Information Technology and Computer Use Policy

Policy Number:	P8
Responsible Post:	Office Manager
Date of first issue:	March 10
Date of this version: (date approved by Trustees)	27/03/17
Date of next review:	June 2020

Information technology and computer use policy statement

Introduction

IT communications are a key part of our business, and so it is crucial that we adhere to certain standards to protect all parties. This policy applies to all employees and volunteers, including those who work from home or remotely.

It must be remembered that our IT systems and associated facilities are primarily a business tool. We aim to take a fair and consistent approach to IT usage within the business.

To support this policy Beat has a procedural document - **Information technology and computer Use Guide** - which gives clear information of the standards Beat expects of its employees, and any volunteers with access to its IT. In addition it describes actions that could lead to disciplinary action.

We have established systems to –

- Manage our networks, administration and maintenance responsibly
- Maintain system security
- Provide secure email and internet facilities
- Allow personal use of our systems appropriately
- Monitor internet, email and computer usage
- Implement an effective virus security strategy
- Provide secure remote access for workers away from the main office
- Monitor external social media postings if there are concerns that they are not within Beat guidelines.

These include –

- Appointing an IT Support Services Provider
- Password protected access to our systems
- Clear guidance on the purpose and limitations of our email and internet facilities

- Allowing use of the internet for personal use outside of work hours
- Identifying any software downloaded by the user
- Checking whether the use of the system is legitimate.
- Guidance on inappropriate social media postings

All employees (and volunteers with access) are required to -

- Use confidential passwords which should not be disclosed to others
- Use our email and internet services in the way intended and not for inappropriate, bullying or abusive purposes.
- Ensure social media does not cause any personal distress to others or reputational damage to Beat.
- Ensure they do not use the internet for any purpose which may cause distress to another colleague or affect the reputation of Beat.
- Clearly mark personal emails
- Arrange suitable anti-virus software on their own devices if being used for Beat systems, and ensure adequate security is in place.

Email

Our email facilities are intended to promote effective and speedy communication on work-related matters. All employees who need to use email as part of their role will normally be given their own business email address and account. We may, at any time, withdraw email access to any employee or volunteer should we feel that this is no longer necessary for the role or that the system is being abused.

Any email, however confidential or damaging, may under certain circumstances be disclosed to third parties and messages can be disclosed in any legal action commenced against Beat relevant to the issues set out in the email. Deleted emails may still be recoverable and are regarded as legitimate forms of evidence in court.

Personal use of our IT systems

Email access is provided for business use, and although it is accepted that occasionally private email will be sent/received, this should be kept to a

minimum. It should be clearly understood that whilst we do not routinely monitor messages, we do reserve the right to monitor and to access any incoming or outgoing messages within our email system.

Messages may be read by other people and therefore anything of a strictly private or personal nature should not be sent or received using our email system. Reasonable access to personal email accounts is permitted and should be used for private or personal messages.

The Internet may be accessed during non-working time for viewing non-work related sites if this has been authorised in advance. However, the loading, sending or viewing of pornographic, non-licensed, suggestive, obscene or offensive material is not acceptable and may lead to disciplinary action, including dismissal as a possible outcome.

System monitoring

Internet, email and computer usage is continually monitored as part of our IT protection against computer viruses, our ongoing maintenance of the system, and when investigating faults.

Such monitoring and the retrieval of the content of any messages may be for the purposes of checking whether the use of the system is legitimate, to find lost messages or to retrieve messages lost due to computer failure, to assist in the investigation of wrongful acts, or to comply with any legal obligation.

We reserve the right to monitor all incoming and outgoing emails. This will normally occur in circumstances where we suspect the viewing or sending of offensive or illegal materials; discriminatory comments or those detrimental to the business; or excessive personal use of our email system.

Computer viruses

Beat's IT Provider is responsible for the implementation of an effective virus security strategy. All machines, networked and standalone, will have up to date anti-virus protection. Remote users will assist in the upgrade of anti-virus software by allowing access to their machines when so requested.

Unknown files or messages must never be introduced into the system without first being checked for viruses. ALL incoming material should be checked for viruses, whether loaded manually (e.g. from CDs or memory sticks) or transmitted from an external source such as the Internet.

Remote working

Beat provides a secure means of accessing Beat systems externally however prior permission for such access must be obtained from the user's line manager. Staff must only connect using software approved by Beat's IT Provider which will encrypt all data between the remote computer and Beat's systems.

Use of own devices

While not requiring this, Beat appreciates that employees may, where business need requires, wish to use their own devices to access our servers, private clouds or networks including, but not limited to, reading their emails, accessing documents or to store data on our server(s) or access data in other services, during normal working hours.

Social media

Inappropriate comments can adversely affect the reputation of Beat, even if it is not directly referenced. It should be noted that if comments/photographs are likely to be construed as linked to Beat or, in more direct cases, if comments about colleagues, volunteers or our service users could be regarded as abusive, humiliating, discriminatory or derogatory, or could constitute bullying or harassment, we will treat this as a serious disciplinary offence.

In addition, postings to websites should not breach copyright or other law or disclose confidential information, defame Beat or its suppliers, users, volunteers or employees, or disclose personal data or information about any individual that could breach the Data Protection Act 1998.

All Beat employees and volunteers with access to IT must comply with the guidance document or risk disciplinary action. Any concerns on the correct use of our systems should be directed to the Finance Director.