INTERNET, EMAIL & SOCIAL MEDIA POLICY

1. Policy Statement

This policy sets out the standards of behaviour expected of employees and contractors using BPM's computer networks (internet, email, computer facilities, and phones) or when referring to BPM Health's on external sites.

2. Scope

The primary purpose for which access to the internet and email is provided to employees and contractors is for work-related purposes in carrying out the duties of their employment.

Users are permitted to use BPM Health's computer network for limited and reasonable personal use. However, any such personal use must not impact the user's work performance or resources or violate this policy or any other policy.

3. Internet, Email and Computers - Prohibited Conduct

Users must not send (or cause to be sent), upload, download, use, retrieve, or access any email or material on BPM Health's computer network that:

- is obscene, offensive, inappropriate and illegal.
- may be defamatory or could adversely impact the image or reputation of the company.
- causes damage to the computer system in any way.
- gives the impression of, or is representing, giving opinions or making statements on behalf of the company or about the company without the express authority of the Director.

Users must not use BPM Health's computer network:

- to violate copyright or other intellectual property rights. Computer software that is protected by copyright is not to be copied from, into, or by using computing facilities, except as permitted by law or by contract with the owner of the copyright.
- to create any legal or contractual obligations on behalf of BPM Health unless expressly authorized
- to disclose any Confidential Information of BPM Health or any customer, client or supplier of BPM Health unless expressly authorized
- to install software or run unknown or unapproved programs on our computer network. Under no circumstances should users modify the software or hardware environments on our computer network
- to gain unauthorised access (hacking) into any other computer within or outside BPM or attempt to deprive other users of access to or use of any of our computer network, and use another user's computer network facilities (including passwords and usernames/login codes)
- to send chain or SPAM emails in any format

4. Social Media

Personal use of social media in the workplace is permitted, subject to certain conditions, as detailed below:

- It must not be abused or overused, and the company reserves the right to withdraw permission at any time.
- It must not involve unprofessional or inappropriate content.
- It must not be detrimental or damaging in any way to the company.
- It should not interfere with your employment responsibilities or productivity.
- Its use must be minimal and take place substantially outside of normal working hours, for example, breaks, lunchtime.

Any use of social media must be in accordance with this policy. The same rules would also apply when using social media outside of work:

- Do not post or forward a link to any abusive, discriminatory, harassing, derogatory, defamatory, or inappropriate content. This includes potentially offensive or derogatory remarks about any other individual (including but not limited to any colleagues or customers, clients, business partners, suppliers, vendors, or 3rd parties) or the company.
- A contractor or employee who feels that they have been harassed or bullied or are offended by material posted by a colleague onto a social media website should refer to BPM Health's Equal Opportunity, Bullying, Harassment & Discrimination Policy.
- Never disclose commercially sensitive, anti-competitive, private, or confidential information. If you are unsure whether the information you wish to share falls within one of these categories, you should discuss this with a manager or the Directors.
- Do not post material in breach of copyright or other intellectual property rights.
- Social media communications should be avoided that might be misconstrued in a way that could damage the company's reputation, even indirectly.
- Use privacy settings where appropriate but bear in mind that even comments in a restricted forum may be passed on.

5. Monitoring use of social media, email, and the internet

Staff should be aware that emails and any use of the internet and social media websites (whether or not accessed for work purposes) may be monitored and, where breaches of this policy are found, action may be taken under the company's Disciplinary Procedure.

The company reserves the right to restrict or prevent access to certain internet sites including social media websites if personal use is considered to be excessive. Monitoring is only carried out to the extent permitted or as required by law and as necessary and justifiable for business purposes.

Misuse of social media and other websites can, in certain circumstances, constitute a criminal offence or otherwise give rise to legal liability against you and the company.

6. Breaches of policy

Where it is believed that an employee has failed to comply with this policy, they will be subject to the company's disciplinary procedure.

You may be required to remove any social media content that BPM Health considers to constitute abreach of this policy. Failure to comply with such a request may in itself result in disciplinary action.

Policies Control

Current from	March 16th 2024
Replaces version	N/A
Approved by	Director