SCBF Electronic Information and Communication Policy

This policy is written to ensure that all users of the Strathnairn Community Benefit Fund's (SCBF) IT resources act in a manner consistent with the values and objectives of the organisation. The policy describes the scope, roles, responsibilities and problem areas associated with use of these resources. This Policy will apply to all users of the resources: all staff (employed, self-employed or contracted from another organisation), Board Members, consultants or any other person working for or on behalf of the organisation.

Policy Statement

The webmail account, website, social media page and SCBF laptop are the property of SCBF and are to be used for legitimate business purposes only. Where SCBF has given you a password to access its website, social media accounts, and/or other online accounts and tools (e.g. Online Banking) you are responsible for keeping this password confidential and must not share it with others.

Board Members are provided with access to a personalised SCBF e-mail address (….@strathnairncbf.com) to assist them in the performance of their roles. When using the SCBF laptop only files needed to assist the user in their role may be downloaded from the internet. All users have a responsibility to use SCBF's laptop, website, social media accounts and e-mail in a professional, lawful and ethical manner.

Use of Log-on Identities and Passwords

Access to webmail and the SCBF website are controlled by passwords. Users should use only the log-on assigned to them and keep their passwords secret.

Where SCBF has set up a dedicated xxxx@strathnairncbf.com e-mail address for Board Members to send and receive SCBF related correspondence through, the person allocated this e-mail address is responsible for password protecting it, keeping this password confidential and must not share it with others.

A new user should change their password the first time they log in so it is not the same as the password provided to them by the website or webmail administrator. Automatic storage should only be used where only the user has access to the device and the device itself is password protected.

If a user thinks their device or webmail password has been compromised all passwords should be changed immediately. Passwords should be complex and not easily guessed by others with access to the same devise e.g. not the name of your family pet.

Sending and Receiving e-mails

Email is a powerful and effective method of communication but has risks and challenges. To minimise those it is important to be aware of the possible problems and then to follow good practice. Otherwise there are serious legal, security and reputational implications. Following good practice will protect yourself and SCBF.

Emails through the SCBF webmail are the property of SCBF and therefore SCBF has authority to access and read emails. Where electronic correspondence is sent to an external organisation the sender is representing SCBF and it should therefore be treated as if it were correspondence on headed paper. Users should be aware that exchange of e-mail may enter into or vary contractual relationships on SCBF's behalf, and such exchanges must therefore be made only with appropriate Board authorisation as necessary.

A SCBF e-mail signature below your own name should be included on e-mails sent to non @strathnairncbf.com e-mail addresses including the generic contact details for the organisation, registered charity and company information including the registered office and registration numbers, a disclaimer statement and Privacy Notice statement and link. An example of which can be cut and pasted from the Secretary's e-mail signature.

Possible Problem Areas to Consider

- Email is not an informal communication tool, it has the same authority as any other communication tool to and from the organisation.
- Emails can be easily recovered and even though deleted they can be traced.
- Overuse or inappropriate use can lead to information overload – do you really need to send to everyone?
- External emails should have disclaimers attached to protect the organisation.
- It should be regarded as published information.
- Emails are not confidential and can be read by anyone with sufficient levels of expertise – is it the right medium?
- Binding contracts may be inadvertently created.
- Defamation of colleagues or other parties (deliberate or otherwise) may occur.
- Abrupt, inappropriate and unthinking use of language can lead to a bullying tone and possible offence to others – CAPITALS ARE OFTEN INTERPRETED AS SHOUTING!
- E-mails with bad spelling in then (possibly down to predictive text on phones) reflect badly on the professionalism of the organisation so read over them before pressing send.
- Emails can be a vehicle for introducing viruses into a computer and the IT systems as a whole.

Good Practice Guidelines

- Manage your email.
- Read emails frequently.
- SCBF mails should be used for business purposes only.
- Delete messages you no longer need quickly.
- Save messages you want in folders.
- Reply to genuine emails promptly.
- E-mail file attachments whose contents cannot be verified should not be opened.
- Information received by e-mail will be treated in the same manner as all other written memos, and therefore e-mails should not be forwarded or further disseminated except where it is for an identified business purpose.
- All emails should be sent with a disclaimer and organisational details summary.

- Beware of hitting 'Reply to All': Do you want everyone to read your reply?
- Be aware of information further down an e-mail chain if you are sending on to a new person in the conversation. It might not be appropriate this is included or could lead to a GDPR breach. If in doubt start a new e-mail.

Content and Style

- Be careful about your use of language and actual words you are using - do not send inappropriate, abusive or discriminatory messages.
- Be careful about the images that you attach or use in emails – these could be misinterpreted.
- Be careful how you express yourself – emails lack the cues and clues of other types of messages and can be misunderstood.
- Keep brief – people do not choose to read large amounts of text on a screen.
- Use a relevant subject header and update the header if replying, especially when a conversation has been through many cycles of message and reply
- Do not use characters such as £ signs – some mail programs do not de.al with these.
- Keep sentences and paragraphs short.

E-mail must not be used for any illegal purpose, or for accessing, receiving or transmitting any material deemed illegal, indecent, offensive or otherwise unacceptable under UK law, the laws of any destination country or any country via which such material travels to reach its destination.

When a Board Member ceases to be a Board Member, and is not immediately re-elected, they will delete all SCBF e-mails they still hold.

Access to Internet via a SBCF device

The internet is a powerful tool, providing a gateway to endless information and services but use of the internet can introduce potential risks and therefore has to be carefully managed. Just as the internet is a portal to the World Wide Web, others can use internet access to find their way into our business, potentially breaching confidentiality.

The internet should generally only be used to access business-related information. Internet access must not be used for accessing, receiving, transmitting or downloading any material deemed illegal, pornographic in nature, indecent, offensive or otherwise illegal under UK law. Users are also prohibited from subscribing to Newsgroups not associated with SCBF's interests. The objective of these good practice guidelines is to encourage safe and effective use of the internet for everyone.

Sites

- Access to websites must be for business purposes only.
- Access to offensive websites is forbidden – this can include pornographic websites, those promoting racism or other discriminatory and inappropriate behaviour.

- SCBF has the right to utilise software that makes it possible to identify and block access to internet sites containing material deemed inappropriate in the workplace and identify the user.

Downloads

Downloaded files may contain viruses, therefore only open files from reliable sources and use virus checking software. It is forbidden to download applications, software, inappropriate files or other programmes. If you feel you need to download applications or similar files, please consult your Line Manager. All software should be installed by our authorised IT supplier(s).

Remember that copyright rules apply to information on the internet and unauthorised copying is a criminal offence.

Monitoring

SCBF may access, monitor, log or disclose private electronic messages or files of a laptop user if it has good cause. Good cause shall include: the need to protect system security, fulfil SCBF's obligations, detect wrong doing, comply with legal process, or protect the rights or property of SCBF. All users are made aware of such monitoring and consent to such monitoring as a condition of access to electronic communications and computers. Acceptance of employment/contract/Directorship will be deemed to be consent for these purposes. Laptop users should bear in mind that all Internet site visits are traceable.

1. Users must not engage in illegal copying of works which are protected by copyright, database right or other neither protection nor may users make available copies of such works.

Security

- Viruses are not contained in plain text email messages;
- Viruses can be contained in an attachment;
- Do not forward messages about viruses to distribution lists;
- Passwords must be used and kept confidentially.

Confidentiality

The Internet and other external electronic communications are not secure. Any message sent over the Internet may potentially be intercepted and read or altered by anyone, and Internet communications are not anonymous. E-mail notes could be easily forwarded to others, or printed and made available to individuals out with SCBF. Information which is in any way confidential, personal, proprietary or otherwise sensitive should not be sent out with SCBF using the Internet or by email.

Responsibility and Accountability

This policy will be communicated to all Employees, Board Members, consultants or any other person working on behalf of SCBF. Compliance with this policy is mandatory and any breach will attract disciplinary action.

Board Members are responsible for the day-to-day implementation of the policy and for ensuring that those for whom they are responsible use the systems and networks in the appropriate manner.

These guidelines are intended to ensure that SCBF is protected adequately and that the right image is portrayed externally when users are representing SCBF. In extreme cases abuse of the policy and guidelines could lead to disciplinary action or being asked to stand down from the Board.

Social Media

SCBF realises that the internet and social media sites provide a number of benefits to the organisation but also personally for staff members. The internet allows individuals a range of interaction which they could participate in, including platforms such as Facebook, Twitter, LinkedIn, Blogs, and wiki's for example. Whilst such platforms are tools for marketing and networking, where misused it could potentially jeopardise SCBF legally and/or bring SCBF into disrepute.

Therefore there are a number of guidelines which must be followed when representing ourselves, SCBF online. The intention of this policy is not to stop users from conducting legitimate activities on the internet or indeed using social media, but to serve as a guideline when conflicts could arise and how this will be addressed.

When someone clearly identifies their association with SCBF and or its activities, or their work online, or otherwise, they are expected to behave appropriately, and in ways that are consistent with the organisations values and operational policies.

The aims and purpose of the social media guidelines are to ensure that users:

- Are not engaged in activities on the internet which might bring SCBF and or its activities into disrepute.
- Do not use the internet in any way to attack or abuse anyone.
- Do not post derogatory or offensive comments on the Internet.
- Do not represent SCBF online without prior authorization.
- Make appropriate use of social media and the internet with positive outcomes.

Responsible use of Social Media

SCBF is committed to ensuring that all social media usage is done so at a responsible and acceptable level. The social media guidelines provides that under no circumstances should derogatory, negative or offensive material be posted about SCBF, our activities, our clients, our contacts, our suppliers, our users or other parties related to our business. This includes communication via the possible channels below, but not limited to:

LinkedIn accounts

Whilst these accounts are primarily used as a professional tool, they cannot be truly private. However, there are a number of sensible steps that users should adhere to when using LinkedIn accounts.

- Should you cease being a Board Member/employment from SCBF, by whatever reason, you will be required to update your status immediately upon termination.
- LinkedIn has a recommendations function, and you must be mindful when or if making a recommendation or making a connection with a contact, that you may indirectly be acting on behalf SCBF, and be mindful that your views may be indirectly representative of SCBF.

> If you are in any doubt as to the content or tone of any recommendations please speak to the Chair.

Facebook accounts

You are not permitted to use your personal Facebook account on the SCBF laptop unless using it to access the SCBF Facebook page, nor be deemed to represent SCBF on your personal account. Users should be mindful of the information that is posted on their own social networking sites. This can include any inference towards other SCBF users, developers, contractors and any other party related to the work of SCBF.

Blogging

Whilst you are encouraged to share SCBF updates and sector news with social media users, you may also be privy to information that is sensitive and that others in the community are not, therefore you must use complete discretion in the information that you post to avoid a breach of confidentiality or personal data.

Blogging at home, not identified as having a connection with SCBF and not discussing the organisation, would fall out-with the remit of this policy. Should you indicate that you are connected to the organisation, you should make clear that these are your personal views and not those of SCBF. You must be mindful of your obligations on confidentiality and data protection. Please remember that what you publish may be read by masses therefore you should keep this in mind before posting any comments on social media sites.

Twitter

Although SCBF doesn't have a Twitter presence at the time of writing this policy it is supportive of the business and personal use of Twitter and it is a useful tool for quick communication with clients and associations alike. Consider what you are writing or what the message is you wish to convey before you post a "Tweet." Staff should remember that Twitter, like all other forms of social media, are not wholly private and once a tweet has been made, it's a permanent entry online.

Any breach of this policy, or where anyone is are deemed to bring SCBF or its activities into disrepute via social media, social networking or other electronic means will be dealt with 1) under the Disciplinary policy for Employees; 2) As per the Articles of Association for Board Members.

This Policy was adopted at the SCBF meeting held on 27 August 2018.