USE OF INTERNET AND SOCIAL MEDIA POLICY

This Internet and Social Media Usage Policy applies to all employees/associates of Beacon-East who have access to computers and the Internet to be used in the performance of their work. Use of the Internet by employees/associates of Beacon-East is permitted and encouraged where such use supports the goals and objectives of the business. However, access to the internet through Beacon East is a privilege and all employees/associates must adhere to the policies concerning computer, email and internet usage. Violation of these policies could result in disciplinary and/or legal action leading up to and including termination of employment. Employees/associates may also be held personally liable for damages caused by any violations of this policy. All employees/associates are required to acknowledge receipt and confirm that they have understood and agree to abide to the company policy and policies of schools they work in.

General Data Protection

In May 2018 the General Data Protection Regulation (GDPR) replaced the Data Protection Act of 1998 and brought about the biggest change to data protection laws in over 20 years. In general it introduced stricter rules on how firms and organisations handle and use of personal data. In particular, the new directive takes aim at how sensitive customer information is processed, stored and exchanged among businesses. This also includes the use of the internet and social media.

The act concentrates on personal data and the main differences is on how we get, keep and protect personal data. It applies to all organisations within the EU holding information about individuals worldwide and worldwide organisations must protect personal data for all EU citizens, personal data kept on identifiable individuals i.e. all personal data relating to living individuals that is held on either computer database or in a structured paper filing system. GDPR gives more power to people over how their personal data is used and make it easier for them to access it.

Background Information - Internet

This policy is designed to guide staff/associates in the acceptable use of telephone, computer and information systems and networks (including local and hard drives, Internet, email and other electronic technologies) provided by Beacon-East.

This policy is intended to be read in conjunction with other relevant policies which includes but are not limited to; the respective codes of conduct relating to staff and associates; the policy on Discrimination and Harassment and the applicable grievance management policies.

Subject to the above understanding, all staff and associates are encouraged to make innovative and creative use of information technologies in support of education and own research. Access to information representing a multitude of views on current and historical issues is allowed for the information and enlightenment of clients.

Consistent with other policies, this policy is intended to respect the rights of individuals and articulate the obligations of academic freedom. The company recognises that the purpose of copyright is to protect the rights of the creators of intellectual property and to prevent the unauthorised use of commercial products.

The company cannot guarantee the protection of individuals against the existence or receipt of material that may be offensive to them. As such, those who make use of electronic communications are warned that they may traverse or be recipients of material they find offensive.

Those who use telephones email and/or make information about themselves available on the Internet should be aware that invasions of privacy may sometimes occur and the University cannot protect users from technological abuse. Users are reminded that email should not be used to send sensitive and confidential information unless appropriate security measures, including encryption, have been taken.

Computer, email and internet usage

- When working company employees/associates are expected to use the Internet responsibly and productively. Internet access should be limited to job-related activities only.
- Job-related activities include research and educational tasks that may be found via the Internet that would help in an employee's role.
- All Internet data that is composed, transmitted and/or received by Beacon-East's computer systems is considered to belong to Beacon-East and is recognized as part of its official data. It is therefore subject to disclosure for legal reasons or to other appropriate third parties
- The equipment, services and technology used to access the Internet are the property of Beacon-East and the company reserves the right to monitor Internet traffic and monitor and access data that is composed, sent or received through its online connections
- Emails sent via the company email system should not contain content that is deemed to be offensive. This includes, though is not restricted to, the use of vulgar or harassing language/images

Unacceptable use of the internet by employees includes, but is not limited to:

- Sending or posting discriminatory, harassing, or threatening messages or images on the Internet or via Beacon-East's email service
- Using computers to perpetrate any form of fraud, and/or software, film or music piracy
- Stealing, using, or disclosing someone else's password without authorisation

- Downloading, copying or pirating software and electronic files that are copyrighted or without authorisation

- Sharing confidential material, trade secrets, or proprietary information outside of the organisation

- Hacking into unauthorized websites

- Sending or posting information that is defamatory to the company, its products/services, colleagues and/or customers

- Introducing malicious software onto the company network and/or jeopardizing the security of the organization's electronic communications systems

- Sending or posting chain letters, solicitations, or advertisements not related to business purposes or activities

- Passing off personal views as representing those of the organization

Under no circumstances will the company tolerate misuse of it's IT facilities for harassment including but not limited to unlawful harassment such as sexual harassment. Further details of what constitutes harassment may be found in the company's policy on Discrimination and Harassment. If a person using any of the IT facilities believes that she/he has been harassed as a result of an electronically transmitted message (or otherwise) it is important that the message (or applicable material) not be erased.

Rather, the message should be saved and the origin, date, time and location of the message should be written down and the procedure followed in the applicable company grievance management policy.

Users must not purport to express views on behalf of the company without official authorisation to do so, or to cause another person to reasonably misconstrue that a personal view represents the official position of the company.

Users must remember that information distributed through Beacon East's IT Facilities is a form of publishing, and many of the same standards apply.

Security

Users are not permitted to gain access to the Website other than through an authorised account registered in their name. Users must not supply false or misleading data nor improperly obtain another's password in order to gain access to company computers or network systems, data or information. The negligence of another user in revealing an account name or password does not constitute authorised use. Users should not attempt to subvert the restrictions associated with their computer accounts.

Users are responsible for all use of their company computer account(s). They should make appropriate use of the system and network-provided protection features and take precautions against others obtaining access to their computer resources. Individual password security is the responsibility of each user.

Use of Social Media when representing Beacon East

Beacon-East is committed to making the best use of all available technology and innovation to improve the way we do business. This includes using all reasonable and cost-effective means to improve the way we communicate, reach out and interact with the different clients and partners we serve.

'Social media' is the term commonly given to web-based tools which allow users to interact with each other in some way – by sharing information, opinions, knowledge and interests online. As the name implies, social media involves the building of online communities or networks to encourage participation and engagement.

These platforms open up many new and exciting opportunities. However, the practical application of such technology by the company is continually developing and there are many potential issues to consider – both as individual employees and as an organisation.

To avoid major mistakes which could result in reputational, legal and ethical issues, and misuse/abuse of a well functioning social media relationship, it is important that we **manage** any potential risks through a common-sense approach and framework as well as proactively monitoring the development of such applications.

Definition of social media

For the purposes of this policy, social media is a type of interactive online media that allows parties to communicate instantly with each other or to share data in a public forum. This includes e-mail, online social forums, blogs, video- and image-sharing websites and similar facilities.

Staff/associates should be aware that there are many more examples of social media than can be listed here and this is a constantly changing area and should follow these guidelines in relation to any social media that they use.

Use of social media

Where the company encourages employees to make reasonable and appropriate use of social media websites as part of their work, it is recognised that it is an important part of how we communicates with our audiences and allows communication and networking between staff and partners.

Staff/associates may contribute to the University's social media activities, for example by writing for blogs, managing a social media account and running an official social communications account for the company.

Beacon-East understands that staff/associates may wish to use their own computers or devices, such as laptops, tablets and mobile telephones, to access social media websites while they are at work. Such use should nonetheless be in accordance with these guidelines.

Employees must be aware at all times that, while contributing to the company's social media activities, they are representing Beacon-East. Staff who use social media as part of their job must adhere to the following safeguards.

Employees should use the same safeguards as they would with any other form of communication about the University in the public sphere. These safeguards include:

- making sure that the communication has a purpose and a benefit for the company;
- obtaining permission from M Bruhin before embarking on a public campaign using social media; and
- getting a colleague to check the content before it is published.

Any communications that employees/associates make in a professional capacity through social media must not:

Breach confidentiality, for example by:

- revealing confidential intellectual property or information owned by the company or;
- giving away confidential information about an individual (such as a colleague or partner contact) or organisation (such as a partner institution); or
- discussing the company's internal workings (such as agreements that it is reaching with partner institutions/customers or its future business plans that have not been communicated to the public) or;
- do anything that could be considered discriminatory against, or bullying or harassment of, any individual, for example by:
- making offensive or derogatory comments relating to sex, gender reassignment, race (including nationality), disability, sexual orientation, religion or belief or age or;
- using social media to bully another individual (such as an employee of the University); or
- posting images that are discriminatory or offensive or links to such content or;

bring Beacon-East into disrepute, for example by:

- criticising or arguing with students, customers, colleagues, partners or competitors or;
- making defamatory comments about individuals or other organisations or groups; or
- posting images that are inappropriate or links to inappropriate content or;
- breach copyright, for example by:
- using someone else's images or written content without permission; or
- failing to give acknowledgement where permission has been given to reproduce something.

Social media in your personal life

Beacon East recognises that many employees make use of social media in a personal capacity. While they are not acting on behalf of the company, employees

must be aware that they can damage the company if they are recognised as being one of our employees.

Staff and Associates are allowed to say that they work for Beacon-East, which recognises that it is natural for its staff sometimes to want to discuss their work on social media. The employee's online profile (for example, the name of a blog or a Twitter name) may contain the company's name, but should be focussed to the area in which the employee works.

If staff do discuss their work on social media (for example, giving opinions on their specialism or the sector in which the company operates), they should include on their profile a statement along the following lines: "The views I express here are mine alone and do not necessarily reflect the views of my employer."

Any communications that employees make in a personal capacity through social media must not:

- breach confidentiality, for example by:
- revealing confidential intellectual property or information owned by the company or;
- giving away confidential information about an individual (such as a colleague or partner contact) or organisation (such as a partner institution); or
- discussing the company's internal workings (such as agreements that it is reaching with partner institutions/customers or its future business plans that have not been communicated to the public) or;
- do anything that could be considered discriminatory against, or bullying or harassment of, any individual, for example by:
- making offensive or derogatory comments relating to sex, gender reassignment, race (including nationality), disability, sexual orientation, religion or belief or age or;
- using social media to bully another individual (such as an employee of the company) or;
- posting images that are discriminatory or offensive or links to such content or;
- bring the company into disrepute, for example by:
- criticising or arguing with students, clients, colleagues partners or competitors or;
- making defamatory comments about individuals or other organisations or groups or;
- posting images that are inappropriate or links to inappropriate content or;
- breach copyright, for example by:
- using someone else's images or written content without permission; or
- failing to give acknowledgement where permission has been given to reproduce something.

Disciplinary action over Internet and social media use

All staff/associates are required to adhere to these guidelines. Employees should be aware that use of Social Media in a way that may be deemed as deliberate or inadvertent misuse which could be a breach of these guidelines, may lead to

disciplinary action. Serious breaches of these guidelines, for example incidents of bullying of colleagues or social media activity causing serious damage to the company, may constitute gross misconduct and may lead to action under the disciplinary procedure up to and including dismissal.

If an employee is unsure about what constituted acceptable Internet and social media usage, then he/she should ask M Bruhin for further guidance and clarification.

Policy Review

Beacon-East may make changes to this policy from time to time to improve the effectiveness of its operation. Staff/associate members who wish to make comments about this policy may forward suggestions to Mark Bruhin.

The company contact for this policy is Mark Bruhin who can be contacted at:
E Mail: mbruhin@beacon-east.co.uk Tel: 01603 673340 / 07766 056330