Computers and Electronic Communications Policy

Starfish 9 Ltd. Computers & Electronic Communications Policy 2023 - Issue 4

(Last Review 7th Jan 2023 - Next Planned Review 26th Jan 2024)

Computers and Electronic Communications

What this policy covers

This policy applies to employees, workers and contractors.

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, Bring Your Own Device to Work, and 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 as notified to you in the Company's Privacy Notice and in compliance with data protection laws.

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 person's password to log on to the computer system, whether or not you have their permission. If you log on to the computer using another person'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 person, 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.

Processing personal data

You may have access to the personal data of other individuals and of our customers and clients that is being processed within the Company's computer systems in the course of your employment. Where this is the case, the Company relies on you to help meet its data protection obligations to staff and to customers and clients.

If you have access to personal data, you are required:

- To access only data that you have authority to access and only for authorised purposes;
- Not to disclose data except to individuals (whether inside or outside the company) who have appropriate authorisation;
- To keep data secure by complying with rules on access to premises, access to computers including password protection and secure file storage and destruction;
- Not to remove personal data, or devices containing or that can be used to access personal data, from the company's premises without adopting appropriate security measures (such as encryption or password protection) to secure the data and the device; and
- Not to store personal data on local drives or on personal devices that are used for business purposes.

Failure to observe these requirements may amount to a disciplinary offence which will be dealt with under the Company's disciplinary procedure. Significant or deliberate breaches of this policy, such as accessing employee, customer or client data without authorisation or a legitimate reason to do so, may constitute gross misconduct and could lead to your dismissal without notice.

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.

E-mails can be the subject of legal action (for example, claims of defamation, breach of confidentiality or breach of contract) against both the person 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 everyone using the Company's system

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 chat rooms, blogs, social network sites
- 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 about the company or any person or organisation connected to the company,
- Unauthorised disclosure of personal data; and
- Loading or running unauthorised games or software

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.

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.

Name: John Jessimer

Signed: 

Position: Managing Director

Date: 7 January 2023

starfish
construction group