

### Social Media Policy

#### Social Media Definition

Social media is an interactive online media that allows users to communicate instantly with each other or to share data in a public forum. It includes social and business networking websites such as Facebook, Myspace, Bebo, Twitter and LinkedIn. Social media also covers video and image sharing websites such as YouTube and Flickr, as well as personal weblogs ("blogs"). This is a constantly changing area with new websites being launched on a regular basis and therefore this list is not exhaustive.

This policy applies in relation to any social media that employees may use.

#### Use of social media at Work

##### Limited social media use at work

Employees are only permitted to log on to social media websites or to keep a personal weblog ("blog") using SWAT access's IT systems and equipment outside their normal working hours (for example, during lunch breaks or before the working day has started or after the working day has finished) and this must not under any circumstances interfere with their job duties or have a detrimental effect on their productivity. This includes laptop and hand-held computers, or devices distributed by SWAT access for work purposes. SWAT access nevertheless reserves the right to restrict access to any of these types of websites at any time. Where employees have their own computers or devices, such as laptops and hand-held devices, again they must limit their use of social media on their own equipment to outside their normal working hours.

However, employees may be asked to contribute to SWAT access's own social media activities as part of their job duties, for example for marketing, promotional and recruitment purposes, they must adhere to the following rules:

- Use the same safeguards as they would with any other type of communication about SWAT access that is in the public arena.
- Ensure that any communication has a purpose and a benefit for SWAT access.
- Obtain permission from their line manager before embarking on a public campaign using social media.
- Request their line manager to check and approve content before it is published online.
- Follow any additional guidelines given by SWAT access from time to time.

The social media rules set out below also apply as appropriate.

#### Social Media Rules

SWAT access recognises that many employees make use of social media in a personal capacity outside the workplace and outside normal working hours. While they are not acting on behalf of SWAT access in these circumstances, employees must be aware that they can still cause damage to SWAT access if they are recognised online as being one of its employees. Therefore, it is important that SWAT access has strict social media rules in place to protect its position.

# SWAT

## access

When logging on to and using social media websites and blogs at any time, including personal use on non-Company computers outside the workplace and outside normal working hours, employees must not:

- Other than in relation to SWAT access's own social media activities or other than where expressly permitted by SWAT access for business networking websites such as LinkedIn, publicly identify themselves as working for SWAT access, make reference to SWAT access or provide information from which others can ascertain the name of SWAT access.
- Other than in relation to SWAT access's own social media activities or other than where expressly permitted by SWAT access for business networking websites such as LinkedIn, write about their work for SWAT access – and, in postings that could be linked to SWAT access, they must also ensure that any personal views expressed are clearly stated to be theirs alone and do not represent those of SWAT access.
- Conduct themselves in a way that is potentially detrimental to SWAT access or brings SWAT access or its employees, clients, customers, contractors or suppliers into disrepute, for example by posting images or video clips that are inappropriate or links to inappropriate website content.
- Other than in relation to SWAT access's own social media activities or other than where expressly permitted by SWAT access for business networking websites such as LinkedIn, use their work e-mail address when registering on such sites or provide any link to SWAT access's website. Allow their interaction on these websites or blogs to damage working relationships with or between employees and clients, customers, contractors or suppliers of SWAT access, for example by criticising or arguing with such persons.
- Include personal information or data about SWAT access's employees, clients, customers, contractors or suppliers without their express consent (an employee may still be liable even if employees, clients, customers, contractors or suppliers are not expressly named in the websites or blogs as long as SWAT access reasonably believes they are identifiable) – this could constitute a breach of the Data Protection Act 1998 which is a criminal offence.
- Make any derogatory, offensive, adverse, discriminatory, untrue, negative, critical or defamatory comments about SWAT access, its employees, clients, customers, contractors or suppliers, or any comments which might reasonably be considered to insult, damage or impugn SWAT access's or their reputation or character (an employee may still be liable even if SWAT access, its employees, clients, customers, contractors or suppliers are not expressly named in the websites or blogs as long as SWAT access reasonably believes they are identifiable).
- Make any comments about SWAT access's employees that could constitute unlawful discrimination, harassment or cyber-bullying contrary to the Equality Act 2010 or post any images or video clips that are discriminatory or which may constitute unlawful harassment or cyber-bullying – employees can be personally liable for their actions under the legislation.
- Disclose any trade secrets or confidential, proprietary or sensitive information belonging to SWAT access, its employees, clients, customers, contractors or suppliers or any information which could be used by one or more of SWAT access's competitors, for example information about SWAT access's work, its products and services, technical developments, deals that it is doing, future business plans and staff morale.

# SWAT

## access

- Breach copyright or any other proprietary interest belonging to SWAT access, for example, using someone else's images or written content without permission or failing to give acknowledgement where permission has been given to reproduce particular work – if employees wish to post images, photographs or videos of their work colleagues or clients, customers, contractors or suppliers on their online profile, they should first obtain the other party's express permission to do so.

Employees must remove any offending content immediately if they are asked to do so by SWAT access.

Work and business contacts made during employment through social media websites and which are added to personal social networking accounts amount to confidential information belonging to SWAT access and accordingly SWAT access may ask for them to be surrendered on termination of employment.

Employees should remember that social media websites are a public forum, even if they have set their account privacy settings at a restricted access or "friends only" level, and therefore they should not assume that their entries on any website will remain private or confidential.

Employees must also be security conscious when using social media websites and should take appropriate steps to protect themselves from identity theft, for example by setting their privacy settings at a high level and restricting the amount of personal information they give out, such as date and place of birth, schools attended, family names and favourite football team. This information may form the basis of security questions and/or passwords on other websites, such as online banking.

Should employees observe inaccurate information about SWAT access on any web sources of information, they should report this to their line manager in the first instance.

### **Social Media References**

Where employees (or ex-employees) has set up personal profiles on business networking websites such as LinkedIn, these websites may include the facility for the user to request their contacts or other users to provide them with open recommendations, endorsements or references which are then published on their personal profile web pages for other contacts or connections, or prospective contacts or connections, to read. As these could potentially be construed as open references given on behalf of SWAT access, employees are prohibited from providing these types of recommendations, endorsements or references online to or for the benefit of other employees or ex-employees without the prior permission of their line manager.

If these types of recommendations, endorsements or references are requested online by clients, customers, contractors, suppliers or other Company-related business connections, employees should refer such requests to their line manager.

# SWAT

## access

### **Social Media Monitoring**

SWAT access reserves the right to monitor employees` use of social media on the internet, both during routine audits of the computer system and in specific cases where a problem relating to excessive or unauthorised use is suspected. The purpose for such monitoring are to:

- Promote productivity and efficiency.
- Ensure the security of the system and its effective operation.
- Ensure there is no unauthorised use of SWAT access`s time, for example to check that an employee has not been spending an excessive amount of time using social media websites for non-work-related activity when they should be working.
- Ensure that inappropriate, restricted or blocked websites are not being accessed by employees.
- Ensure that all employees are being treated with respect and dignity at work, by discovering and eliminating any material that is capable of amounting to harassment contrary to the Equality Act 2010.
- Ensure there is no breach of commercial confidentiality.

SWAT access reserves the right to restrict, deny or remove internet access, or access to particular social media websites, to or from any employee.

### **Contravention of This Policy**

Failure to comply with any of the requirements of this policy is a disciplinary offence and may result in disciplinary action being taken under SWAT access`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.

# SWAT

## access

### Computer and Telephone Use Policy

#### Computer misuse

Some employees have access to computers in the workplace for the use by them in connection with SWAT access's business. Computers are provided to employees to undertake business-related activities only. Employees who are discovered unreasonably using SWAT access's computers for personal and private purposes will be dealt with under SWAT access's disciplinary procedure.

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

#### Security

As many computer files contain some form of confidential or otherwise sensitive business information, SWAT access takes the security of these files very seriously. Employees must abide by the following security precautions:

- If you need to leave your computer for more than a couple of minutes, lock the computer screen.
- If you need to leave your computer for 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.

#### 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. Employees should not delete or amend any documentation or programs which are stored on SWAT access'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.

# SWAT

## access

### **Use of Portable Storage Devices**

Some employees may be provided with portable storage devices (such as memory sticks and portable hard drives) that can be plugged into the USB port of a computer. Whilst they are provided 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. If this involves the deliberate transfer of sensitive commercial information to a competitor, it will be treated as gross misconduct.

### **Computer Software**

SWAT access licences the use of computer software from a variety of outside companies. SWAT access does not own this software or its related documentation and, unless authorised by the software developer, neither SWAT access 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 SWAT access'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.

### **Computer Viruses**

SWAT access'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 SWAT access'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 SWAT access's disciplinary procedure.

### **Computer Games**

There are computer games on network. Employees may only access these outside their normal working hours, for example during lunch breaks. Employees must not install their own games on to work computers.

### **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 SWAT access'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 SWAT access's disciplinary procedure.

The purpose of these rules is to protect SWAT access's legal interests. Unregulated access increases the risk of employees inadvertently forming contracts through e-mail and increases SWAT access

# SWAT

## access

the opportunity for wrongful disclosure of trade secrets and other confidential information. In addition, carelessly worded e-mail can expose SWAT access to an action for libel. As such, e-mail to clients and customers must follow SWAT access'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 SWAT access's disciplinary procedure. E-mail should not be used for unsolicited correspondence or marketing campaigns and employees may not commit SWAT access 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 for personal and private purposes during their normal working hours. Employees are also prohibited from using e-mail to circulate by non-business material. Not only does excessive time spent online lead to loss of productivity and constitute an unauthorised use of SWAT access's time, sexist, racist or other offensive remarks, pictures or jokes sent by e-mail are capable of amounting to unlawful harassment. Employees are also prohibited from using SWAT access'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 SWAT access'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 systems must be expressly approved in advance by the employee's line manager.

Employees who are authorised users are permitted to surf the internet for personal purposes outside their normal working hours. SWAT access 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 only permitted to log on to social networking and video sharing websites such as Facebook, Twitter and YouTube or use SWAT access IT systems to keep a personal weblog ('blog') outside their normal working hours and during any lunch break SWAT access 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 SWAT access'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.

# SWAT

## access

### **Social Networking and Video Sharing Websites**

When logging on to and using social networking and video sharing websites and blogs at any time, employees must not:

- Publicly identify themselves as working for SWAT access, refer to SWAT access or provide information from which others can ascertain the name of SWAT access.
- Conduct themselves in a way that is detrimental to SWAT access or brings SWAT access 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 SWAT access.
- Include personal information about SWAT access'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 SWAT access reasonably believes they are identifiable).
- Make any derogatory, offensive or defamatory comments about SWAT access, its employees, suppliers, customers or clients (an employee may still be liable even if SWAT access, its employees, suppliers, customers or clients are not expressly named in the websites or blogs as long as SWAT access reasonably believes they are identifiable).
- Make any comments about SWAT access's employees that could constitute unlawful discrimination, harassment or bullying.
- Disclose any confidential information or trade secrets belonging to SWAT access or its suppliers, customers or clients, or any information which could be used by one or more of SWAT access's competitors.

Employees who are discovered contravening these rules, whether inside or outside the workplace, may face serious disciplinary action under SWAT access'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.

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

### **Downloading Information from the Internet and File Sharing**

Employees may be tempted to make illegal download 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.

# SWAT

## access

### **E-mail and Internet Monitoring**

SWAT access 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 purpose for such monitoring includes:

- To promote productivity and efficiency.
- To ensure the security of the system and its effective operation.
- To ensure there is no unauthorised use of SWAT access'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.

Communications of a sensitive or confidential nature should not be sent by e-mail because it is not guaranteed to be private.

When monitoring e-mails, SWAT access will, save in exceptional circumstances, confine itself to looking at the address and heading of the e-mails. However, where the circumstances warrant it, SWAT access 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. SWAT access 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 SWAT access's spam software which indicates the message is spam. Again, the e-mail will be blocked. SWAT

# SWAT

## access

access 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 SWAT access'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.

### **Telephone Misuse**

SWAT access's telephone lines (including Company mobile phones) are for the exclusive use by employees in connection with SWAT access's business. Whilst SWAT access 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, is also constitutes an unauthorised use of SWAT access's time. If SWAT access discovers that the telephone has been used excessively for personal calls, this will be dealt with under SWAT access's disciplinary procedure and the employee will be required to pay to SWAT access 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 times 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 SWAT access'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 SWAT access'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 SWAT access will tolerate the use of employees' own mobile phones for essential personal calls during normal working hours, excessive use for personal calls is prohibited. Also prohibited are lengthy calls, casual chats, text messaging, e-mailing, web browsing and the taking of video and/or still images. 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.

### **Contravention of This Policy**

# SWAT

## access

Failure to comply with any of the requirements of this policy is a disciplinary offence and may result in disciplinary action being taken under SWAT access's disciplinary procedure.