Email and Internet Acceptable Use Policy

Version 2.1

This document sets out the Email and Internet Acceptable Use Policy for Magic Beans Group Limited

Document Responsibility	***Operations Director***	Created	***04/06/2021***

Contents

Introduction

The purpose of this policy is to protect the quality and integrity of the company's electronic communications and to provide employees with standards of behaviour when using them. Any breach of this policy or misuse of electronic communications may constitute a serious disciplinary matter and may lead to dismissal.

Policy

It is the policy of the company to encourage the use of its email and internet services to share information, to improve communication and to prohibit unauthorised and improper use of these means of communication. Use of the internet and email facilities is permitted and encouraged for business purposes and supports the goals and objectives of the company. It is to be used in a manner that is consistent with the company's standards of business conduct and as part of the normal execution of an employee's job responsibilities. Those who use the company's internet and email services are expected to do so responsibly and must comply with this policy.

Access

We reserve the right to designate those employees to whom it will provide access to the internet and email services and may revoke access at any time to persons who misuse the system. The company's computer equipment and systems must only be accessed and operated by those authorised to do so. Unauthorised use, intentional interference with the normal operation of the network or failure to comply with this policy will be regarded as gross misconduct and may lead to dismissal and possible criminal prosecution.

Viruses

All computers should use authorised and current anti-virus protection software. No unauthorised anti-virus software should be installed, transmitted, or downloaded.

Security

All software downloaded to a company computer must be approved by a member of the senior management team before installation to assure compatibility with software already installed on the computer. No software may be brought in from an employee's home and used on the company's system at any time.

Employees must not download software or electronic files without implementing virus protection. All files attached to external email as well as files downloaded from the internet must be scanned. Users must report suspected incidents of software viruses or similar contaminants from email attachments and/or downloads from the internet immediately to the Operations Director or IT Officer.

Passwords, encryption keys and other confidential information relating to the company's systems must not be transmitted over the internet or by email.

Employees must not change or use another person's files, output, or username for which they do not have express authorisation. Employees should use password protection or switch off their computer when away from it.

Monitoring

By accessing the internet and email services through facilities provided by the company the user acknowledges that the company can monitor and examine all individual connections and communications. The company respects the privacy of internet and email users and will not monitor email or internet access activities without an employee's knowledge or without good cause. Any such monitoring will comply with the provisions of the Data Protection Act 1998 and the General Data Protection Regulations 2018.

Prohibited Use

Employees must not view, store, transmit, upload, download or intentionally receive communications, web pages, files or documents that are or could be interpreted as intimidating, harassing or illegal or containing hostile, degrading, sexually explicit, pornographic, discriminatory, or otherwise offensive material.

Email Use

As well as the many benefits of email, it is essential that all employees realise the following potential pitfalls:

- It is not an informal communication tool, but has the same authority as any othercommunication to and from the company;
- It should be regarded as published information;
- Emails are not confidential and can be read by anyone given sufficient levels of expertise;
- Binding contracts may be inadvertently created;
- Defamation of colleagues or other parties (deliberate or otherwise) may occur;
- Abrupt, inappropriate and unthinking use of language can lead to a bullying tone and possible offence to others, even harassment, for example, capitals are often interpreted as shouting;
- Consider whether a phone call may be a better way of discussing a complex or confidential matter.

Email Retention

Staff should retain all emails in their deleted and sent folders for at least three months to ensure auditable process compliance.

Phishing Awareness

All staff have a responsibility to complete mandatory phishing training when allocated.

All suspected phishing emails must be reported to the IT Team via the Phishing Tackle 'phish hook' within Outlook.

Confidentiality

Email can be inadvertently sent to the wrong address. It may also be read by someone other than the intended recipient. Caution must be exercised when communicating sensitive information or information relating to the company when using email systems and users should ensure that they have the authority to send it.

No personal information should be sent without the prior consent of the individual.

Copyright

Employees must adhere to all intellectual property and copyright law. Employees must not upload, download, or otherwise transmit any copyrighted materials belonging to parties outside the company without the copyright holder's written permission.

Personal Use

Company email and internet systems may not be used for personal purposes.

Personal emails must not be sent using company email accounts.

Personal devices should not be connected to company Wi-Fi at any time.

E-Safety

The development and expansion of the use of ICT, particularly of the internet, social media sites and mobile devices, has transformed learning in recent years.

Our E-safety policy is to ensure that all staff and learners/apprentices are trained to ensure that young people are safe and are protected from potential harm. The potential for excessive use, which may impact on the social and emotional development and learning of the young person. As with all other risks, it is impossible to eliminate them completely. It is therefore essential, through good educational provision to build learner's understanding of the risks to which they may be exposed, so that they have the confidence and skills to face and deal with these risks.

All staff and learners/apprentices are to be educated in;

- Access to illegal, harmful, or inappropriate images or other content.
- Unauthorised access to/loss of/sharing of personal information.
- The risk of being subject to grooming by those with whom they make contact on the internet, through social media sites and on mobile devices.

- The sharing/distribution of personal images without an individual's consent or knowledge.
- Inappropriate communication/contact with others, including strangers.
- Cyber-bullying.
- Access to unsuitable video/internet games/films.
- An inability to evaluate the quality, accuracy, and relevance of information on the internet.
- Plagiarism and copyright infringement.
- Illegal downloading of music or video files.
- Access to gambling arenas that are not age appropriate and may result in consequences that may affect a young person in the long term.

Anyone attending a training course/apprenticeship with Qdos Training are asked to respect that centres are run as any other workplace.

Contracts

Employees should be aware that contracts which bind the company can be created on the internet or by email. Employees must not enter into contracts or subscribe for, order, purchase, sell or advertise for sale any goods or services on the internet or by email, unless with the express authorisation of the company.

Disciplinary Action

Any breach of this policy may be subject to disciplinary action, up to and including dismissal and may result in criminal prosecution.

Contact Person

Employees should contact the Operations Director if they have any queries about any aspect of the policy.

Linked Policies

MBG001 - Acceptable use of IT Policy

Policy Revision & Review

Version No	Revision Description	Section	Date of Revision	Approved By
2.0	Policy Format Update including change to policy owner	All Policy Update	17/11/2022	Operations Director
	Change of roles – Operations Director/IT Officer	Security	17/11/2022	Operations Director
2.1	Addition of Phishing Awareness and Email retention to policy	Phishing Awareness / Email Retention	31/01/2023	Operations Director
	Update to Personal Use section of the policy – Personal use of company email / Personal emails / Personal devices using company Wi-Fi	Personal Use	31/01/2023	Operations Director