Information Security Policy

Ede's (UK) Ltd

IT Security

Technology is an integral part of our business. However, it also poses risks in terms of data breaches, reputational damage and financial impacts.

Any breach of the IT Security policy will be managed in line with the Disciplinary procedure, with a sanction up to and including gross misconduct (or termination of engagement). We may withdraw your internet and/or email access. Examples of gross misconduct are included within the Disciplinary procedure.

Use of the Company's Computer Systems

You may use our computer systems, or other electronic devices, for the purposes of our business. To reduce the risk to the Company's systems or network, these may only be accessed from your usual workplace (including your home address where this has been agreed) or other Company premises using authorised equipment, or remotely using authorised equipment via secure means.

You must never access the Company's systems or networks using an unsecure Wi-Fi connection.

Email use — general

All communications, including email, should reflect the highest professional standards at all times. You should ensure that you check all emails before sending for accuracy and ensure they are being sent to the correct recipient.

All emails should be sent from your own business email address, unless otherwise authorised in the proper performance of a colleague's duties and only for business-related communications. If you receive an inappropriate message, you must delete it immediately and report it. Whilst we have antivirus software, this does not eliminate risk. Be careful when opening unknown emails and report them to No One Internet Ltd if the email is suspicious. You should use password protection of emails where appropriate.

Emails — personal use and monitoring

The email system is primarily for business use. Any personal emails must be minimal and reasonable and take place mainly outside of normal working hours. Personal emails must not affect job performance or otherwise interfere with the business. You should not use the Company email system for personal emails.

We may monitor Company email and instant messaging systems or a network to see if an email is relevant and appropriate to our business, and in other instances not limited to but including:

- Establishing the facts in an investigation.
- Checking you are following legal and Company guidelines for using the system.
- Checking employees using the system in the course of their duties are in line with contractual requirements, Company policy or data protection rights.
- Investigating or detecting the unauthorised use of the system.
- Preventing or detecting crime.
- Responding to, or reviewing, emails in your absence.

Internet use

Internet use in Company time should be for work-related issues. Reasonable, limited personal use of the internet is permitted. Any unauthorised use of the internet is strictly prohibited, and we may therefore monitor internet usage (including searches made, the IP addresses of sites visited, and the duration and frequency of visits) if we suspect that an individual has been using the internet inappropriately and in a way that is potentially detrimental to the Company, such as:

- Viewing material that is pornographic, illegal, criminal, offensive, obscene, in bad taste or immoral and/or which is liable to cause embarrassment to us, our staff or to our clients/customers or supplier.
- By spending an excessive amount of time creating, viewing or accessing any webpage, or posting, transmitting or downloading any image, file or other information that is unrelated to your employment.
- Engaging in computer hacking and/or other related activities.
- Attempting to disable or compromise security of information contained on our systems or network of those of a third party.

Monitoring may include internet usage at the workplace, internet usage outside the workplace during working hours using Company systems or network, and internet usage using hand-held or portable electronic devices.

You must not publish confidential or sensitive information or use the Company name in any internet posting (inside or outside work) unless it is approved by your line manager. Information posted or viewed on the internet may constitute published material, so check if it is protected by copyright and meets licence conditions.

In some instances, we may block or restrict access to individual websites.

Internet — personal use

Reasonable personal use of our systems or network to browse the internet is allowed provided that it does not interfere with the performance of your duties and that the terms of the IT Security policy are strictly adhered to. We reserve the right, at our absolute discretion, to withdraw this privilege at any time and/or to restrict access for personal use.

Personal use must meet the following conditions (in addition to those set out elsewhere in this policy): the time spent, and frequency, must be minimal and reasonable and should take place mainly outside normal working hours, i.e., during lunch or other breaks, or before and after work. The golden rule is that it must not affect the job performance of any member of staff or otherwise interfere with our business. In addition, it must not commit the Company to any costs.

Passwords and security

You must use passwords on all IT equipment allocated to you. You must keep them confidential and change them regularly. You must not use another person's username and/or password to access our systems or network, nor allow any other person to use your password(s) unless required for business reasons.

Bring your own device

Before using your device at work to connect to the Company's IT systems and/or to access Company information, you must ensure that you follow Company guidelines by discussing this with your line manager. We accept no liability for use of your own devices at work. All confidential information must be transferred to the Company on leaving employment with us.

Off-site work

Remember that when working off-site, others may be able to view or attempt to access your device. Lock your device when appropriate and do not leave it unattended. Be aware of who can see your screen and avoid using confidential information. You must ensure any internet connection that you use is secure. Your device must be transported securely whilst travelling and should not be left on display in an unoccupied vehicle.

Social media

Any social media produced in the Company name must be approved by Dave Matthews. It must reflect our values and be in our best interests, be grammatically correct, accurate, objectively justifiable, reasonable and appropriate.

Never use your work email address to sign up for personal social media. Please be aware that we may monitor social media use in the same way as we monitor internet usage. Remember that even if you are using social media in a personal capacity, other users who are aware of your association with us might reasonably think that you speak on our behalf and damage our reputation. Harassment, bullying or inappropriate behaviour on social media will be dealt with in the same manner as if the conduct had happened in the workplace and may result in disciplinary action being taken.

Any contacts created on social media through your employment with the Company are the property of the Company.

Employees using messaging platforms as a communication tool with work colleagues (for example, WhatsApp, Snapchat etc) should be professional and respectful in their language and conduct. Harassment, bullying or inappropriate communication will not be accepted and may result in disciplinary action being taken.