied by FV and non-business mobile data connections).

Due to the high security risk, public Wi-Fi hotspots (such as in restaurants, shops, cafes, hotels and public transport) are not to be connected to with any device that is used for business purposes. Data is very easily intercepted and decrypted in these environments by low-knowledge hackers.

If you need mobile or home access to the Internet for business purposes, please contact the IT service provider who will arrange this through their recommended provider.

13.0 End of Employment

Upon ending employment with John Rowan and Partners, you must return all IT equipment supplied to you by the business to the Office Manager or HR Department. This includes desktop computers, laptops, mobile phones, tablet computers, networking equipment (e.g. broadband routers and Wi-Fi access points), and any data storage devices (e.g. external hard drives, USB flash drives, CDs, DVDs).

You are not permitted to take any data belonging to John Rowan and Partners when you leave the business. This includes any files stored on your computer or networked drives, any files stored on cloud services, any emails or data held in Microsoft Office (including address book contacts), or report files (e.g. Weekly Trading Reports). No hard copy information is to be removed from the business, with any hard copies being handed to your line manager upon exit.

Do not pass your login codes and passwords for any system onto colleagues or management. The IT service provider will make arrangements for emails addressed to your account to be routed to other employees, and your data files will be archived.

In situations where the company believes that continued access to IT systems, data and services will be at risk, **John Rowan and Partners reserves the right to suspend user accounts without prior notification.**

14.0 Policy Non-Compliance

In the event that the rules and procedures of this policy are not followed by users of John Rowan and Partners IT services, and depending on the severity of that breach, **John Rowan and Partners reserves the right to suspend your user accounts**, effectively removing an employee's ability to use any IT service.

Please refer to Appendix D of the John Rowan and Partners Employee Handbook in reference to

disciplinary and appeal processes.

15.0 Policy Agreement

Agreement to this policy document is mandatory for any employee, contractor, volunteer or representative of John Rowan and Partners who comes into contact with either IT systems or personal data (such as customer name and delivery address). Employees who do not agree to this policy will not be granted access to systems or be allowed to handle personal data.