Security, Confidentiality & Data Protection

Security

Email, Internet and Telephones

Your contract of employment sets out your contractual obligations with regard to the use of email, the internet and telephones and how we will audit and monitor these.

We recognise the importance of efficient, reliable IT and telecommunications (telecoms) equipment and resources to ensure the most effective running of services, communications and business activities. We also recognise that as a resource, IT and telecoms systems can be costly and open to abuse, so therefore we aim to ensure that appropriate, safe and cost effective use is made of our IT and telecoms equipment and services at all times.

Our aim is for all users to be aware of their responsibilities when using IT and telecoms equipment and facilities provided by the Company, and to ensure that the Company's IT and telecoms equipment and facilities are not abused in any way.

Telephone usage

The Company's telephone lines (including Company mobile phones) are for the exclusive use by employees in connection with the company's business. In view of this, please keep

Personal calls to a minimum so there is minimum disruption to the business.

You are able to have your mobile phone switched on during your working hours which will ideally be switched to a silent ring tone. Personal mobile calls must be kept to a minimum so there is minimum disruption to the business.

Using a mobile phone whilst driving is a criminal offence in the Isle of Man and UK. You must not use a hand-held mobile phone or similar hand-held electronic device whilst driving as part of your job duties, whether this is to make or receive telephone calls, send or read text or image/picture messages or to access the Internet or e-mail.

Company Issued Mobile Phones

The Company may provide you with a mobile phone if you require it for business use. Requests for Company Issued Mobile Phones should be made to your line manager in the first instance.

If you are provided with a Company Issued Mobile Phone, please remember that they are primarily for business use and are not an additional employee benefit. You may use a Company Issued Mobile Phone for personal calls however these calls should be kept to a minimum.

If you have voice mail functionality on your Company Issued Mobile Phone, you must set up a personalised voice mail greeting which identifies you to callers.

Mobile phones should be switched to silent where possible during meetings, lectures, seminars, training courses etc.

Roaming and 3/4G Data SIM Cards

If you are planning to travel outside of the United Kingdom with your Company Issued Mobile Phone, you must contact the IT Department so that the appropriate roaming tariff can be applied.

Telephone manner

When dealing with internal and external customers, we request that you adopt the following approach:

- Identify yourself
- Speak in a pleasant tone of voice
- Speak clearly and in a professional manner
- Answer their colleague’s phones if they are not at their desks
- When transferring a call to a colleague, give them details of who the caller is and provide details of their query.

The use of text messaging for business purposes should be discouraged and only used if no other method of communication would be more efficient.

Indecent, obscene or immoral conduct towards staff, customers and/or third parties over the telephone will not be tolerated and will be treated as Gross Misconduct in accordance with the Disciplinary Policy and procedure.

Security and Data Protection

Cellular networks are not secure and that conversations conducted in inappropriate environments may be overheard. Therefore care must be taken as to where, when and what is discussed.

All Company Issued Mobile Phones should be PIN code protected and kept locked at all times to minimise security risks, particularly if the phone is stolen.

Personal data stored on Company Issued Mobile Phones such as address books, text messages and email is subject to Data Protection regulations and as a minimum must be protected by a PIN or alphanumeric password.

Confidential messages regarding named individuals should not be left on voice mail if possible and never left on a voice mail service which does not confirm the identity of the intended recipient in the voice mail greeting.

Laptops and tablets

We may provide a laptop or tablet to you if you require it for business use. Requests for Company Issued laptops or tablets should be made to the IT Manager or IT HelpDesk by the employees Line Manager.

External drives

USB or mass storage devices should not be connected to any company Laptop, Server or PC that are connected directly to the internal company network without prior signoff from the I.T. department and also having been checked for viruses.

Computer security

Never leave computers ‘unlocked’ when unattended and always log off your computer at the end of each working day to ensure that your documents and data can be backed up correctly overnight. Company data remains the property of the company and must not be shared externally without the correct approval.

No data should be held on non-secure or approved machines or external devices. Approval should be gained from the IT team All PC’s or other Company owned computers must have Group authorised antivirus software installed. Please contact the IT team for further information on antivirus protection. Please be vigilant for any suspicious activity on your PC which could cause issues.

Please think before you act :

- Do not open any emails which you do not recognise who they are from.
- Do not open attachments or links in emails which you wouldn’t normally do as part of your role within the business.
- Take care not to browse on the internet for personal use and click on sites which maybe suspicious.
- If you notice anything odd with accessing systems please report it immediately to I.T. or your line manager.
- If you do accidently click something ‘don’t hide’, report it quickly so it can be investigated.

Internet usage

The company also recognises that the internet is integral to many people’s daily lives. As such, it allows employees to use the internet for personal reasons, with the following stipulations:

- Personal internet use should be of a reasonable level and restricted to non-work times, such as breaks and during lunch.

- All rules described in this policy apply equally to personal internet use. For instance, inappropriate content is always inappropriate, no matter whether it is being accessed for business or personal reasons.

- Personal internet use must not affect the internet service available to other people in the company. For instance, downloading large files could slow access for other employees.

Only people who have been authorised to use the internet may do so.

Authorisation is usually provided by an employee’s line manager or the company IT department. It is typically granted when a new employee joins the company and is assigned their login details for the company IT systems.

Unauthorised use of the company’s internet connection is prohibited and may be dealt with in accordance with the Company’s disciplinary policy, a copy of which can be found in the Staff Handbook.

Internet security

Although advantageous in many ways, the internet can be a source of security problems that can do significant damage to the company’s data and reputation.

- Users must not knowingly introduce any form of computer virus, Trojan, spyware or other malware into the company.

- Employees must not gain access to websites or systems for which they do not have authorisation, either within the business or outside it.

- Company data should only be uploaded to and shared via approved services. The IT team can advise on appropriate tools for sending and sharing large amounts of data.

- You must not steal, use, or disclose someone else’s login or password without authorisation.

You must always consider the security of the company’s systems and data when using the internet. If required, help and guidance is available from the IT team.

Inappropriate content

There are many sources of inappropriate content and materials available online. It is important that you understand that viewing or distributing inappropriate content is not acceptable under any circumstances.

You must not:

- Take part in any activities on the internet that could bring the company into disrepute.

- Create or transmit material that might be defamatory or incur liability for the company.

- View, download, create or distribute any inappropriate content or material.

  Inappropriate content includes: pornography, racial or religious slurs, gender-specific comments, information encouraging criminal skills or terrorism, or materials relating to cults, gambling and illegal drugs.

  This definition of inappropriate content or material also covers any text, images or other media that could reasonably offend someone on the basis of race, age, sex, religious or political beliefs, national origin, disability, sexual orientation, or any other characteristic protected by law.

- Use the internet for any illegal or criminal activities.

- Send offensive or harassing material to others.

- Broadcast unsolicited personal views on social, political, religious or other non-business related matters.

- Send or post messages or material that could damage the Company's image or reputation.

Copyright

The Company respects and operates within copyright laws. Users may not use the internet to:

- Publish or share any copyrighted software, media or materials owned by third parties, unless permitted by that third party.

- Download illegal copies of music, films, games or other software, whether via file sharing services or other technologies.

Employees must not use the company's equipment, software or internet connection to perform any tasks which may involve breach of copyright law.

Software

No software should be downloaded or installed to any company PC, Server or Laptop without prior approval.

All software should be properly licensed and have appropriate support service level contracts in place for the product where required.

Email usage

The Company recognises that email is a key communication tool. It encourages its employees to use email whenever appropriate.

For instance, staff members may use email to:

- Communicate with customers or suppliers
- Market the company's products
- Distribute information to colleagues

The company also recognises that email is an important tool in many people's daily lives. As such, it allows employees to use their company email account for personal reasons, with the following stipulations:

- Personal email use should be of a reasonable level and restricted to non-work times, such as breaks and during lunch.

- All rules described in this policy apply equally to personal email use. For instance, inappropriate content is always inappropriate, no matter whether it is being sent or received for business or personal reasons.

- Personal email use must not affect the email service available to other users. For instance, sending exceptionally large files by email could slow access for other employees.

It is the user's responsibility to maintain and manage their email box and deleted any unwanted emails. This helps reduced backup sizes and restoration.

Only people who have been authorised to use email may do so.

Authorisation is usually provided by an employee's line manager or the company IT department. It is typically granted when a new employee joins the company and is assigned their login details for the company IT systems.

Unauthorised use of the company's email system is prohibited and may be dealt with in accordance with the Company's disciplinary policy, a copy of which can be found in the Staff Handbook.

Email security

Used inappropriately, email can be a source of security problems for the company. Users of the company email system must not:

- Open email attachments from unknown sources, in case they contain a virus, Trojan, spyware or other malware.

- Disable security or email scanning software. These tools are essential to protect the business from security problems.

- Send confidential company data via email. The IT department can advise on appropriate tools to use instead.

- Access another user's company email account. If they require access to a specific message (for instance, while an employee is off sick), they should approach their line manager or the IT department.

Users must also be aware that potential hackers are also able to send emails and attachments which appear to be from a legitimate email address such as a colleague or client, it is therefore important to be vigilant, and if in any doubt always contact the IT department before opening any attachment which is in any way suspicious or unexpected, regardless of its title or perceived origin.

Staff members must always consider the security of the company's systems and data when using email. If required, help and guidance is available from line managers and the company IT department.

Inappropriate content

The company email system must not be used to send or store inappropriate content or materials.

It is important employees understand that viewing or distributing inappropriate content via email is not acceptable under any circumstances.

Users must not:

- Write or send emails that might be defamatory or incur liability for the company.
- Create or distribute any inappropriate content or material via email.

  Inappropriate content includes: pornography, racial or religious slurs, gender-specific comments, information encouraging criminal skills or terrorism, or materials relating to cults, gambling and illegal drugs.

  This definition of inappropriate content or material also covers any text, images or other media that could reasonably offend someone on the basis of race, age, sex, religious or political beliefs, national origin, disability, sexual orientation, or any other characteristic protected by law.
- Use email for any illegal or criminal activities.
- Send offensive or harassing emails to others.
- Send messages or material that could damage the Company's image or reputation.

Any user who receives an email they consider to be inappropriate should report this to their line manager or supervisor.

Email Copyright

The Company respects and operates within copyright laws. Users may not use company email to share any copyrighted software, media or materials owned by third parties, unless permitted by that third party.

Employees must not use the company's email system to perform any tasks that may involve breach of copyright law.

Users should keep in mind that the copyright on letters, files and other documents attached to emails may be owned by the email sender, or by a third party. Forwarding such emails on to other people may breach this copyright.

Email etiquette

Email is often used to communicate with customers, partners and other important contacts. Although a relatively informal medium, staff should be aware that each email they send does affect the company's image and reputation.

It's a good idea to follow rules of good email etiquette. Users must:

- Not forward on chain emails or 'humorous' messages. These clog up people's inboxes and some topics are not appropriate for the workplace.
- Always use a meaningful subject line rather than leaving it blank or using a single word like 'hello'.
- Only use the 'important message' setting sparingly, for messages that really are important.
- Not use ALL CAPITAL LETTERS in messages or subject lines. This can be perceived as impolite.
- Be sparing with group messages, only adding recipients who will find the message genuinely relevant and useful.
- Use the 'CC' (carbon copy) field sparingly. If someone really needs to receive a message, they should be included in the 'to' field.
- Use the 'BCC' (blind carbon copy) field to send group messages where appropriate. It stops an email recipient seeing who else was on the email.

Video Conferencing

The company has now invested in Video conferencing units which will allow connections between sites and potentially other parties. Request for use will need to be booked through IT at least two days before any meeting is required. If you have questions regarding the operation of this equipment please contact IT directly.

Video Conferencing use should be for business purposes. Users of any video conference should act in an appropriate and professional manner. Recording of any conference is prohibited unless all parties are aware of the recording.

Fault Reporting and Replacements

Should any of the IT or telecoms equipment and facilities develop a fault, details should be passed immediately to the Senior IT Manager or IT HelpDesk.

Any damage or theft/loss of any of the IT or telecoms equipment should be reported immediately to the Senior IT Manager or IT HelpDesk.

Existing Company Issued Mobile Phones will not normally be replaced unless they are no longer fit for purpose.

All old Company Issued Mobile Phones must be returned to the IT Department no matter what condition they are in.

Employees who neglect to look after their Company Issued Mobile Phone resulting in loss or damage requiring a replacement may be issued with a basic mobile phone depending upon the business requirements.

Damage to Company IT or telecoms equipment may not lead to a replacement. Repairs will be investigated before any replacement is issued. Costs for repairs will be charged direct to associated department.

Any employees who upon investigation, are found to have wilfully damaged any Company IT or telecoms equipment may face disciplinary action as per the Company's Disciplinary Policy.