SOCIAL MEDIA, INTERNET AND EMAIL SECURITY POLICY

Who is covered by the policy

This policy applies to all staff including its directors or officers, contractors, home-workers, part-time and fixed-term employees, secondees, temporary staff, casual staff, agency staff and volunteers. This policy does not form part of your terms and conditions of employment and the organisation reserves a right to amend the policy at any time.

Purpose of policy

The policy is intended to help employees of the organisation make appropriate decisions about the use of internet, email and social media and social networking sites to include (but not limited to) to internet, video, picture and audio postings and blogging.

The policy applies to use of social media for business purposes as well as personal use that affects our business in any way.

This policy outlines the standards the organisation requires staff to observe when using the internet, email and social media, the circumstances in which the organisation will monitor your use of these media and the action that will be taken in respect of breaches of this policy.

The principles of this policy apply to use of these media regardless of the method used to access it and covers static and mobile IT/computer equipment, as well as work and/or personal smartphones etc.

Personnel responsible for implementing policy

The Board has overall responsibility for the effective operation of this policy, but has delegated day-to-day responsibility for its operation to the CEO.

Responsibility for monitoring and reviewing the operation of this policy and making recommendations for change to minimise risks lies with the CEO who will review this policy on an annual basis to ensure that it meets legal requirements and reflects best practice.

Managers have a specific responsibility for operating within the boundaries of this policy, ensuring that all staff understand the standards of behaviour expected of them and taking action when behaviour falls below its requirements.

All staff are responsible for the success of this policy and should ensure that they take the time to read and understand it. Any misuse of social media should be reported to the CEO. Questions regarding the content or application of this policy should be directed to the CEO.

Using work-related social media

Only the [position of relevant persons/team] is/are permitted to post material on a social media website in the company's name and behalf. Anyone who breaches this restriction will be subject to the company's disciplinary procedure.

Approved social media websites for the organisation are [insert list of sites eg Facebook, Twitter etc]. This list may be updated by [position of relevant person].

Before using work-related social media you must:

- have read and understood this policy and [refer to any other relevant policies and guidelines]; and
- have sought and gained prior written approval to do so from [position of relevant person].

The roles and functions which will be needed moving forward have been identified as follows: [insert functions and people responsible as applicable such as:

Any employee involved in the organisation's social media activities must remember that they are representing the organisation, use the same precautions as they would with any other communication and adhere to the following rules:

- Ensure that the purpose and benefit for the organisation is clear;
- Obtain permission from a manager before using social media; and
- Ensure the content is checked before it is published.

Personal use of 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 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; and
- It should comply with the terms of this policy and all other policies which might be relevant (to include but not limited to) the organisation's Equal Opportunities Policy, the Bullying & Harassment Policy, the GDPR Policy and Disciplinary Procedure.

You are also personally responsible for what you communicate on social media sites **outside the workplace**, for example at home, in your own time, using your own equipment. You must always be mindful of your contributions and what you disclose about the company.

General rules for social media use

Whenever you are permitted to use social media in accordance with this policy, you must adhere to the following general rules. 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.

- A member of staff who feels that they have been harassed or bullied, or are offended by material posted by a colleague onto a social media website should inform [insert position of relevant person].

- 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 [insert position of relevant person].

- Do not post material in breach of copyright or other intellectual property rights.

- Be honest and open, but be mindful of the impact your contribution might make to people's perceptions of the company.

- You are personally responsible for content you publish – be aware that it will be public for many years.

- When using social media for personal use, use a disclaimer, for example: 'The views expressed are my own and don't reflect the views of my employer'. Be aware though that even if you make it clear that your views on such topics do not represent those of the organisation, your comments could still damage our reputation.

- The employee's online profile must not contain the company name.

- You should avoid social media communications that might be misconstrued in a way that could damage our business reputation, even indirectly.

- Do not post anything that your colleagues or our customers, clients, business partners, suppliers or vendors would find offensive, insulting, obscene and/or discriminatory.

- Do use privacy settings where appropriate but bear in mind that even comments in a restricted forum may be passed on.

- If you have disclosed your affiliation as an employee of our organisation you must ensure that your profile and any content you post are consistent with the professional image you present to client and colleagues.

If you are concerned or uncertain about the appropriateness of any statement or posting, refrain from posting it until you have discussed it with your manager.

If you see social media content that disparages or reflects poorly on us, you should contact [your manager or department]

Use of the internet and email

Limited personal use of the internet and of email at work is acceptable provided it does not interfere with or impede your normal duties. Such use should take place substantially outside of normal working hours, for example, breaks, lunchtime.

Users may access non- business-related sites, but are personally responsible for what they view.

You should not engage in any activity which is illegal, offensive or likely to have negative repercussions for the company.

The Organisation employs software to block some non-business related and offensive websites.

Always ensure that the organisation is neither embarrassed nor liable in any way by your use of the internet.

You may not upload, download, use, retain, distribute or disseminate any images, text, materials or software which:

- Are or might be considered to be indecent, obscene or contain profanity;
- Are or might be offensive or abusive in that the context is or can be considered to be a personal attack, rude or personally critical, sexist, racist, or generally distasteful;
- Encourage or promote activities which make unproductive use of your time;
- Encourage or promote activities which would, if conducted, be illegal or unlawful;
- Involve activities outside the scope of your responsibilities – for example, unauthorised

selling/advertising of goods and services;
- Might affect or have the potential to affect the performance of, damage or overload system, network and/or external communications in any way;
- Might be defamatory or incur liability on the part of the organisation or adversely impact on the reputation.
- You must not include anything in an email which you cannot or are not prepared to account for.

You must not make any statements on your own behalf or on behalf of the organisation which do or may defame or damage the reputation of any person.

Care should be taken when adding attachments to your Outlook email.

Attachments to emails should only be used when strictly necessary. When hyperlinks are available these should be used. Large files should be compressed and key information from small files may be cut and pasted into the email itself.

Remember that a phone call or face to face discussion may often be more appropriate than an email, bearing in mind that an email may be misinterpreted or lead to a chain reaction. Also, consider carefully who really needs to be copied on emails. Unnecessary email can be a major distraction.

Access to all email Internet sites (e.g. Hotmail, Yahoo mail etc.) is restricted to your 'own time' as defined above.

You must not download any software, executable files or potentially offensive graphic image files (GIFs and JPGs) unless you have obtained prior permission from the organisation.

The following activities are expressly prohibited:

- The introduction of network monitoring or password detecting software on user machine or part of the network;
- Seeking to gain access to restricted areas of the network;
- The introduction of any form of computer virus;
- Other hacking activities;
- Knowingly seeking to access data which you know, or ought to know, to be confidential and therefore would constitute unauthorised access.

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.

If you notice any use of social media by other members of staff in breach of this policy please report it to [position of relevant person such as line manager].

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. If the employee is found to have breached the policy, they will face a disciplinary penalty ranging from a verbal warning to dismissal.

The penalty applied will depend on factors such as the seriousness of the breach; the nature of the posting; the impact it has had on the organisation or the individual concerned; whether the comments cause problems given the employee's role; whether the employer can be identified by the postings; other mitigating factors such as the employee's disciplinary record etc.

Any member of staff suspected of committing a breach of this policy will be required to co-operate with the organisation's investigation, which may involve handing over relevant passwords and login details

You may be required to remove any social media content the organisation considers to constitute a breach of this policy. Failure to comply with such a request may in itself result in disciplinary action.