FIS | Information

KNOWLEDGE HUB

Electronic Communications Policy

All companies should have a formal Electronic Communication Policy. A sample follows, which members may adapt as necessary to suit their company needs.

The company has invested in the necessary resources to ensure that it is able to make the most of the advantages offered by modern electronic communication methods. It is committed to maintaining an up to date capability, and will ensure that all members of staff who will benefit from the use of this facility will receive ongoing training. The Internet, Intranet and email facilities may only be used for business purposes except in certain circumstances outlined below.

These guidelines are to be regarded as a code of conduct for all members of staff and failure to observe procedures may be regarded as misconduct or gross misconduct, and will be dealt with according to the company's normal disciplinary procedure.

Any member of staff who experiences problems concerning abuse of the electronic communication facility, should in the first instance approach their immediate manager.

Computer misuse

Some employees have access to computers at work for use in connection with the company's business. 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 otherwise intentionally interfering with, the company's computers/network constitutes a gross misconduct offence and could render the employee liable to summary dismissal under the company's disciplinary procedure.

Email and the Internet

Some employees also have access to email and the Internet for exclusive use in connection with the company's business and as part of the normal execution of the employee's job duties. The purpose of these rules is to protect the company's legal interests. Unregulated access increases the risk of employees inadvertently forming contracts through email and increases the opportunity for wrongful disclosure of confidential information. In addition, carelessly worded email can expose the company to an action for libel. As such, email 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. Email should not be used for unsolicited correspondence or marketing campaigns and employees may not commit the company financially by email 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 email for personal and private purposes during their normal working hours. Employees are also prohibited from using email 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 or jokes sent by email are capable of amounting to unlawful harassment. As 'cyber-bullying' is an emerging risk, 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 systems must be expressly approved in advance by the company. Employees

FIS
Olton Bridge, 245 Warwick Road
Solihull, West Midlands B92 7AH
+44(0)121 707 0077
info@thefis.org
www.thefis.org

are permitted to surf the Internet for personal purposes during the following hours . . . . . (insert details).

Employees should also be aware that whilst the company considers personal use of the Internet for activities such as online shopping, booking holidays and banking acceptable, 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 who are authorised users are also not permitted to log on to Ebay, social networking and video sharing websites such as Facebook, MySpace, Bebo and YouTube or use the company's IT systems to keep a personal weblog ('blog') at any time. The company has added websites of this type to its list of restricted websites.]

OR

[Employees who are authorised users are also only permitted to log on to Ebay, social networking and video sharing websites such as Facebook, MySpace, Bebo and YouTube or use the company's IT systems to keep a personal weblog ('blog') at designated times during the day. These are during the following hours …… (insert details). (Employees should note that whilst they may visit Ebay during these designated times, they may not trade on the site.) The company nevertheless reserves the right to restrict access to websites of this type at any time.]

Logging on to sexually explicit websites or the downloading and/or circulation of pornography or obscene material or using the Internet for gambling or illegal activities constitutes gross misconduct and could render the employee liable to summary dismissal under the company's disciplinary procedure.

Illegal file sharing

Due to faster computer networks, employees may be tempted to make illegal downloads of material that is subject to copyright. This includes, but is not confined to, music, film and business software. As this and any subsequent file sharing of this material breaches copyright laws, it is prohibited on any computer that is owned or leased by the company. This also applies to any download or dissemination of material made outside of working hours. Any breach is likely to lead to disciplinary proceedings.

When logging on to and using social networking and video sharing websites and blogs at any time, including personal use outside the workplace, 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.
- Conduct themselves in a way that is detrimental to the company or brings the company into disrepute.
- Use their work email 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, contractors, suppliers, customers or clients without their express consent (an employee may still be liable even if employees, contractors, 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, discriminatory or defamatory comments about the company, its employees, contractors, suppliers, customers or clients (an employee may still be liable even if the company, its employees, contractors, 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 harassment or bullying.
- Disclose any trade secrets or confidential information belonging to the company, its employees, contractors, suppliers, customers or clients or any information which could be used by one or more of the company's competitors.

Employees who are discovered contravening these rules, whether inside or outside the workplace, 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 monitor employees' emails and use of 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 purposes for such monitoring are:

- To promote productivity and efficiency.
- For security reasons.
- To ensure there is no unauthorised use of the company's time eg that an employee has not been using email 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, by discovering and eliminating any material

that is capable of amounting to unlawful harassment.

Communications of a sensitive or confidential nature should not be sent by email because it is not guaranteed to be private. When monitoring emails, the company will, except in exceptional circumstances, confine itself to looking at the address and heading of the emails. However, where circumstances warrant it, the company may open emails and access the content. In this case, the company will avoid, if possible, opening emails clearly marked as private or personal.
The company reserves the right to deny or remove email or Internet access to or from any employee.

Use of portable storage devices

Some employees may be provided with portable storage devices, such as memory sticks, 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 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 is likely to be treated as gross misconduct.

Computer software, games and viruses

The company licenses the use of computer software from a variety of outside companies. The company does not own this software 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. Contravention is a disciplinary matter and will be dealt with in accordance with the company's disciplinary procedure.

The company's computer network makes it vulnerable to viruses. Therefore, only duly authorised personnel have the authority to load new software onto the network system. Even then, software may be loaded only after having been checked for viruses by authorised personnel. Any employee found to be contravening this will face disciplinary action under the company's disciplinary procedure.

Employees may only access any computer games that are on the network outside their normal working hours.

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, we have introduced some basic security precautions that all employees must abide by. These are as follows:

- If you need to leave your computer for more than a couple of minutes, close the screen or lock your computer.
- 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.
- Always keep your password private and do not divulge it to any colleague except for….. (insert details).
- If you suspect that someone knows your password, change it in the normal way.
- If you are provided with a company computer, family members are/are not (amend as necessary) allowed to use it.

(amend or delete as necessary)

Managers

- In addition to the above points, managers will be required to notify the IT department in advance of any computer users that will be leaving the company. This should be done at least…. (insert period here) before the employee leaves, so that the individual's account can be closed on their departure.
- From time-to-time, the company will review its storage of confidential information and the media upon which it is stored. As part of their job role, all managers will be expected to co-operate in terms of identifying such files, the employees or other staff with access to them and the file locations.

(amend or delete as necessary)

Remote access

Some employees will spend at least part of their working week on company business away from the premises. This includes sales staff, (insert other categories as applicable) and those who may work from home. These employees and others who may work remotely on an informal basis should be aware that all aspects of this policy apply to them. Remote working employees will also be expected to comply with any additional guidelines that may be introduced in order to reduce the likelihood of the company's computer networks being compromised as a result of remote access.

Telephone misuse

The company's telephone lines 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 the company the cost of the personal calls made.

Acceptable telephone use should be no more than …… (insert a suitable figure) 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. If employees wish to make or take a particularly sensitive, private or confidential personal telephone call, they are advised that they can use the telephone located:…… (insert details) which will not be subject to any form of monitoring or recording by the company.

Mobile phones

Whilst the company will tolerate use of mobile phones for essential calls during working hours, excessive use for personal calls is prohibited. Also prohibited are lengthy calls, casual chats, text messaging, emailing, web browsing and the taking of video and/or still images (if your phone is so enabled). Your mobile phone should be set to a silent ring during working hours. If you wish to use your mobile phone, you are requested to do so during official breaks.

Temporary workers

From time-to-time, the company may need to use temporary staff in order to cover busy periods or annual leave etc. Should any temporary worker need to use a computer as part of their job role, the manager responsible for their day-to-day supervision will be required to bring this policy and its contents to their attention. The temporary worker will need to sign it. It is also company policy that any temporary workers who are required to use a computer for more than …….(insert number) days will be given their own log-in details (amend/delete as necessary). For longer bookings, managers will need to identify if there are any directories or computer files on the computer that will be used that are of a sensitive or confidential nature. If so, the IT department needs to be involved in restricting access to them. The same principles will apply to any self-employed contractors engaged by the company.

This policy is non-contractual and is therefore subject to revision at any time.

Acknowledgement: This information has been reproduced from information kindly provided by Indicator Ltd, which publishes 'Tips and Advice – Personnel', a fortnightly guide to being a cost effective employer www.indicator.co.uk