



DAYSPRING
PLACEMENT SOLUTIONS LIMITED

Computer Systems Policy

Computer Systems Policy Information Pack

June 2020

COMPUTER SYSTEMS CODE OF CONDUCT & EMAIL/INTERNET POLICY

1.0 The policy

The purpose of this document is to explain the guidelines relating to use of computer systems, email and the internet.

Dayspring Placement Solutions has developed its code of conduct and policy on email and internet usage:

- To ensure the correct use of Company resources
- to prevent the harassment and bullying of individuals by electronic means
- to inform individuals of their responsibilities concerning computer systems, email and the internet
- explain the consequences of misuse of computer systems and electronic communication and potential liability for both the individual and the Company

2.0 Consequence of misuse

Computers, email and the internet must only be used as expressly permitted or authorised by the Company. If you have any doubts discuss it with your Manager.

All activities on the Company's computers systems, email or the internet, whether business or pleasure, should not in any way bring the Company's name into disrepute and any action which results in this outcome could be treated as a disciplinary matter.

Owing to the importance of the Company's computer systems these requirements are considered to be essential to the Company's business. Misuse is regarded by the Company as an example of misconduct, which will lead to the implementation of the Company's disciplinary procedure. Depending on the circumstances, serious misuse of these systems may constitute gross misconduct in accordance with the terms of the Company's disciplinary procedure, which could result in dismissal. Intentional failure to comply with this code could also result in dismissal.

For serious breaches, it may be that the law has been broken and legal prosecution could follow.

2.1 Harassment

Email or Internet messages which are aggressive, rude, and abusive or which amount to disability, sexual or racial harassment can have a serious impact on the recipient. If you receive such a message you must inform your Manager, as soon as possible. Any individual found sending hostile, harassing or bullying messages will be dealt with under the Company's disciplinary procedure, which could lead to dismissal.

2.2 Liability

Libel is an untrue written statement, which damages the reputation of a person (or Company) or holds him/her/it up to hatred, ridicule or contempt. It need not be obviously insulting. It could, for example, be a suggestion that a competitor is in financial difficulties or is unprofessional in the conduct of its business.

The Company and you may be held liable for the damage caused by internal and external email messages and all other electronic communication as they can be regarded as libellous material. The law does not distinguish between such messages and paper memoranda when evaluating whether the material is potentially libellous or not, therefore, you must ensure that when circulating information which relates to individuals, firms or companies (including clients and competitors) that the information is accurate.

If the Company is found liable because of an act of an employee, the Company reserves the right to claim compensation from the employee involved.

Every individual has the responsibility to protect the Company against the electronic dissemination of a potentially libellous communication. Should you receive or become aware of an electronic communication, which could be considered as libellous, you must report it to your Manager as a matter of urgency.

3.0 Using the equipment

3.1 General

- Computer equipment and Internet and email facilities are the Company's property and are intended for Company business. There is no objection to your making reasonable use for personal purposes such as electronic mail or preparing personal letters outside of normal working hours, providing you observe the guidelines contained in this policy
- do not waste materials, or waste time on the computers to the detriment of others or your personal workload

- you are not allowed to use Company computers for personal commercial gain
- you should use the system status facility to inform you of any imminent service notices
- the playing of computer games during working hours is not allowed
- the Company relies heavily upon its computer systems. Preserving the integrity of those systems is therefore vital. For this reason, you should not under any circumstances load computer software or other computer data from an external source onto Company computer equipment or onto any computer equipment that is linked in any way to computer equipment of the Company or of an associated Company without the express prior written authorisation from the IT department

3.2 Maintenance

- Please treat computer equipment with respect
- Do not delete, disable, modify or move any software or hardware provided by the Company except where instructed to do so by the IT department
- Do not connect your own personal computer equipment to the network
- You must always comply with any maintenance instructions issued by the IT department

3.3 Security

- It is your responsibility to keep equipment under your control free from viruses or anything else with the potential of causing damage.
- The Company has a license to run an anti-virus package. If you suspect you have a virus on your computer, contact the IT Department immediately
- It is your responsibility to keep your account secure. Never allow anyone else access to it.
- Keep your password secret. Do not use your name, your partner's name, your car registration or anything else that someone might guess. If you have to write it down, disguise it. Change your password regularly. If you think someone might have watched you typing it in, change it immediately. You are responsible for ensuring your password is protected and kept confidential.

- Please ensure that when you are not using the computer you log off or lock the workstation. This will prevent unauthorised use.
- Remember, you are personally responsible for any actions performed under your account's name.
- Never use anyone else's account.

3.4 Looking after your data

- Power, disc and system failures usually take effect without warning. Think about the consequences before you use the computers. The following good practice is recommended:
- Files should be saved at frequent intervals
- Keep your own multiple back-up copies of anything that is important. Set the write protect tab on the target disc after copying. Discs are cheap - use plenty!

3.5 Data protection

- The law requires that you do not hold any information in electronic form about living persons unless you are registered to do so.
- Any information held on computer may be accessed by individuals under Data Protection legislation. Therefore, do not use words or phrases, which may be deemed libellous.
- Ensure all information held on computer is accurate, relevant and not excessive.

3.6 Copyright restrictions

- Do not copy any software without permission from the IT department or line manager. You should assume that all software is under copyright.
- Do not copy any data without permission from the IT department. This includes copying text or graphics - whether by using a scanner or by typing it in.

4.0 Email & the internet

The use of email and the Internet is for business purposes. When using electronic communication methods individuals must not breach other Company policies.

4.1 Email

- The primary use of email is to access/distribute/update information, confirm arrangements, confirm meetings
- It should not be used as a substitution for face to face or telephone conversation where these are necessary and cannot substitute for managerial control.
- An email message should be treated as if it were a hard copy letter and drafted and checked in the same way
- On no account should email be used for vindictive, harassing, discriminatory or abusive comment or criticism of anyone whether the target is another employee or any third parties
- Any individual in receipt of an item which they feel should have been prohibited by the above point should inform their Manager immediately
- All messages should be clear and unambiguous
- No response to an email message should be sent in haste, anger or hostility
- Your use must be lawful, honest and decent, and must have regard to the rights and sensitivities of other people as failure could result in action being brought against you
- The facility is provided for Company business. Like telephone calls reasonable personal use of is acceptable but should be kept to a minimum and used with consideration
- Note that email is NOT private.
- You must not forward Company sensitive information to external sources
- Remember - mail might accidentally reach somebody for whom it was not intended
- In summary, you must not use email for:
 - making libelous or potentially libelous statements
 - sending offensive/obscene/untrue or malicious statements or attachments
 - use foul or offensive language – including indecent, sexist, obscene or racist remarks
 - breaches of confidentiality or copyright
 - anything which may damage the business interests of the Company or the group
- harassment

Note: This list is not exhaustive

4.2 Internet

Internet access will provide you with a wealth of ever-growing resources and, when used correctly, can be a valuable tool. You will be able to research prospect clients and identify key information, enabling you to understand their needs and work in partnership with them, and gain that all important edge over the competition.

However, the Internet can also be a source of information and data not relevant to the Company. Viruses can be contained in various formats and can quite easily wipe out whole systems if downloaded. For an acceptable use of the internet, follow those already established for email usage. You are expected to use the Internet in a responsible and conscientious manner, primarily for accessing material related to your job role.

- Internet correspondence is not guaranteed to be private, as messages can be intercepted. Use of the internet is monitored by the Company for security and network management.
- You must not download ANYTHING not related to the Company e.g. software, games, screensavers.
- Misuse of the Internet by, for example, viewing or downloading ANY offensive material is strictly forbidden; it may result in dismissal and could also constitute a criminal offence
- Certain sites and materials are regarded as inappropriate by the Company including, but not limited to: pornography, jokes (which may be regarded as offensive); terrorism; cults; gambling; illegal drugs. In summary, you must not use the internet for:
 - private or freelance business
 - gambling
 - visiting pornographic sites
 - receiving pornographic information
 - conducting political activities
 - accessing or contributing to chat rooms

Note: This list is not exhaustive

4.3 Monitoring and reporting abuse

Messages sent via email and the Internet are more permanent and accessible than you may think. Such messages should be treated in the same way as other written material in that they may be accessible even when apparently deleted. The way in which the information in most computer systems (including ours) is archived or backed up means that even after you think you have deleted the message from your machine it can be accessible for months. It is estimated that messages sent via the internet are kept for 2 years and can be retrieved by the Police. Access to internet web pages is also recorded by the firewall systems, which connect the Company network to the internet.

The Company reserves the right to monitor all such communication and access on a periodic basis.

Where evidence of misuse comes to light, as a consequence of monitoring, this will be investigated further, and appropriate action will be taken as referred to in 'Consequence of Misuse'

You should report any instance of abuse through your Manager. If you receive anything offensive, you should retain the message as evidence.

I have read and understood this policy and agree to comply with all of it.

Name

Signature

Date: _____