Brídhaven
Professional Dignified Care

Email, Internet and Social Media Policy

Std Reference:	AA 014	**Written by:**	Helen Morley
Revision No:	3	**Reviewed by:**	Shane Scanlan
Pages:	6	**Approved by:**	Donna McNamara
Review Date:	February 2016		
Next Review:	February 2017		

AA014 Email, Internet and Social Media Policy

1. **INTRODUCTION**

Electronic mail (email) and internet usage (including social media) enables a prompt and efficient service from Brídhaven to its clients and suppliers. Email and the internet can also be used to communicate with other individuals and organisations with whom Brídhaven staff interact. While Email and the internet bring many benefits to Brídhaven in terms of communications, it also brings risks to the business, particularly where employees use it outside of their Organisation roles. It also brings risks where employees have more general access to the Internet. For that reason it is necessary to have a code of practice which regulates its use and which sets down specific rules for the use of Email, Internet and Social Media at Brídhaven. Every employee has a responsibility to maintain the Organisation's image, to use these electronic resources in a productive manner and to avoid placing the Organisation at risk for legal liability based on their use and causing damage to its financial status and reputation.

2. **Potentially dangerous material**

Do not launch, detach or save any executable file (i.e. those ending with 'exe' or 'vbs') under any circumstances.

All incoming attachments must be virus checked. Please note that all external disks, memory sticks, smartphones and CD's brought into the office from home PC's should also be virus checked. The safer option is to forward these attachments by email from your home PC as they will be automatically screened by the mailsweeper software.

Do not open, detach or save any unofficial file attachments to your hard disk or any network drive. Official attachments should be placed in the relevant document Library or detached to a shared drive. Please beware of saving any documentation to the hard drive of your PC (as opposed to Bridhaven's main network server) as this will not be backed up and will be irretrievable in the event of your PC breaking down.

3. **Obscenity, Child Pornography and Incitement to hate.**

Every individual is subject to all legislation regulating Internet use, including the provisions regarding obscenity, child pornography, sedition and the incitement of hate. In particular, persons have obligations under the Irish Child Trafficking and Pornography Act 1997, not to allow any of its systems (mail, internet, etc) to be used for downloading or distributing offensive material.

4. **Other Offensive and Time wasting Material**

Unsolicited material can arrive from anywhere. Should you receive material which you find offensive, abusive or time wasting, respond to it just as you would an offensive letter: complain directly to the sender and bring it to the attention of the sender's employing organisation and your manager as appropriate.

In the case of spam mail, do not issue a reply.

5. **Misleading Information**

Always be aware that the Internet is an unregulated, worldwide environment. It contains information and opinions that range in scope from reliable and authoritative to controversial and extremely offensive. It is your responsibility to assess the validity of the information found on the Internet.

6. **Material You Send**

Remember that email sent from Bridhaven's email address is on official headed paper and can be traced back to place, date and time of sending. Make sure you are satisfied with its content and that it has been approved at the appropriate level. Double check the address of the intended recipient. *Once the 'send' key is pressed, email cannot be stopped or retrieved*. Deleting mail from your system does not make it untraceable.

Do not send any unofficial graphics or executable files under any circumstances. Do not instigate or forward 'unofficial mail' to users either within or outside the organisation or send any material which may be offensive or disruptive to others or which may be construed as harassment. Do not make derogatory comments regarding gender, marital/civil status, family status, sexual orientation, religion, age, disability, race or membership of the travelling community.

Do not use another's email account.

All emails are automatically backed up and recoverable. All emails leaving Brídhaven should have the following text or equivalent automatically appended:-

"The information transmitted is intended only for the person or entity to which it is addressed and may contain confidential and/or privileged material. Any review, retransmission, dissemination or other use of, or taking of any action in reliance upon this information by persons or entities, other than the intended recipient is prohibited. If you received this in error, please contact the sender and delete the material from any computer.

> *It is the policy of Brídhaven Nursing Home to disallow the sending of offensive material and should you consider that the material contained in this message is offensive you should contact our IT administrator on info@bridhaven.ie*
>
> *While Brídhaven Nursing Home has taken every reasonable precaution to minimize the risk from viruses, we cannot accept liability arising from same. You should carry out your own virus checks before opening attachments."*
>
> *DATA PROTECTION: Any personal data may be stored on our databases for communication with you.*
>
> *CONFIDENTIAL AND URGENT COMMUNICATIONS: Brídhaven Nursing Home cannot be responsible for unauthorised access to e-mail and internet communications. Care should be taken with confidential matters. Where an urgent response is required please check by telephone or otherwise the attendance of the recipient in the organisation that you are looking to communicate with."*

In general – think before you send.

Remember that **screensavers** can be a means of causing offence and the same cautions should apply.

7. Screening Procedures

The IT screening system will automatically screen all email for known viruses, attachments, etc.

The Organisation does not normally read individuals email or open mail boxes except:

a) where the screening software or a complaint from an individual indicates that a particular mailbox contains material which is dangerous or offensive;

b) where a legitimate work reason exists to open the email.

Where investigation proves that a problem exists, it will be reported to the sender, their organisation, the staff member concerned and their manager for appropriate action. Where the problem concerns material such as a virus or an unauthorised .exe file, which can damage the network, the account of the individual concerned may be closed down pending further investigation and action.

Blocked messages either inbound or outbound are deleted if a request for release is not received. Messages containing virus files are not retained.

8. Social Media

Social media may be used by Brídhaven employees for business-related purposes only, subject to the restrictions set out below. These restrictions are intended to ensure compliance with legal and regulatory restrictions, privacy and confidentiality agreements, and organisation policy. Social media includes items such as blogs, podcasts, discussion forums, and social networks including but not limited to LinkedIn, Facebook, Twitter, MySpace, etc. All the rules that apply to other Brídhaven communications apply also to social media activity specifically: respecting clients, suppliers and one another; protecting confidentiality, privacy and security; and safeguarding and proper use of Brídhaven assets and reputation.

You must not post any material that is obscene, defamatory, profane, libellous, threatening, harassing, abusive, hateful, or embarrassing to another person or entity.

You may not post content or conduct any activity that fails to conform to any and all applicable legislation. It is critical that all employees abide by the copyright laws by ensuring that they have permission to use or reproduce any copyrighted text, photos, graphics, video or other material owned by others.

You must not disclose any confidential or proprietary information of or about Brídhaven**,** its residents, clients, suppliers, or staff including but not limited to personal, business and financial information. You must not represent that you are communicating the views of Brídhaven, or do anything that might reasonably create the impression that you are communicating on behalf of or as a representative of Brídhaven. Furthermore, you must not say or suggest that the views and opinions you express relate to Brídhaven or represent the official views of the organisation**.**

It is also against this policy to post offensive material or comments on your personal Social Media platforms that may be open to interpretation as directed towards colleagues or Residents of Bridhaven.

9. Time wasting and resources

Network resources such as storage space and capacity to carry traffic are not unlimited. However your time and that of your colleagues is the most valuable resource available to Brídhaven.

You must not deliberately perform acts which waste your own and your colleague's time or computer resources. These acts include:

- Playing games
- Online chat groups
- Uploading/Downloading large unofficial files which create unnecessary non-business related loads on network traffic
- Accessing streaming audio/video files, for example, listening to music or watching movie clips (for example on U Tube)
- Forwarding audio/video files to colleagues
- Participating in mass non-business related mailings such as chain letters (emails)
- Sending unofficial attachments

Do not download any material/software from the Internet for which a registration fee is charged without first obtaining the express permission of your manager. Only the software installed by Brídhaven is deemed to be legally sourced and covered by the appropriate licence agreement. No other software is approved for use on any of Bridhaven's computers or laptops.

Tablet computers/Screens in place at Brídhaven should be used for the sole purpose of accessing the EpicCare programme. Any other use is strictly prohibited.

10. **Security**
    You are responsible for the use of the facilities granted in your name. The main protection at present is your password or intranet login details. Make it difficult to guess and above all, do not write down your password, share it with anyone, or give it out over the phone. If you think someone knows your password, change it as soon as possible. Maintaining the privacy of your password is your responsibility and consequently you are responsible for any abuses taking place using your name and password.

    All programmes requiring a login (EpicCare, Complete GP, PC access,etc) must be logged in by the individual using the device at the time. **Sharing of logins is not permitted**. This is to both protect employees and ensure accuracy of documentation. Do not leave the computer or tablet you are using unattended without securing the session by password or signing off.

    In the interest of the environment please ensure that your computer is turned off and switched off from the mains if you are leaving work.

    Users accessing the Internet through a computer attached to the Bridhaven's network must do so through an approved Internet firewall or other security device. Bypassing the Bridhaven's computer network security by accessing the Internet directly by modem or other means is strictly prohibited.

    You are reminded that files obtained from sources outside of Bridhaven, including disks brought from home, files downloaded from the Internet, news groups, bulletin boards or other online services and files attached to e-mail messages may contain computer viruses that may damage Brídhaven's computer network. While Brídhaven is continually upgrading its virus protection infrastructure, the potential introduction of viruses on the IT system always remains a threat. All incoming material, regardless of origin, should be virus checked before being used on any PC on Brídhaven's network. This threat is real and will not be diminishing. If you suspect that a virus has been introduced into Brídhaven's network, notify your manager immediately.

    The Internet is not secure. Whether by e-mail or via the World Wide Web, do not give out more information than is necessary to fulfil your purpose. Beware of demands for unnecessary information. Be wary of sites which request more data than is necessary for accessing the site or for making a transaction, or which do not tell you why they require this data from you. In particular, no information on IT systems or resources should be disclosed over the Internet or through e-mail without authorisation from your manager.

    External email should only be used to transmit unclassified information to individuals outside the business. Classified or confidential material should not be sent by e-mail unless it is secure, contact Adapt IT for support in this regard.

11. **Personal Use**
    Just as with the phone, a small amount of limited personal use of e-mail and internet facilities is permitted if such use does not otherwise infringe this policy, for example for accessing payslips where it is not possible to do so elsewhere.

12. **Virtual Private Network (VPN)**
    If your computer has been set up with a VPN it is your responsibility to ensure that all passwords and login protocols remain secret. Access to our network is only to be made available to those who it is intended for.

    Laptops – Please do not download any 3rd party software onto your laptops that does not directly relate to your job. All 3rd party software must be approved by the network administrator prior to being downloaded.

13. Other Devices

This policy also applies to any phone or other relevant handheld or portable device that either has been or will be issued to you by the organisation.

14. **Infringement - Breach of Email, Internet and Social Media rules.**

Any breaches of these rules will be treated seriously and will be subject to disciplinary action up to and including dismissal. Please refer to the Brídhaven's Disciplinary Policy and Procedure for details of potential disciplinary action and appeals procedure.

We reserve the right to inform the relevant external authorities such as An Garda Siochana if material such as child pornography is found to be in your possession.

15. Document Revision Record:

Revision No.	Reviewed by:	Date:	Changes: Yes/No	Reason for Review