Care Ashore

Communications Policy

Version 1 created	August 2019
Implemented	August 2019
Review Date	August 2020
All policies and procedures location	Staff office at Care Ashore
Date Published on Care Ashore website	

Objects of the charity

Are, for the public benefit, to provide exclusively charitable support services and grants to:

- Those men and women who are of have been seafarers, and their dependents, who need assistance by the provision of accommodation, financial allowances or grants and in other such ways as the board think fit.
- Those men and women who are or have been seafarers and who are sick, disabled, aged or infirm or those who require rest or convalescence by the provision and maintenance of a convalescent home or rest home or in other ways as the board think fit.
- To extend its services to those persons having an appropriate connection with the sea as the board think fit, that includes potential visitors and their families to Care Ashore.

A) Aims

1) IT and Communication plays an essential role in the conduct of Care Ashore's business. The IT infrastructure including e-mail and internet access have therefore significantly improved business operations and efficiencies.

2) How you communicate with people not only reflects on you as an individual but also on Care Ashore as a business. As a result of this Care Ashore values your ability to communicate with colleagues, members and business contacts but we must also ensure that such systems and access are managed correctly, not abused in how they are used or what they are used for.

3) This policy applies to all members of Care Ashore who use Care Ashore's or its members' communications facilities, whether The Council of Management, full or part-time employees, contract staff or temporary staff. The parameters and restrictions are outlined below, and you are required to read them carefully.

B) General Principles

1) You must use Care Ashore's information technology and communications facilities sensibly, professionally, lawfully, consistently with your duties and in accordance with this policy and other Care Ashore procedures.

2) At all times employees must behave with honesty and integrity and respect the rights and privacy of others in relation to electronic communication and information. Care Ashore reserves the right to maintain all electronic communication and files.

3) Every employee will be given access to the Intranet and/or Internet as appropriate to their job needs. For those who do not have daily PC access occasional access will be arranged, as necessary, by Care Ashore General Manager.

4) All PC/network access will be through passwords, and no individual is permitted onto the system using another employee's password. Employees are not permitted to share their password with anyone inside or outside Care Ashore. Individuals will be allowed to set their own passwords.

5) All information relating to Care Ashore's residents and the organisations business operations is confidential. You must treat Care Ashore's paper-based and electronic information with utmost care.

6) Many aspects of communication are protected by intellectual property rights which can be infringed in a number of ways. Downloading, copying, possessing and distributing material from the internet may be an infringement of copyright or of other intellectual property rights.

7) Particular care must be taken when using e-mail as a means of communication because all expressions of fact, intention and opinion in an e-mail may bind you and/or Care Ashore and can be produced in court in the same way as other kinds of written statements.

8) If you are speaking with someone face to face, via the telephone, in writing via whatever medium you are a representative of Care Ashore. Whilst in this role you should not express any personal opinion that you know, or suspect might be contrary to the opinions of Care Ashore.

9) You must not use any of Care Ashore's or its partnership organisation media to do or say anything which would be subject to disciplinary or legal action in any other context such as sending any sexist, racist, defamatory or other unlawful material. If you are in doubt about a course of action, take advice from a member of management.

C) Use of electronic mail

1) **Business use**

Always use the "Bcc" box when mailing to groups whenever the members of the group are unaware of the identity of all the others (as in the case of marketing mailing lists), or where you judge that the membership of the group of one or more individuals should perhaps not be disclosed to the others (as in the case of members of a staff benefit scheme), because if you use the "Cc" box each recipient is informed of the identity (and in the case of external recipients, the address) of all the others. Such a disclosure may breach any duty of confidence owed to each recipient, breach Care Ashore's obligations under the General Data Protection Regulation or may inadvertently disclose confidential business information such as a marketing list. This applies to both external and internal e-mail.

Expressly agree with the member that the use of e-mail is an acceptable form of communication bearing in mind that if the material is confidential, privileged or commercially sensitive then un-encrypted e-mail is not secure.

If you have sent an important document, always telephone to confirm that the e-mail has been received and read.

In light of the security risks inherent in web-based e-mail accounts, you must not e-mail business documents to your personal web-based accounts. You may send documents to a member's web-based account if you have the members express written permission to do so. However, under no circumstances should you send sensitive or highly confidential documents to a member's personal web-based e-mail account (e.g. Yahoo, or Hotmail), even if the member asks you to do so.

2) **Personal use**

a) Although Care Ashore's e-mail facilities are provided for the purposes of the organisations business, Care Ashore accept that staff may occasionally want

to use them for their own personal purposes. This is permitted on condition that all the procedures and rules set out in this policy are complied with. Be aware, however, that if you choose to make use of Care Ashore's facilities for personal correspondence, Care Ashore may need to monitor communications for the reasons shown below.

b) Under no circumstances may Care Ashore's facilities be used in connection with the operation or management of any business unless express permission has been obtained from a member of management.

c) You must ensure that your personal e-mail use:

- does not interfere with the performance of your duties;
- does not take priority over your work responsibilities;
- does not cause unwarranted expense or liability to be incurred by Care Ashore or the organisations members;
- does not have a negative impact on Care Ashore's business in any way; and
- is lawful and complies with this policy.

d) Care Ashore will not tolerate the use of the E-mail system for unofficial or inappropriate purposes, including:

(i) any messages that could constitute bullying, harassment or other detriment;

(ii) on-line gambling;

(iii) accessing or transmitting pornography;

(iv) transmitting copyright information and/or any software available to the user; or

(v) posting confidential information about other employees, Care Ashore or its members or suppliers.

D) Use of Internet (external) and Intranet (internal)

1) Care Ashore trust you to use the internet sensibly. Although internet facilities are provided for the purposes of Care Ashore's business, we accept that you may occasionally want to use them for your own personal purposes. This is permitted on condition that all the procedures and rules set out in this policy are complied with and your use of the internet does not interfere in any way with the performance of your duties.

2) Whenever you access a web site, you should always comply with the terms and conditions governing its use. Care must be taken in the use of information accessed through the Internet. Most information is unregulated, and as such there is no guarantee of accuracy.

3) The use of the Internet to access and/or distribute any kind of offensive material, or material that is not work-related, leaves an individual liable to disciplinary action which could lead to dismissal.

4) You must not:

   a) use any images, text or material which are copyright-protected, other than in accordance with the terms of the license under which you were permitted to download them;

   b) introduce packet-sniffing (**Packet sniffers** work by intercepting and logging **network** traffic that they can 'see' via the wired or wireless **network** interface that the **packet sniffing** software has access to on its host computer) or password-detecting software;

   c) seek to gain access to restricted areas of Care Ashore's network;

   d) access or try to access data which you know or ought to know is confidential;

   e) introduce any form of computer virus; nor

   f) carry out any hacking activities.

E) VIRUS PROTECTION PROCEDURES

In order to prevent the introduction of virus contamination into the software system the following must be observed: -

a) unauthorised software including public domain software, magazine cover disks/CDs or Internet/World Wide Web downloads must not be used; and

b) all software must be virus checked using standard testing procedures before being used.

F) Use of Computer Equipment

In order to control the use of Care Ashore's computer equipment and reduce the risk of contamination the following will apply:

a) The introduction of new software must first of all be checked and authorised by a member of management or a member nominated senior member of management before general use will be permitted.

b) Only authorised staff should have access to Care Ashore's computer equipment.

c) Only authorised software may be used on any of Care Ashore's computer equipment.

d) Only software that is used for business applications may be used.

e) No software may be brought onto or taken from Care Ashore's premises without prior authorisation.

f) Unauthorised access to the computer facility will result in disciplinary action.

g) Unauthorised copying and/or removal of computer equipment/software will result in disciplinary action, such actions could lead to dismissal.

h) Strong complex passwords that follow the guidance below (4)

G) SYSTEM SECURITY

1) Security of Care Ashore's members' IT systems is of paramount importance. Care Ashore owe a duty to all of its residents, staff and trustees to ensure that all business transactions are kept confidential. If at any time we need to rely in court on any information which has been stored or processed using Care Ashore's IT

systems, it is essential that the organisation are able to demonstrate the integrity of those systems. Every time you use the system you take responsibility for the security implications of what you are doing.

2) Care Ashore's system or equipment must not be used in any way which may cause damage or overloading, or which may affect its performance or that of the internal or external network.

3) Keep all confidential information secure, use it only for the purposes intended and do not disclose it to any unauthorised third party.

4) Admin password changes for security reasons adhere to the following structure.
Prerequisites:

- *To include -10 chars + Upper and lower case + Numeric + Special chars*
- *To have a pattern that allows it to be potentially decipherable while on a site with no internet access*
- *To be complex enough that it can't be shared easily by word of mouth.*

5) Best practice for remembering passwords, if you utilise multiple, is to use an encrypted Excel spreadsheet.

H) Working Remotely (see Lone Working policy)

1) This part of the policy and the procedures in it apply to your use of Care Ashore's systems, to your use of Care Ashore's laptops, and also to your use of your own computer equipment or other computer equipment (e.g. member's equipment) whenever you are working on Care Ashore business away from Care Ashore's premises (working remotely).

2) When you are working remotely you must:

a) password protect any work which relates to Care Ashore's business so that no other person can access your work;

b) position yourself so that your work cannot be overlooked by any other person;

c) take reasonable precautions to safeguard the security of Care Ashore's laptop computers and any computer equipment on which you do Care Ashore business, and keep your passwords secret;

d) inform the police and Care Ashore as soon as possible if either a Care Ashore laptop in your possession or any computer equipment on which you do Care Ashore's work has been stolen; and

e) ensure that any work which you do remotely is saved on Care Ashore system or is transferred to Care Ashore's system as soon as reasonably practicable.

3) PDAs or similar hand-held devices are easily stolen and not very secure so you must password-protect access to any such devices used by you on which is stored any personal data of which Care Ashore is a data controller or any information relating to Care Ashore's business, its members or their business.

I) Personal telephone calls/ mobile phones

1) Telephones are essential for Care Ashore's business. Incoming/outgoing personal telephone calls are allowed at Care Ashore's office but should be kept to a minimum. We reserve the right to recharge for excessive personal use. When visiting or working on client premises you should always seek permission before using Care Ashore's members' telephone facilities.

2) Personal mobile phones should be switched off or 'on silent' during working hours and only used during authorised breaks.

3) Personal mobile phones should ONLY access Care Ashore's Guest Wi-Fi

J) Monitoring of communications by Care Ashore

1) Care Ashore is ultimately responsible for all business communications but subject to that will, so far as possible and appropriate, respect your privacy and autonomy. Care Ashore may monitor your business communications for reasons which include:

a) providing evidence of business transactions;

b) ensuring that Care Ashore's business procedures, policies and contracts with staff are adhered to;

c) complying with any legal obligations;

d) monitoring standards of service, staff performance, and for staff training;

e) preventing or detecting unauthorised use of Care Ashore's communications systems or criminal activities; and

f) maintaining the effective operation of Care Ashore's communication systems.

2) From time to time Care Ashore may monitor telephone, e-mail and internet traffic data (i.e. sender, receiver, subject; non-business attachments to e-mail, numbers called and duration of calls; domain names of web sites visited, duration of visits, and non-business files downloaded from the internet) at a network level (but covering both personal and business communications).

3) This includes monitoring of any additional accounts you may be requested to set up for the purposes of performing your work tasks, which are subject to the same rules as your work email account. Information acquired through such monitoring may be used as evidence in disciplinary proceedings.

4) Sometimes it is necessary for us to access your business communications during your absence, such as when you are away because you are ill or while you are on holiday.

K) Data Protection

1) As an employee using Care Ashore's communications facilities, you will inevitably be involved in processing personal data for Care Ashore as part of your job. Data protection is about the privacy of individuals and is governed by the General Data Protection Regulation.

2) Whenever and wherever you are processing personal data for Care Ashore you must keep this secret, confidential and secure, and you must take particular care not to disclose such data to any other person (whether inside or outside Care Ashore) unless authorised to do so. Do not use any such personal data except as authorised by us for the purposes of your job. If in doubt, please speak to Care Ashore designated Data Protection Officer.

3) GDPR gives every individual the right to see all the information which any data controller holds about them. Bear this in mind when recording personal opinions about someone, whether in an e-mail or otherwise. It is another reason why

personal remarks and opinions made should be given responsibly, must be relevant and appropriate as well as accurate and justifiable.

4) For your information, the GDPR provides that it is a criminal offence to obtain or disclose personal data without the consent of the data controller. "Obtaining" here includes the gathering of personal data by employees at work without the authorisation of the employer. You may be committing this offence if without authority of Care Ashore: you exceed your authority in collecting personal data; you access personal data held by us; or you pass them on to someone else (whether inside or outside Care Ashore).

L) Use of social networking sites

Any work-related issue or material that could identify an individual who is a member or work colleague, which could adversely affect a member or Care Ashore's relationship with any member must not be placed on a social networking site. This means that work related matters must not be placed on any such site at any time either during or outside of working hours and includes access via any computer equipment, mobile phone or PDA.

M) Confidentiality

Employees are not permitted to register with sites or electronic services in Care Ashore's name without the prior permission of the General Manager. They are not permitted to reveal internal Care Ashore information to any sites, be it confidential or otherwise, or comment on Care Ashore matters, even if this is during after-hours or personal use. The Care Ashore confidentiality policy applies to all electronic communication and data.

N) Compliance with this policy

1) Failure to comply with this policy may result in disciplinary action being taken against you. If there is anything in this policy that you do not understand, please discuss it with the General Manager.

2) Please note that the procedures and policies outlined in this policy, and in any related policy, may be reviewed or changed at any time.

Review

This policy will be reviewed every 2 years or as and when there are changes in legislation relating to communication procedures at Care Ashore.

All current management, including trustees and staff have read and understood the contents of this policy and all new staff will be required to read and sign this policy during their induction to Care Ashore.

Date	Print Name	Signature