Computers and Electronic Communications

What this policy covers

This policy sets out the Company's guidelines on access to and the use of the Company's computers and on electronic communications. It sets out the action which will be taken when breaches of the guidelines occur.

You are only permitted to use the Company's computer systems in accordance with the Company's Data Protection, Monitoring Policies and the following guidelines.

Your responsibilities

The Company's computer systems and software and their contents belong to the Company and they are intended for business purposes only. You are not permitted to use the Company's systems for personal use, unless authorised by your manager.

You are not permitted to download or install anything from external sources unless you have express authorisation from your manager.

No device or equipment should be attached to the Company's systems without prior approval of your manager.

The Company has the right to monitor and access all aspects of its systems, including data that is stored on the Company's computer systems in compliance with the Data Protection Act 1998.

System security

You must only log on to the Company's computer systems using your own password which must be kept secret. You should select a password that is not easily broken (e.g. not your surname).

You are not permitted to use another employee's password to log on to the computer system, whether or not you have that employee's permission. If you log on to the computer using another employee's password, you may be liable to disciplinary action up to and including summary dismissal for gross misconduct. If you disclose your password to another employee, you may also be liable to disciplinary action.

To safeguard the Company's computer systems from viruses, you should take care when opening documents or communications from unknown origins. Attachments may be blocked if they are deemed to be potentially harmful to the Company's systems.

All information, documents, and data created, saved or maintained on the Company's computer system remains at all times the property of the Company.

Use of e-mail

Where the Company's computer systems contain an e-mail facility, you should use that e-mail system for business purposes only.

E-mails should be written in accordance with the standards of any other form of written communication and the content and language used in the message must be consistent with best practice. Messages should be concise and directed to relevant individuals on a need to know basis.

You should take care when opening e-mails from unknown external sources. Attachments to e-mails may be blocked if they are deemed to be potentially harmful to the Company's systems. If in any doubt please contact Holly Roberts prior to opening the email.

E-mails can be the subject of legal action (for example, claims of defamation, breach of confidentiality or breach of contract) against both the employee who sent them or the Company. As e-mail messages may be disclosed to any person mentioned in them, you must always ensure that the content of the e-mail is appropriate.

Abusive, obscene, discriminatory, harassing, derogatory or defamatory e-mails must never be sent to anyone. If you do so, you may be liable to disciplinary action up to and including dismissal without notice.

Internet access

You are required to limit your use of the internet to sites and searches appropriate to your job. The Company may monitor all internet use by employees.

You are expressly forbidden from accessing web pages or files downloaded from the internet that could in any way be regarded as illegal, offensive, in bad taste or immoral.

Monitoring

Monitoring of the Company's computer systems and electronic communications may take place in accordance with the Company's Monitoring Policy. Please refer to the Company's Monitoring Policy for further details.

Procedure

Misuse of computer systems

Examples of misuse include, but are not limited to, the following:

- accessing on-line public messaging / chat rooms, blogs, social network sites without express written permission from the company.
- use of on-line auction sites
- sending, receiving, downloading, displaying or disseminating material that discriminates against, degrades, insults, causes offence to or harasses others
- accessing pornographic or other inappropriate or unlawful materials
- engaging in on-line gambling
- forwarding electronic chain letters or similar material
- downloading or disseminating copyright materials
- issuing false or defamatory statements about any person or organisation via the Company's electronic systems
- unauthorised sharing of confidential information and data about the Company, its clients, suppliers, other 3rd parties or any person or organisation connected to the Company,
- loading or running unauthorised games or software
- Use of file sharing software without prior consent, and
- Use of web based emails other than that provided by the company

Any evidence of misuse may result in disciplinary action up to and including dismissal without notice. If necessary, information gathered in connection with the investigation may be handed to the police.

Should you deem it necessary to your role to access any of the above, please contact Holly Roberts or Antony Greenberg prior to doing so. They will review your requirements and confirm whether it is safe, secure and within company standards to do so.

Complaints of bullying and harassment

If you feel that you have been harassed or bullied or are offended by material received from a colleague, you should inform your manager immediately.

Social Networking Sites and Blogs

What this policy covers

This policy sets out the Company's position on employees' use of social networking sites and blogs, whether conducted on Company media and in work time or your own private media in your own time.

Your responsibilities

Social networking sites and blogs offer a useful means of keeping in touch with friends and colleagues, and they can be used to exchange views and thoughts on shared interests, both personal and work-related.

The Company does not object to you setting up personal accounts on social networking sites or blogs on the internet, in your own time and using your own computer systems. However, you must not do so on Company media or in work time.

You must not link your personal social networking accounts or blogs to the Company's website. Any such links require the Company's prior consent.

You must not disclose Company secrets, breach copyright, defame the Company or its clients, suppliers, customers or employees, or disclose personal data or information about any individual that could breach the Data Protection Act 1998 on your blog or on your social networking site.

Social networking site posts or blogs should not be insulting or abusive to employees, suppliers, Company contacts, clients or customers.

References to the Company

If reference is made to your employment or to the Company, you should state to the reader that the views that you express are your views only and that they do not reflect the views of the Company. You should include a notice such as the following:

'The views expressed on this website/blog are mine alone and do not reflect the views of my employer'

You should always be conscious of your duty as an employee to act in good faith and in the best interests of the Company under UK law. The Company will not tolerate criticisms posted in messages in the public domain or on blogs about the Company or any other person connected to the Company.

You must not bring the Company into disrepute through the content of your website entries or your blogs.

Any misuse of social networking sites or blogs as mentioned above may be regarded as a disciplinary offence and may result in dismissal without notice.

You should be aware that any information contained in social networking sites may be used in evidence, if relevant, to any disciplinary proceedings.

Third parties

You must not disclose any information that is confidential or proprietary to the Company or to any third party that has disclosed information to the Company. The Company's Data Protection Policy (detailed elsewhere in the Employee Handbook) provides guidance about what constitutes confidential information.

This policy should be read in conjunction with the Company policy on Computers and Electronic Communications.

Procedure

Breaches of this policy will be dealt with under the Company's Disciplinary Procedure. You should be aware that the Company regards breach of any part of this policy as gross misconduct that may result in disciplinary action up to and including dismissal without notice.

If you become aware of information relating to the Company posted on the internet, you should bring this to the attention of your manager.