Mobile Devices,Email,Internet and Social Media Policy

Fair for all

Background

The purpose of this policy is to ensure that staff are aware of their responsiblities in the usage and care of their mobile devices and in accessing and using web-based services at any time.

The use of e-mail, the internet and social media by staff is permitted where such use is required for business purposes and supports the aims and objectives of the company. Use of these media for personal purposes is freely permitted before and after normal working hours and during authorised lunch-breaks.

Rydon provides staff with mobile devices when the individual's role requires this for the effective execution of their responsiblities. When appropriate, the device may provide access to the internet via 3G, 4G and/or WiFi connections.

Policy

Security and passwords

Access to and use of the Rydon IT system is only available to Rydon employees. Limited access by authorised third parties may be permitted on a controlled basis. To prevent the risk of access by non-authorised personnel, Rydon utilises a number of hardware and software tools which help to protect the system. The use of robust passwords to access the system is one such tool.

Passwords used to access business systems should not be the same as each other, or the same as the main account password.

Passwords should not be shared with anyone, including administrative assistants or secretaries. All Rydon passwords will be treated as confidential Rydon information.

The 'Remember Password' feature in some applications must never be used. Passwords should never be written down and stored in, or around desks or workplaces.

Mobile devices

The mobile device that is provided by Rydon is intended for business purposes. Many people will have their own devices which they will continue to use, as well as their work devices, particularly phones.

Where they do not have another device, reasonable use of the Rydon device for personal calls, texting, browsing, etc. is permitted.

Individual usage for both calls and data is monitored by the IT department. Monthly reports of high internet users during working hours are sent to all MDs and Corporate Services heads, and individual reports are available to managers should they require them. Managers are responsible for ensuring that this policy is adhered to by their staff and that usage is acceptable.

Company devices should not be taken outside the country unless authorised by a director.

Purchases for mobile devices, including Apps, should not be made without prior authorisation from a director.

Users must take all reasonable steps to protect against the installation of unlicensed and/or malicious applications.

Individuals are responsible for the care of their devices. These should be suitably protected and the appropriate covers used. These are available from the IT department.

If a device is lost or stolen this must be reported to both the IT Helpdesk and to your line manager immediately.

If a user persistently breaks or loses their device, the company reserves the right to deduct the value of the device from the individual's pay. A written warning will

be given to the individual by their manager should this situation be reached.

E-mail
E-mail is not a secure means of communication. Where the contents of a communication are particularly confidential or sensitive, staff should consider whether it is appropriate to use e-mail.

Use of e-mail for personal purposes is permitted but should be kept to a minimum.

Rydon's system has restrictions on incoming/outgoing e-mail containing certain properties.

In this respect, e-mail is monitored and certain types of e-mail will be quarantined before being forwarded (subject to vetting). The criteria for quarantining e-mail in this way will be periodically reviewed.

All external incoming and outgoing messages are screened for viruses.

As a matter of course, staff should not:

- Send or receive any emails that are obscene, discriminatory, defamatory, or which are intended to annoy, harass or intimidate another person.
- Use e-mail for private commercial purposes, product advertisement, political or religious lobbying.
- Represent personal opinions as those of Rydon.

Public File Storage
Company and/or client information which is commercially sensitive should not be stored on public file storage (e.g. Drop Box, Microsoft OneDrive, Google Drive, etc.), nor should it be transmitted using unapproved transmission services (e.g. Gmail, Hotmail, Mail.com, etc.) Where such information needs to be sent externally and where approved services (Rydon email or R-Way link) are not available/practical, the information should be stored on a portable device such as a memory stick, CD or DVD, and sent by registered mail.

Internet
It is acknowledged that use of the internet is now a requirement for many roles within the Group and, as such, that staff should have free access to its use.

Users shall not:

- Visit Internet sites that contain obscene, hateful or other objectionable materials
- Make or post indecent remarks, proposals or materials on the Internet.
- Download certain types of file, such as executable, compressed, movie or music files. If a member of staff needs to download any of these types of file for work purposes, they should contact the IT Helpdesk who will arrange for the files to be downloaded providing they do not breach any copyright laws or cause damage to the network or the system.
- Upload, download or otherwise transmit commercial software or any copyright materials belonging to parties outside of Rydon.
- Reveal or publicise privileged, confidential or proprietary Rydon information.

Social Media
It is now commonplace for companies to use social media as part of the media mix through which they communicate with their various stakeholders.

Rydon currently uses Twitter and Facebook for this purpose. In addition, other social media such as LinkedIn are widely used within professional circles. Other media platforms are constantly emerging.

As with the internet, social media should only be accessed and used by staff during working hours where this is required for business purposes. Use of such media for personal reasons should be restricted to out of normal office hours or during lunch-breaks.

Monitoring and reporting
For the purposes of preventing or detecting abuse, securing the effective operation of our network and to protect the business, Rydon reserves the right to monitor all communications, including e-mail and all access to internet and social media by its staff.

Access to the Internet is monitored by specialist software which keeps a record of all sites visited by every user.

It is the responsibility of each individual employee to apply these guidelines. Inappropriate use of company time on email, the internet and social media may be regarded as a breach of trust and may lead to disciplinary action.

Governance

All policies within the company are approved by the Group Board which is chaired by the Chief Executive. Each policy is reviewed at least once annually to ensure that we respond to clients, business strategy, legislation and any standards or codes of practice determined by the market.

Administration of the Mobile Devices, Email, Internet and Social Media Policy is the responsibility of the Director of IT.

Signature(s) removed for security reasons:
Signed copies available on request

Signed: _____

Adam Jackson

Signature(s) removed for security reasons:
Signed copies available on request

Signed: _____

Robert Bond
Group Chief Executive

Dated: March 2017