**BLACKPOOL MUSIC SCHOOL**

**Information Technology/Security and Social Media Policy**

**Feb 2024**

In this document the term 'BMS' relates to the charity known as Blackpool Music School.

# Introduction

This policy sets out what is and what is not acceptable behaviour when using the computer facilities on behalf of the work of the organisation and includes use of (but not limited to) the internet, smart phones, social media and networking websites.

# Scope

This policy applies to all employees, Trustees, volunteers and anyone engaged with the organisation to carry out its services.

Any deviation from this policy may be subject to disciplinary review or other appropriate action.

# Overview and Definitions

* 1. **Information Security**

The security of information/data covers three main aspects:

**Confidentiality** (**C**), i.e. to protect information/data from breaches, unauthorised disclosures, or unauthorised viewing.

**Integrity** (**I**), i.e. to retain the integrity of the information/data by not allowing it to be modified or deleted maliciously or accidentally.

**Availability** (**A**), i.e. to maintain the availability of the information/data by protecting it from cyber-attacks, destruction, disruption and denial of service.

In addition to the core principles of **C**, **I** and **A**, information security also relates to the protection of the organisation’s reputation. Reputational loss can occur when any of

these principles are breached.

Information/data” can be held in computerised digital form, but also covers

information/data held in printed form and hand-written. It is the organisation's policy to ensure that the use of documents, computers, mobile computing, mobile communications,

portable storage devices, mail, voice mail, voice communications in general, multimedia, postal services and fax machines must be controlled to prevent unauthorized use and to reduce security risks.

# Social Media

**Social media** is the term used for internet-based applications and web sites which help people keep in touch and enable them to interact. It allows people to share information, ideas and views.

Social media can affect communications amongst managers, employees, volunteers, donors, suppliers and job applicants; how organisations promote and control their reputation; and how colleagues treat one another. It can also distort what boundaries there are between home and work.

Misuse of IT and social media can create issues such as time-theft, defamation, loss of reputation, cyber-bullying, freedom of speech and the invasion of privacy as well as going against the General Data Protection Regulations and principles to which everyone must adhere.

# Legal Considerations

**The Human Rights Act 1998** Article 8 gives a 'right to respect for private and family life, home and correspondence'. Case law suggests that employees have a reasonable expectation of privacy in the workplace.

**General Data Protection Regulations (GDPR) May 2018 which** describes how organisations must collect, handle and store personal information.

**The Regulation of Investigatory Powers Act 2000** covers the extent to which organisations can use covert surveillance.

**Computer Misuse Act 1990** made it an offence to access any computer to which a person does not have an authorised right to use. The Act introduced three criminal offences:

1. Unauthorised access to computer material.
2. Unauthorised access with intent to commit or facilitate commission of further offences.
3. Unauthorised modification of computer material

# Roles and Responsibilities

* 1. **Chairperson**

The Chairperson is responsible for the overall management of information security, and should also ensure that all employees (if any), trustees, and volunteers are trained to understand, implement and maintain the security objectives set out in this policy and as detailed in any work instructions.

trained to

# IT Support

The person or persons fulfilling the role of IT support are responsible for operating within the confines of their authorisation in terms of upholding the confidentiality, integrity and access to personal and organisational information/data and not abusing their privileged access rights.

IT support personnel are also responsible for ensuring that any access rights, applications, tools and equipment provided to staff , trustees and volunteers are provided with the appropriate limitations to access rights, profiles and security measures that enables services to be delivered efficiently and effectively but without compromising security.

# All Staff (if any), Trustees and Volunteers

Information Security is the responsibility of all individuals, who are always expected to act

in a professional and responsible manner whilst conducting Centre business, in line with the charity's Code of Conduct. Individuals are responsible for information security and remain accountable for their actions in relation to the Centre's information and information systems. Individuals also have a responsibility not to compromise the Centre e.g. by sending defamatory or harassing electronic mail, or by making unauthorised purchases, and must also be aware that the confidentiality and integrity of information transmitted by E-mail or other means may not be guaranteed. No personal information about clients, colleagues or others must be given out by emails, social media or other means and all case studies etc MUST be made anonymously at all times. Any actions taken by staff that could potentially put clients and service users, staff or anyone else involved with the charity in danger or at risk will render themselves subject to immediate disciplinary action.

Access to the Internet via computing facilities provided by BMS is restricted to business use only.

Individuals granted access to BMS's information systems must only use their own login IDs,

keep their passwords private and must not share usernames or passwords with anyone else. Passwords should also be changed on a regular basis; it is recommended that they are changed every three months. They should ensure

that they understand their role and responsibilities, and that failure to comply with

this policy may result in the withdrawal of access rights and/or disciplinary action.

# Securing Data

The following section outlines the procedures to be used SEC to secure

essential organisational data. A summary of these procedures is shown in Appendix 1, taken from the National Cyber Security Centre’s “Small Charity Guide” (November 2018).

# Backing up “cloud” based applications

Whenever possible BMS will utilise “cloud” based resources and rely on the

provider of those resources to guarantee industry-wide best practice on the reliability and frequency of their data backup and recovery procedures.

When considering the use of cloud-based applications BMS will use the National Cyber Security Centre’s guidance on how to configure, deploy and use cloud services securely (https:/[/www.ncsc.](http://www.ncsc.gov.uk/collection/cloud-security))g[ov.uk/collection/cloud-security).](http://www.ncsc.gov.uk/collection/cloud-security))

# Backing up other digital information

Should any other computer-based data not be being supported by cloud-based applications any essential data will be backed up by BMS trustees at least once a week. The backups, whether on a USB, on a separate drive or a separate computer,

will be restricted so that they:

* + - Are not accessible by all staff or volunteers
    - Are not permanently connected (either physically or over a local network) to the device holding the original copy.

Ideally, the backup copies will be held off-site in a different physical location from the original copy.

# Lost or stolen devices

The majority of devices include free web-based tools that can mitigate the impact of their loss. Users of BMS phones, tablets and other devices are encouraged to use these tools which can:

* + - track the location of the device
    - remotely lock access to the device, to prevent other people using it
    - remotely erase the data stored on the device
    - retrieve a back up data stored on the device.

# Use of Wi-Fi Hotspots

BMS staff and volunteers undertaking BMS business are not allowed to connect

to the Internet using unknown or unsecured Wi-Fi hotspots, instead they should use a 3G or 4G mobile network, or a Virtual Private Network (VPN) provided by a

reputable service provider.

# Protection from Malware

Malware, i.e. malicious software, is software or web content that can harm the charity, usually through the deployment of viruses, which are self-copying programs that infect legitimate software. In order to protect against malware will carry out the following steps.

* + - Install and activate antivirus software on all computers, laptops and tablets.
    - Prevent the download or installation of any unauthorised software applications from unknown vendors/sources. Third party applications downloaded onto SEC phones or computers must be approved by the Chairperson and only downloaded from manufacturer-approved stores, such as Google Play or Apple App Store.
    - Ensure that operating systems on all BMS devices are always kept up to date with the latest versions from software developers, hardware suppliers and vendors. Operating systems, programs, phones and apps will be set to “automatically update” wherever this is an option.
    - Replace devices and operating systems when suppliers end their support for older models/versions and updates are no longer be available.
    - Use “firewalls” to create a “buffer zone” between the BMS network and external networks.
    - Raise awareness of malicious emails and scams to prevent phishing attacks trying to gain access to sensitive data.

# BMS Social Media Core Values

The following sets out the core values that BMS will deploy in the online social media community:

# Transparency in every social media engagement.

BMS does not condone manipulating the social media flow by creating “fake” destinations and posts designed to mislead followers and control a conversation. Every web site, Twitter “account”, or other online destination that is ultimately controlled by BMS or its associates must make that fact known to users and must

be authorised according to applicable internal protocols in order to track and monitor

BMS’s online presence. BMS also requires bloggers and social media influencers to act with transparency and honesty in all their dealings.

# Protection of our clients’ privacy.

This means that all staff and volunteers should be conscientious regarding any

Personally Identifiable Information (PII) that BMS collects, including how we collect, store, use, or share that PII, all of which should be done pursuant to BMS’s Personal Data Protection Policy – particular attention is made to point 5.3 above.

# Protection of individual's privacy.

BMS will balance the need for monitoring individual's safety and behaviour with their right to privacy.

# Protection of job applicants’ privacy.

BMS will be mindful of all legislative and regulatory requirements protecting the privacy of any job applicants and will not put pressure on applicants to grant access to online social media accounts nor make any unauthorised access to online social media accounts.

# Copyright

BMS and its associates will respect all copyrights, trademarks, rights of publicity, and other third‐party rights in the online social media space, including user‐ generated content (UGC).

# Responsibility in use of technology.

BMS personnel will not use or align BMS with any organisations or web sites that deploy the use of excessive tracking software, adware, malware or spyware.

# Maintaining Best Practice

BMS will utilise best practices, including listening to the online community, and compliance with applicable regulations to ensure that these online social media principles remain current and reflect the most up‐to‐date and appropriate standards of behaviour.

# Individuals’ Use of Online Social Media

There’s a big difference between speaking “on behalf of BMS” and speaking “about” BMS. This set of principles refers to those personal or unofficial online activities where staff and volunteers might refer to BMS.

# Adhere to the Code of Conduct and other applicable policies.

Anyone involved with BMS is subject to the Code of Conduct in every public

setting. In addition, other policies, including the Personal Data Protection Policy, govern individuals’ behaviour with respect to the disclosure of information;

these policies are applicable to all personal activities online, as well as the unauthorised removal or copying of personal or organisational information/data.

# Responsibility for your own actions.

Individuals should be aware that anything that they post online or email that

can potentially tarnish the organisation’s image will ultimately be their own responsibility.

We encourage individuals to participate in online social media, but urge

everyone to do so properly, exercising sound judgement and common sense.

# Pass on compliments and criticism.

Even if an individual is not an official spokesperson for BMS, they are recognised as one BMS’s most vital assets for monitoring social media. If you

come across positive or negative remarks about BMS or its associates, online that they believe are important, they should consider sharing them by forwarding them to the person tasked with BMS Public Relations.

# Senior Officer(s) respond to negative posts.

If staff or volunteers come across negative or disparaging emails/posts about BMS or its associates, or see third parties trying to spark negative conversations, unless they are an authorised spokesperson, they should avoid reacting to the post(s)

themselves. Individuals should pass the email(s)/post(s) along to the appropriate spokesperson trained to address such comments.

# Be conscious when mixing business and personal lives.

Online a person’s personal and business personas are likely to intersect. BMS respects the free speech rights of all of its associates, but likewise they must remember that clients, colleagues, donors and supporters often have access to the online content they post or email. BMS staff, trustees or volunteers are required to keep this in mind when publishing information online that can be seen by more than friends and family, and know that information originally intended just for friends and family can be forwarded on. Individuals must never to disclose non‐public information of BMS

(including confidential information), and be aware that taking public positions online that are counter to BMS’s interests might cause conflict.

# Online Spokespeople/Representatives

Just as with traditional media, BMS have an opportunity – and a responsibility – to effectively manage the group’s reputation online and to selectively engage and participate in social media. The following principles guide how authorised spokespeople should represent BMS in an online, official capacity when they are speaking on behalf of BMS:

1. Be trained in the use of Social Media.
2. Follow the Code of Conduct and all other Company policies, i.e. as a representative of BMS they must act with honesty and integrity in all matters
3. Be mindful that they are representing BMS. As an official representative, it is important that all posts be respectful of all individuals in accordance with the Equality and Diversity policy and associated legislation.
4. Fully disclose affiliation with BMS. BMS requires all associates who are communicating on behalf of BMS to always disclose their name and their affiliation. It is never acceptable to use aliases, to speak anonymously or otherwise deceive people.
5. Keep records. It is critical that representatives keep records of their interactions in the online social media space and monitor the activities of those with whom they engage. Because online conversations are often fleeting and immediate, it is important to keep track of them when officially representing BMS. Representatives must be aware that online BMS statements can be held to the same legal standards as traditional media communications.
6. When in doubt, do not post. Associates are personally responsible for their words and actions, wherever they are. Online spokespeople must ensure that their posts and emails are completely accurate and not misleading, and that they do not reveal non‐public information of BMS.
7. Give credit where credit is due and don’t violate others’ rights. Representatives must not claim authorship of something that is not theirs. If using another party’s content, they must make certain that they are credited for it in the post and that they approve of BMS utilising their content. Representatives must not use the copyrights, trademarks, publicity rights, or other rights of others without the necessary permissions of the rights holder(s).
8. BMS copyright. Any content generated by or on behalf of BMS will remain the copyright or BMS, and BMS will retain the Intellectual Property Rights of, for example, any original artwork, photography, video, music, web content and sound recordings.
9. Be responsible to your work. BMS understands that associates engage in online social media activities at work for legitimate purposes and that these activities may be helpful to BMS. However,BMS encourages all associates to exercise sound judgement and common sense to prevent online social media sites from becoming a distraction at work.
10. Remember that local posts can have global significance. The way that a spokesperson answers an online question might be accurate in some parts of the world, but inaccurate (offensive or even illegal) in others. Representatives should keep that “world view” in mind when participating in online conversations.
11. Know that the Internet is permanent. Once information is published online, it is essentially part of a permanent record, even if a person “removes/deletes” it later or attempts to make it anonymous. If a complete thought, along with its context, cannot be squeezed into a character‐restricted space (such as Twitter), it is good practice to provide a link to an online space where the message can be expressed completely and accurately.

# Equality and Diversity

We are committed to ensuring that the way it provides services to the public and the way staff are treated reflects their individual needs and does not discriminate against individuals or groups on any grounds. This policy has been appropriately assessed.

# Monitoring and Compliance

The Trustees will maintain effective monitoring systems to ensure implementation of this policy, including the following:

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Standard/**  **process / issue** | **Monitoring and audit** | | | |
| **Method:** | **By:** | **Reporting to:** | **Frequency:** |
| Breaches | Report of Incident | Nominated Trustee | Trustees | As and when incident occurs |
| Backup of locally held data | Regular Audit | Nominated Trustee | Trustees | Monthly |

Signed:

Chairperson

Blackpool Music School Date:

|  |  |  |
| --- | --- | --- |
| Approved | Reviewed | Amended |
|  |  |  |

National Cyber Security Centre - Guide for Small Charities Appendix 1

