Whistle IT Policy (Version 1.0)

Introduction

The Whistle Remote IT (Information Technology) policy is a guideline for Whistle's remote staff who will have access to Whistle's data and Whistle's client data. This policy must be followed by all remote staff and covers such topics as:

- Acceptable Usage
- Security
- Software Usage
- Internet and Email Usage

Acceptable Usage

Whistle's software and tools must be used and accessed responsibly by all remote staff who must respect the integrity of the network and data to which they have access to. Whistle remote staff must not:

- Use their computer to knowingly access or distribute illegal or inappropriate materials

- Use their computer or network resources for the purpose of gaining unauthorised access to the accounts, systems or equipment of any third party. Attempts at ‘hacking’ may result in criminal prosecution

- Use Whistle resources for commercial activities or to otherwise further commercial objectives which are not a part of their work in Whistle

- Infringe the copyright, patent or other intellectual property rights of any person including, downloading unlicensed software or other unauthorised materials

- Infringe the data protection or other privacy rights of any person

- Access, modify, or interfere with material and data, belonging to Whistle or another user, except with their express permission.

Security

Good security is essential to Whistle so there are a number of security measures Whistle remote staff are required to follow:

- Strong passwords must be used for accessing all systems
- Two Factor Authentication should be employed where possible (Authenticator app)
- Passwords should not be sent by email
- Computers must be locked or password protected when left unattended
- Remote staff must not share logins or usernames, transfer them to other users, or divulge passwords to other users
- Remote staff must not knowingly introduce any virus, malware or other destructive programs that could compromise Whistle's data
- **When computers are not being used they must be locked away in a secure safe**

Software Usage

Whistle remote staff accessing Whistle data and environments must agree to the following conditions:

- Legal versions of the software must be installed on staff computers
- All software must be used in accordance with the software's own license agreements. This can be checked with Whistle IT as required
- Remote staff allow Whistle IT to perform regular security and maintenance on their remote computers

Internet and Email Usage

Whistle staff are expected to use the Internet and email responsibly and productively. Internet and email access is limited to job-related activities and must not be used for:

- Sending or posting discriminatory, harassing, or threatening messages or images on the Internet or via Whistle's email service
- Using computers to perpetrate any form of fraud, and/or software, film or music piracy
- Stealing, using, or disclosing someone else's password without authorization
- Downloading, copying or pirating software and electronic files that are copyrighted or without authorization
- Sharing confidential material, trade secrets, or proprietary information outside the Whistle organization
- Hacking into unauthorized websites
- Sending or posting information that is defamatory to the Whistle, its products/services, colleagues and/or customers
- Introducing malicious software onto the Whistle networks and/or jeopardizing the security of the organization's electronic communications systems
- Sending or posting chain letters, solicitations, or advertisements not related to business purposes or activities
- Passing off personal views as representing those of Whistle

Signed:

Print Name_____ Date_____

Signature_____