Barmoor HUB
Main Road, Ryton
Gateshead
NE40 3AG
Tel: 0191 4132053 or 07960 293013
email: office@barmoorhub.com

COMPUTER, SOCIAL MEDIA, EMAIL AND TELEPHONE USE POLICY

Computer misuse

Some employees and others who work for us, including workers, contractors, volunteers, interns and apprentices, have access to computers in the workplace for the use by them in connection with the Company's business. Access to computers, including devices such as laptops, are provided to employees and others working for the Company to undertake business-related activities only. Employees who are discovered unreasonably using the Company's computers for personal and private purposes will be dealt with under the Company's disciplinary procedure.

Vandalism of, or intentionally interfering with, the Company's computers or network constitutes a potential gross misconduct offence and could render the employee liable to summary dismissal under the Company's disciplinary procedure.

Security

As many computer files contain some form of confidential or otherwise sensitive business information, the Company takes the security of these files very seriously. With this in mind, employees must abide by the following security precautions:

- If you need to leave your computer for:
  (i) more than a couple of minutes, lock the computer screen.
  (ii) a long period of time, log off – never leave an unattended computer logged on.

- When creating a computer password, do not use one that is obvious, such as your date of birth or the name of a close family member – passwords should preferably be a mix of letters and numbers and should not be the same as any other personal passwords you may have (such as online banking passwords).
- Always keep your password private, do not write it down and do not divulge it to anyone else (including other members of staff).
- If you suspect that someone knows your password, change it in the normal way.
- Change your password at regular intervals in any event.
- Always shut down your computer when you go home at the end of the day.
- If you notice any suspicious activity, for example an employee trying to gain unauthorised access to another employee's computer, notify your line manager immediately.

Barmoor HUB
Main Road, Ryton
Gateshead
NE40 3AG
Tel: 0191 4132053 or 07960 293013
email: office@barmoorhub.com

Data

The computers and the data they contain are provided to undertake business-related activities and to enable employees to carry out their job duties. As such, data should not be amended, deleted, copied or taken away unless this is both specifically related to the work the employee is undertaking and they have the authority to make such amendment, deletion or copy. In particular, employees should not delete or amend any documentation or programs which are stored on the Company's communal drives unless they have the requisite level of authority to do so.

Non-work related data should not be copied onto or stored on Company computers.

Use of portable storage devices

Some employees may be provided with portable storage devices (such as memory sticks or memory cards) that can be plugged into the computer. Whilst they are provided so as to allow for the copying and transferring of files and images between an employee's desktop or laptop computer, their small size and storage capacity makes them vulnerable to misuse. For this reason, any employee issued with these devices must not transfer any data to a third party computer (including one at home) without first having obtained approval from their line manager. From time to time, user guidelines will be produced on the usage of such devices and employees will be expected to follow them. Any employee who transfers files to a third party without permission is likely to be subject to disciplinary action. In the event that this involves the deliberate transfer of sensitive commercial information to a competitor, it will be treated as gross misconduct. Additionally, if the unauthorised transfer includes personal data, this is likely to result in a breach of the legal rules and principles relating to data privacy and security, and as such may be treated as gross misconduct

Computer software

The Company licences the use of computer software from a variety of outside companies. The Company does not own this software or its related documentation and, unless authorised by the software developer, neither the Company nor any of its employees have the right to reproduce it. To do so constitutes an infringement of copyright. Any employee found to be contravening this may face disciplinary action under the Company's disciplinary procedure.

Software that employees need to use to carry out their job duties will be provided and installed. Installation of any non-approved software is prohibited, including screen savers and wallpapers.

Barmoor HUB
Main Road, Ryton
Gateshead
NE40 3AG
Tel: 0191 4132053 or 07960 293013
email: office@barmoorhub.com

Computer viruses

The Company's computer network makes it vulnerable to viruses and virus protection software has been installed. Therefore, only duly authorised personnel have the authority to load program software onto the network system and re-configuring or disabling the virus protection software is prohibited. Data compatible with the Company's system may be loaded only after being checked for viruses by the IT department. Any employee found to be contravening this may face disciplinary action under the Company's disciplinary procedure.

E-mail and internet usage

Some employees also have access to internal and external e-mail and the internet for the exclusive use by them in connection with the Company's business and as part of the normal execution of their job duties. Only duly authorised personnel have the authority to use e-mail and the internet at work. Any employee found to be contravening this may face serious disciplinary action under the Company's disciplinary procedure.

The purpose of these rules is to protect the Company's legal interests. Unregulated access increases the risk of employees inadvertently forming contracts through e-mail and increases the opportunity for wrongful disclosure of trade secrets and other confidential information. In addition, carelessly worded e-mail can expose the Company to an action for libel. As such, e-mail to clients and customers must follow the Company's designated house style, which will be supplied to authorised users. Failure to follow house style is a disciplinary matter and will be dealt with under the Company's disciplinary procedure. E-mail should not be used for unsolicited correspondence or marketing campaigns and employees may not commit the Company financially by e-mail unless they have been granted a specific level of delegated authority to do so.

Employees who are authorised users are not permitted to surf the internet or to spend excessive time "chatting" by e-mail or instant messaging applications for personal and private purposes during their normal working hours. Employees are also prohibited from using e-mail to circulate any non-business material. Not only does excessive time spent online lead to loss of productivity and constitute an unauthorised use of the Company's time, sexist, racist or other offensive remarks, pictures or jokes sent by e-mail, instant messaging applications, group chats or through social media sites are capable of amounting to unlawful harassment. Employees are also prohibited from using the Company's electronic communications as a means of intimidating or bullying employees or third parties. Employees who are discovered contravening these rules may face serious disciplinary action under the Company's disciplinary procedure. Depending on the seriousness of the offence, it may amount to gross misconduct and could result in the employee's summary dismissal.

Use of instant messaging applications must be expressly approved in advance by the employee's line manager.

Barmoor HUB
Main Road, Ryton
Gateshead
NE40 3AG
Tel: 0191 4132053 or 07960 293013
email: office@barmoorhub.com

Employees who are authorised users are permitted to surf the internet for personal purposes outside their normal working hours. The Company considers acceptable personal use of the internet to include activities such as personal online shopping, booking holidays and banking. It does not include visiting online gambling sites or participating in online gaming. Employees should note that any purchases or other transactions made online whilst at work are made entirely at their own risk. Employees must not use their work e-mail address to make orders for personal goods and services.

Employees who are authorised users are also only permitted to log on to social networking and video sharing websites such as Facebook, X (formerly known as Twitter), Instagram and YouTube or use the Company IT systems for personal and non-Company related use outside their normal working hours and during any lunch break. The Company reserves the right to restrict access to social networking and video sharing websites at any time.

Logging on to sexually explicit websites or the downloading and/or circulation of pornography or other grossly offensive, obscene or illegal material or using the internet for illegal activities constitutes gross misconduct and renders the employee liable to summary dismissal under the Company's disciplinary procedure. Rogue websites exist that appear harmless but instead direct the user automatically to another website that may contain inappropriate material. If this occurs, please contact the IT department immediately.

Employees must be aware at all times that, while contributing to our social media activities, they are representing the Company appropriately. Staff are authorised to use social media as part of their role within the Company must adhere to the following rules:

- Obtaining permission from their line manager before publishing using social media; and
- Ensuring that the content is checked by the Company in draft format before it is published.

Any communications that employees make in a professional capacity through social media must not bring the Company into disrepute or amount to unlawful conduct or breach of contract, for example by:

- criticising or arguing with customers, colleagues or competitors;
- making defamatory comments about individuals or other organisations or groups; or
- posting images that are inappropriate or links to inappropriate content;
- writing anything that could be considered discriminatory against, or bullying or harassment of, any individual by, for example making offensive or derogatory comments relating to sex, gender reassignment, race (including nationality), disability, sexual orientation, religion or belief or age;
- using social media to bully another individual (such as another employee); or posting images that are discriminatory or offensive, or which links to such content.

- breach Company confidentiality, for example by revealing trade secrets or information owned by our Company;
- revealing confidential information about an individual (such as a colleague or customer contact) or company (such as a competitor business); or discussing our Company's internal business or plans (such as business it is conducting with a [customer/client] or its future business plans that have not been communicated to the public);
- breach copyright, for example by:
    - using someone else's images or written content without the content owner's permission; or
    - failing to give acknowledgment where permission has been given to reproduce something.

Social media

When logging on to and using social networking, video sharing websites and other social media sites at any time, whether using the Company's or the employee's computers and devices, employees must not:

- Publicly identify themselves as working for the Company, make reference to the Company or provide information from which others can ascertain the name of the Company, without the written consent of the Company.
- Conduct themselves in a way that is detrimental to the Company or brings the Company into disrepute.
- Use their work e-mail address when registering on such sites.
- Allow their interaction on these websites or blogs to damage working relationships between employees and clients of the Company.
- Include personal information about the Company's employees, suppliers, customers or clients without their express consent (an employee may still be liable even if employees, suppliers, customers or clients are not expressly named in the websites or blogs as long as the Company reasonably believes they are identifiable).
- Make any derogatory, offensive or defamatory comments about the Company, its employees, suppliers, customers or clients (an employee may still be liable even if the Company, its employees, suppliers, customers or clients are not expressly named in the websites or blogs as long as the Company reasonably believes they are identifiable).
- Make any comments about the Company's employees that could constitute unlawful discrimination, harassment or bullying.
- Disclose any confidential information or trade secrets belonging to the Company or its suppliers, customers or clients, or any information which could be used by one or more of the Company's competitors.

Main Road, Ryton
Gateshead
NE40 3AG
Tel: 0191 4132053 or 07960 293013
email: office@barmoorhub.com

Employees who are discovered contravening these rules, during working hours or outside of those hours, may face serious disciplinary action under the Company's disciplinary procedure. Depending on the seriousness of the offence, it may amount to gross misconduct and could result in the employee's summary dismissal.

The Company reserves the right to deny, remove or limit e-mail and/or internet access to or from any employee or other worker who contravenes these provisions.

Downloading information from the internet and file sharing

Employees may be tempted to make illegal downloads of material that is subject to copyright. This includes, but is not limited to, music, film and business software. As this and any subsequent file sharing of this material constitutes an infringement of copyright, it is prohibited on any Company computer. This also applies to any download or dissemination of material made outside of normal working hours. Any breach is likely to lead to disciplinary action being taken.

Employees may need to download documents and information from the internet in order to undertake their job duties. Employees should only download documents and information that they are sure about and which is required to fulfil the job duties they are undertaking.

E-mail and internet monitoring

The Company reserves the right to monitor employees' internal and external e-mails and use of the internet, both during routine audits of the computer system and in specific cases where a problem relating to excessive and/or unauthorised use is suspected.

The purposes for such monitoring include:

- To promote productivity and efficiency.
- To ensure the security of the system and its effective operation.
- To ensure there is no unauthorised use of the Company's time, for example to check that an employee has not been using e-mail to send or receive an excessive number of personal communications.
- To ensure the smooth running of the business if the employee is absent for any reason and communications need to be checked.
- To ensure that all employees are treated with respect and dignity at work, by discovering and eliminating any material that is capable of amounting to unlawful harassment.
- To ensure that inappropriate websites are not being accessed by employees.
- To ensure there is no breach of commercial confidentiality.

Barmoor HUB
Main Road, Ryton
Gateshead
NE40 3AG
Tel: 0191 4132053 or 07960 293013
email: office@barmoorhub.com

Communications of a sensitive or confidential nature should not be sent by e-mail because it is not guaranteed to be private. Such communications or files should instead be sent by Company-authorised file sharing systems with the appropriate file permissions set up.

When monitoring e-mails, the Company will, save in exceptional circumstances, (see monitoring in the workplace fact sheet), confine itself to looking at the address and heading of the e-mails. However, where the circumstances warrant it, the Company may open e-mails and access the actual content. Employees should mark any personal e-mails as such and encourage those who send them to do the same. The Company will avoid, where possible, opening e-mails clearly marked as private or personal.

Reading and storing e-mails

Employees must check their mailboxes regularly during normal working hours. It is their responsibility to read and action any e-mail received.

If an employee is going to be out of the office for a day or longer and as such they will be unable to check e-mail, they should switch on their "out of office assistant" message. E-mail received in their absence will not normally be read by other members of staff unless the employee has specifically requested a colleague to undertake this task. However, e-mail may need to be checked by line managers for business-related reasons when the employee is absent for any reason. It may therefore be unavoidable that some personal e-mails might be read in these circumstances.

E-mail viruses and spam

All incoming and outgoing external e-mails are checked for computer viruses and, if a virus is found, the message will be blocked. E-mails may also be checked for other criteria, for example, having an attached image file or containing offensive or inappropriate material or including a banned word or from a banned user under the criteria in the Company's spam software which indicates the message is spam. Again, the e-mail will be blocked. The Company reserves the right for the IT department to block and then read these messages to ascertain whether they are business-related.

If employees receive an e-mail or data file that is in a format or comes from a source that they do not recognise, they should not open the item but should contact the IT department immediately. Any executable files received by e-mail must be referred to the IT department for clearance before any other action is taken.

If employees receive any unsolicited e-mails or spam that manages to bypass the Company's spam software, they must not respond in any way. The e-mail should be forwarded to the IT department and they will add the sender to the list of banned users.

Barmoor HUB
Main Road, Ryton
Gateshead
NE40 3AG
Tel: 0191 4132053 or 07960 293013
email: office@barmoorhub.com

Telephone misuse

The Company's telephone lines (including Company mobile phones) are for the exclusive use by employees in connection with the Company's business. Whilst the Company will tolerate essential personal telephone calls concerning an employee's domestic arrangements, excessive use of the telephone for personal calls is prohibited. This includes lengthy, casual chats and calls at premium rates. Not only does excessive time engaged on personal telephone calls lead to loss of productivity, it also constitutes an unauthorised use of the Company's time. If the Company discovers that the telephone has been used excessively for personal calls, this will be dealt with under the Company's disciplinary procedure and the employee will be required to pay to the Company the cost of personal calls made.

Acceptable telephone use should be no more than five minutes of personal calls in each working day. Personal telephone calls should be timed so as to cause minimum disruption to the employee's work and should, as a general rule, only be made during breaks except in the case of a genuine emergency.

Employees should be aware that telephone calls made and received on the Company's telephone network will routinely be monitored and recorded to assess employee performance, to ensure customer satisfaction and to check that the use of the telephone system is not being abused or used in an unauthorised manner. In addition, an itemised call log may be maintained and retained of all external calls made and received on the Company's telephone network. This may include details of the external caller's number and the date, time and duration of the call.

Employees should also be aware that voicemail messages may be checked by line managers for business calls when they are absent for any reason. It may therefore be unavoidable that some personal messages might be heard in these circumstances.

Mobile phones

Whilst the Company will tolerate the use of employees' own mobile phones for essential personal calls or messaging during normal working hours, excessive use for personal calls, lengthy calls, casual chats, text messaging, instant messaging, e-mailing and web browsing is prohibited. Also prohibited in the course of employment is, the taking of videos, photographs, images and audio recordings, unless expressly authorised by the Company in advance, or in the case of recordings where both the recording and processing of it is otherwise lawful and does not contravene the Company's policies, with the express permission of the relevant data subject given in advance and for the stated purpose only. You must not use your mobile phone to record any Company confidential information or documentation. Personal mobile phones should be set to a silent ring during normal working hours. If employees wish to use their personal mobile phone, they should do so outside their normal working hours or during authorised break times.

If you bring your mobile phone other personal device to work, it is your responsibility to look after it and keep it secure at all times.

Contravention of this policy

Failure by employees to comply with any of the requirements of this policy is a disciplinary offence and may result in disciplinary action being taken, up to and including dismissal for more serious breaches of this policy, under the Company's disciplinary procedure.

Data Protection

The Company will process the personal data collected in connection with the operation of the computer and telephone policy in accordance with its data protection policy and any internal privacy notices in force at the relevant time. Inappropriate access or disclosure of this data will constitute a data breach and should be reported immediately to the Company's Data Protection Officer in accordance with the Company's data protection policy. Reported data breaches will be investigated