ACCEPTABLE USAGE POLICY

1. Overview

The purpose of this policy is to establish acceptable and unacceptable use of electronic devices and network resources at the Music for Schools Foundation (the "Company") in conjunction with its established culture of ethical and lawful behavior, openness, trust, and integrity.

The Company provides computer devices, networks, and other electronic information systems and must manage them responsibly to maintain the confidentiality, integrity, and availability of its information assets. This policy requires the users of information assets to comply with company policies and protects the company against damaging legal issues.

2. Scope

All employees, contractors, consultants, temporary and other workers at The Company, including all personnel affiliated with third parties must adhere to this policy. This policy applies to information assets owned or leased by the Company, or to devices that connect to a Company network or reside at a Company site.

3. Policy Statement

3.1 General Requirements

3.1.1 You are responsible for exercising good judgment regarding appropriate use of Company resources in accordance with Company policies, standards, and guidelines. Resources may not be used for any unlawful or prohibited purpose.

3.1.2 For security, compliance, and maintenance purposes, authorized personnel may monitor and audit equipment, systems, and network traffic. Devices that interfere with other devices or users on the Company network may be disconnected. Information Security prohibits actively blocking authorized audit scans. Firewalls and other blocking technologies must permit access to the scan sources.

3.2 System Accounts

3.2.1 You are responsible for the security of data, accounts, and systems under your control. Keep passwords secure and do not share account or password information with anyone, including other personnel, family, or friends. Providing access to another individual, either deliberately or through failure to secure its access, is a violation of this policy.

3.2.2 You must maintain system-level and user-level passwords in accordance with section 9.3 of the Company IT and Data Security Policy.

3.2.3 You must ensure through legal or technical means that proprietary information remains within the control of The Company at all times. Conducting Company

business that results in the storage of proprietary information on personal or non-Company controlled environments, including devices maintained by a third party with whom The Company does not have a contractual agreement, is prohibited. This specifically prohibits the use of an e-mail account that is not provided by The Company, or its partners, for Company Business.

3.3 **Computing Assets**

3.3.1 All PC's, PDAs, laptops, and workstations must be secured with a password-protected screensaver with the automatic activation feature set to 5 minutes or less. You must lock the screen or log off when the device is unattended.

3.3.2 Do not interfere with corporate device management or security system software.

3.4 **Network Use**

You are responsible for the security and appropriate use of Company network resources under your control. Using Company resources for the following is strictly prohibited.

3.4.1 Causing a security breach to either Company or other network resources, including, but not limited to, accessing data, servers, or accounts to which you are not authorized; circumventing user authentication on any device; or sniffing network traffic.

3.4.2 Causing a disruption of service to either Company or other network resources, including, but not limited to, ICMP floods, packet spoofing, denial of service, heap or buffer overflows, and forged routing information for malicious purposes.

3.4.3 Introducing honeypots, honeynets, or similar technology on the Company network.

3.4.4 Violating copyright law, including, but not limited to, illegally duplicating or transmitting copyrighted pictures, music, video, and software.

3.4.5 Use of the Internet or Company network that violates the Company policies, or local laws.

3.4.6 Intentionally introducing malicious code, including, but not limited to, viruses, worms, Trojan horses, e-mail bombs, spyware, adware, and keyloggers.

3.5 **Electronic Communications**

The Following are strictly prohibited:

3.5.1 Inappropriate use of communication vehicles and equipment, including, but not limited to, supporting illegal activities, and procuring or transmitting material that violates Company policies against harassment or the safeguarding of confidential or proprietary information.

3.5.2 Sending Spam via e-mail, text messages, pages, instant messages, voice mail, or other forms of electronic communication.

3.5.3 Forging, misrepresenting, obscuring, suppressing, or replacing a user identity on any electronic communication to mislead the recipient about the sender.

3.5.4 Use of a Company e-mail or IP address to engage in conduct that violates Company policies or guidelines. Posting to a public newsgroup, forum, Social Media site (or similar) with a Company e-mail or IP address represents the Music for Schools Foundation to the public; therefore, you must exercise good judgement to avoid misrepresenting or exceeding your authority in representing the opinion of the company.

4. Enforcement

An employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment. A violation of this policy by a temporary worker, contractor or vendor may result in the termination of their contract or assignment with the Music for Schools Foundation.

5. Policy Review

The Company shall review this Policy not less than annually and otherwise as required in order to ensure that it remains up-to-date and fit for purpose. You will be notified of any change(s) to this policy immediately upon such change(s) being made.

6. Implementation of Policy

This Policy shall be deemed effective as of 24th May 2018. No part of this Policy shall have retroactive effect and shall thus apply only to matters occurring on or after this date.

This Policy has been approved and authorised by:

Name: Ali Wooding

Position: Head of Service

Date: 24th May 2018

Due for Review by: 24th May 2019

Signature: