Policy Data Sheet

Policy Name:	Internet Email and social Networking Policy
Document Reference:	BC006
Version Number:	1
Ratified By:	Director
Reviewed:	Dec 2022
Review Period:	3 years
Next Review Date:	Dec 2025

Content

The IT, email, social networking policy should be read in conjunction with the Information Governance Framework, Information Security and Keeping Records and Data Protection Policies.

This policy is relevant to all employees (temporary and bank staff), contractors, consultants, casual and agency staff, volunteers and student placements.

This policy covers the use of IT equipment when working in Beetroot Consulting from any location. The use of online and social media for business and for personal purposes, during working hours or otherwise.

1. Aims of the Policy

The aims of this policy are to;

- Provide a framework that ensures that all Beetroot Consulting service users or customers are kept safe.
- Provide staff with the overarching principles that guide our approach to e-safety
- To ensure that as an organisation we operate in line with our values and within the law of how we use information technology.
- Prolong the life of the network and prevent damage to the system
- Increase understanding of the potential problems associated with IT, Internet and use of e-mail
- Outline appropriate IT Internet and E-mail use
- Ensure employees are aware of the consequences of misuse
- Avoid or reduce unnecessary time being spent on non-work-related activities
- Ensure the business' online activities are legally responsible
- Protect the brand of Beetroot Consulting
- Ensure staff are clear about the purpose of online communication, roles and responsibilities.

This document describes the policies applied by Beetroot Consulting, on the use of the communication systems.

The systems are defined as any and all means used by the business and its employees, partners or volunteers to communicate both within and outside the business. These systems include but are not limited to telephones, email, voicemail, computers (including laptops, tablets, iPad's, smartphones, storage devices and fax and machines).

Use of the business's system in violation of this policy may result in disciplinary action up to and including termination of employment and/or legal action, depending on the seriousness of the violation.

2. Monitoring

The business reserves the right to monitor (e.g.: content and level of traffic), record, access and/or disclose any messages or data transmitted through the business's systems at any time and from any location, in the following circumstances:

- To investigate or detect the unauthorised use of business systems (e.g. breaches of this policy)
- To monitor staff for training and assessment purposes
- To prevent or detect crime
- To ensure the effective operation of the system (e.g.: including monitoring for viruses)
- To establish the existence of facts relevant to the business's business (e.g.: communications relevant to a contractual relationship that has been entered into by use of the business's system) and
- To ascertain compliance with regulatory or self-regulatory practices or procedures relevant to the business's business
- For the purpose of routine audits to ensure appropriate and secure use of the IT infrastructure

The business also reserves its right to monitor (e.g. content and level of traffic) messages or data for the purpose of determining whether or not the communications are relevant to the business (e.g. opening of e-mail accounts in order to access business communications when a member of staff is on holiday or off sick)

3. Confidentiality

Confidentiality is very important, as the system cannot be considered private and messages (whether through misdirection, response to legal process or otherwise) may be read or heard by someone other than the intended recipient inside or outside the business.

Confidential information must therefore not be sent electronically without adequate security measures. Unless an employee is using a data encryption technique, electronic communication must not be used to forward confidential, financial or employee information outside the business without the specific authorisation of the Director to transmit the data unencrypted. Refer to Information Security Policy for more information.

All representatives must be aware that any transmission through the system may be accessed by the business in accordance with this policy and consequently no employee should have any expectation of privacy in connection with their messages, once transmitted through the system regardless of whether such transmission has been deleted, or is marked in some manner to indicate that it may be a personal transmission to or from that employee.

When travelling on public transport and in a public location, staff must take precautions to keep confidential information secret.

4. E- safety

Information technology is an essential part of all our lives. The technology is of great benefit to us all, however if misused children, young people and vulnerable adults can be actually or potentially harmed, for this reason Beetroot Consulting Director can support with:

- Examining and assessing risks of any emerging new technologies before they are used within the business areas
- Assisting each business area in ensuring all relevant procedures provide clear and specific directions to staff and volunteers on the appropriate use of ICT

5. Use of the Internet

All employees will be allowed access to the Internet for business use. Where possible employees should ensure that any browsing is focused and does not become time-consuming.

Employees should ensure that if information downloaded from the Internet is to be relied on for business purposes, appropriate steps should be taken to validate the authenticity and accuracy of the information and ensure such downloads are not in breach of the Data Protection Act (2018) or any other legislation

It is the employees' responsibility to ensure that they do not infringe copyright, patent rights, or any other intellectual property rights.

Employees must not download and install software from the internet on any company device, without appropriate authorisation. Staff may download apps if required on to their work phone providing these are from the Apple App Store or Android Play Store.

Any use by employees of hardware, software and internet access, other than for business, is only limited to occasional and incidental use, provided that it;

- Does not consume more than an insignificant amount of business resources and employee time (eg: during lunchtimes, scheduled breaks or out of office hours)
- Does not interfere or conflict with the employee's responsibility and productivity
- Does not pre-empt, interfere or conflict with any business–related activity
- Does not pre-empt, interfere or conflict with existing employee standards of conduct or other policies or standards of conduct that may be implemented from time to time.
- Employees must follow the appropriate guidelines surrounding material protected by copyright (The Copyright, Designs and Patents Act 1998) and ensure that they do not illegally copy documents or software.
- To prevent the introduction of viruses no software should be downloaded from the Internet or loaded onto hard disks by other means, without permission of IT staff and line manager.
- Employees must bear in mind that information available on the Internet can often be inaccurate and unregulated and may need checking against a reliable source.

6. Use of E-mail

BC has agile working, working in this way means that we are utilising Email frequently as a means of transferring data. This may be internally or externally.
Employees should determine the appropriate method of transferring data electronically and refer to the Information Security Policy for guidance.

It may be necessary to discuss issues related to disciplinary, grievance or redundancy matters *with the employee concerned* via e-mail. We ask that the usual caution relating to email security is applied when sending messages relating to sensitive issues. If you are required to send an external email that contains sensitive or confidential data this should be sent using a secure transfer method. Please see the Information Security Policy for more information regarding this.

Emails sent to all staff in Beetroot Consulting or to all staff in a particular business within the business must contain information relevant to most staff. Individuals should not use business emails as a means of raising their views about a staff member or business practices; such issues should be raised through the appropriate channels for example supervision, or by following the grievance or whistle blowing policies.

Employees must avoid overloading email systems by sending or requesting large attachments, for example video files or large presentation files. Alternative file transfer systems are available for this purpose.

Employees must not undertake any fraudulent activities, including impersonating any person or entity or forging anyone else's digital or manual signature, email address.

There may be occasions when it is necessary to gain access to users email or storage systems when they are absent from work to enable the business to perform its functions, deliver its services and meet its statutory obligations. Only authorised senior managers will be able to apply for such access. It will not be normal practice to access any emails marked 'personal', unless it is justified for legal or business purposes.

Any use by employees of these systems other than for business business is only limited to occasional and incidental use, provided that it

- Does not consume more than an insignificant amount of business resources and employee time (eg: during lunchtimes, scheduled breaks or out of office hours)
- Does not interfere or conflict with the employee's responsibility and productivity
- Does not pre-empt, interfere or conflict with any business–related activity
- Does not pre-empt, interfere or conflict with existing employee standards of conduct or other policies set out by the business, or other such standards of conduct that may be implemented from time to time.

7. E-mail Style and Language

Employees should be aware that email is not an informal communication tool when used for business purposes. The appropriate language should be used at all times.

8. Legal Implications

Employees should be mindful at all times that e-mail and Zoom, Slack/ Trello correspondence has the same authority as any other communication to and from the organisation.

Employee's e-mails create an enforceable contract. E-mail should only be used in third party negotiations when employees have the right to do so and when the recipient understands what authority the employee has. Employees should obtain confirmation of receipt of important messages.

Employees need to be aware that the same laws apply to e-mails as to written documents and therefore it is important to avoid making statements that may be inaccurate or libelous. If employees have any doubts about the content of e-mail they should seek advice from their line manager before sending.

9. E-mail Signature

The following is an example of an e-mail signature.

Name Surname I job title
address, postcode
Tel: I Mobile: I Fax:
www.beetrootconsulting.org

Staff working in an agile way should also include the following statement: *At Beetroot Consulting we work agile, so while it suits me to email you now, I don't expect a reply outside of your working hours.*

10. Prohibited Uses of Beetroot Consulting business systems

Employees should never attempt to use or access information via these systems in an unauthorised or inappropriate manner, or even give the appearance of inappropriateness in such use or access.

An employee who becomes aware of an unauthorized or inappropriate communication should bring it to the attention of their manager and should never redistribute such communications.

In particular, these systems must not be used in ways that violate applicable laws, including copyright, defamation, privacy and obscenity laws, or in ways that may be disruptive, offensive to others or harmful to morale, or in a way that would be likely to expose the business to liability.

Any transmission or use of the business's systems that contains sexually explicit images, messages or cartoons, ethnic slurs, racial epithets or anything else that may be construed as harassment or offensive to others based on actual or perceived race, national origin, sex, sexual orientation, age, disability, religious or political beliefs is against business policy and strictly prohibited.

The sending of offensive e-mails will not be tolerated. This includes e-mails that can be seen as threatening or as harassment. Any employee found to be sending such e-mails will be subject to disciplinary procedures.

Accessing or downloading offensive, obscene or indecent material is forbidden. This includes accessing material that is pornographic, racist, sexist or that advocates intolerance of others in anyway. (Please note that these are just examples of types of offensive, obscene and indecent material and this list is by no means exhaustive.) Any employee found to be in breach of this will face disciplinary action this is gross misconduct and could lead to dismissal.

11. Indecent Images

The Criminal Justice Act of 1988 made the possession of indecent photographs of children an offence. This is an arrestable offence carrying a maximum sentence of 5 years.

Making an indecent image of a child is a Serious Arrestable Offence carrying a maximum sentence of 10 years imprisonment.

Note: The term "make" includes downloading images from the Internet and storing or printing them out.

Any member of staff found downloading inappropriate images will be seen to have committed gross misconduct and will be subject to a disciplinary process which could result in dismissal. Beetroot Consulting would have a responsibility to inform the Police of any indecent images of children found on IT equipment.

12. What to do if you receive indecent Images of children by E-mail, text or WhatApp

If an employee receives unsolicited mail including such an image they should report it immediately to the police.

Once an image has been reported to the police the employee should then log onto www.iwf.org.uk and click the icon at the top right hand side of the page "Report Illegal Content Click Here".

The employee should then report the image to the Director to enable the image to be deleted completely.

13. Use of personal computers, mobile telephones and other equipment whilst at work

Employees may use personal mobile phones (in accordance with the mobile phone policy) and other equipment whilst they are at work however, they must not use such equipment in any way that may cause disruption or offence to other employees or members of the public. This includes excessive use of the equipment, disruptive levels of nose and images or sounds which may cause offence.

Any material that contains sexually explicit images, messages or cartoons, ethnic slurs, racial epithets or anything else that may be construed as harassment or offensive to others based on actual or perceived race, national origin, sex, sexual orientation, age, disability, religious or political beliefs is against business policy and strictly prohibited during working hours whether you are using company or personal equipment.

14. Security (Passwords & Virus Checks)

The inappropriate or careless use of the computer network can lead to a breach of security and can endanger the entire network.

To prevent unauthorised parties from obtaining access to electronic communications, employees must ensure that they have secured their computer when away from them in any place of work . In particular, all employees who share the use of a computer with other staff members, or who temporarily use a computer that is assigned to someone else, must ensure that they log off the network each time they have finished using the computer in order to avoid any subsequent use of the computer being attributed to them.

Passwords should be unique and be a mixture of alpha-numeric characters. Passwords should never be written down and shouldn't be disclosed without the permission of a senior manager..

All employees have a responsibility to protect the business's systems from viral infection due to the downloading of data from dubious or unknown sources. In the event of a computer virus infecting the business's computing systems; it is the responsibility of the individual discovering the infection to notify the Director immediately.

Beetroot Consulting Representatives;

- Are responsible for their own IT equipment and they must not allow it to be used by an unauthorized person.

- Should ensure that their computers are locked and secure when they are away from them, and should always be shut down at the end of their working period.

- Should never download documents, files or material where they are unsure of the source or content unless approved by IT

- Should not disclose their network or database system passwords to anybody. If an employee suspects that their password has been leaked to unauthorized persons they should report this to IT helpdesk immediately

Suspicious emails, such as phishing, spam and fraud or those known to contain viruses, should not be opened and should be reported to the Director immediately.

Employees connecting remotely should ensure that the environment in which they are working is safe and secure. Employees should ensure that the server cannot be accessed by anybody outside the organization. If an employee suspects that there has been a breach of security they should inform Director immediately. When working remotely employees should continue to use their network passwords in the normal way and should ensure that their password is not disclosed to anybody.

It is essential that employees understand that when they have finished working remotely they must log-off the all systems. This is to avoid anyone else being to access potentially confidential information.

15. Personal use of Online, Social Media, Blogs and Websites

This part of the policy and the procedures in it apply to content that you publish on the internet (e.g. your contributions to blogs, message boards and social networking or content-sharing sites) even if created, updated, modified or contributed to outside of working hours or when using personal IT systems.

Beetroot Consulting recognises that in your own private time you may wish to publish content on the internet. For the avoidance of doubt, such activities should be limited to non-working hours.

- If you post any content to the internet, written, vocal or visual, which identifies, or could identify, you as a member of Beetroot Consulting and/or you discuss your work or anything related to Beetroot Consulting or its business, customers or staff, Beetroot Consulting expects you, at all times, to conduct yourself appropriately and in a manner which is consistent with your contract of employment and with Beetroot Consulting's policies and procedures. It should be noted that simply revealing your name or a visual image of yourself could be sufficient to identify you as an individual who works for the business.

- If you already have an online presence that indicates in any way that you work for any part of Beetroot Consulting you should report this to the Director.

- If you intend to create a personal blog or website that will say that you work for Beetroot Consulting or in any way could identify you as someone who works for it then you should report this to the Director.

- If your online presence clearly identifies that you work for Beetroot Consulting and you express any idea or opinion then you should add a disclaimer such as "these are my own personal views and not those of Beetroot Consulting".

- Employees must not post disparaging or defamatory statements about the organisation, clients, suppliers or vendors, affiliates or stakeholders. The following matters will be treated as gross misconduct capable of resulting in summary dismissal (this list is not exhaustive):

- Revealing confidential information about Beetroot Consulting's businesses in a personal online posting. This might include revealing information relating to its clients, business plans, policies, staff, financial information or internal discussions. Consult the Director if you are unclear about what might be confidential.

- Criticising or embarrassing Beetroot Consulting's businesses, its customers or its staff in a public forum (including any website). You should respect the corporate reputation of the business and the privacy and feelings of others at all times. If you have a genuine complaint to make about a colleague or workplace matter the correct procedure is to raise a grievance using the business's grievance procedure.

- If you think that something on a blog or a website could give rise to a conflict of interest and in particular concerns issues of impartiality or confidentiality required by your role then this must be discussed with your line manager.

- If someone from the media or press contacts you about your online publications that relate to Beetroot Consulting, its businesses or charities, you should talk to your line manager before responding and the communications department must be consulted.

- Online publications which do not identify the author as a member of Beetroot Consulting's staff and do not mention Beetroot Consulting and are purely concerned with personal matters will normally fall outside the scope of Beetroot Consulting's policy.

16. Taking of and using images of service users, including all children, young people and vulnerable businesss

Any Images or recordings taken for official purposes within services taken using Beetroot Consulting's equipment must only be taken following permission obtained and only for the purpose for which consent has been given. (Please see form within appendix)

17. Use of Online, Social Media Blogs and Websites for business

Setting up a social networking account/online activity for business

- Staff wanting to set up an online space to promote their service must discuss this with the Director, who will work with them to decide whether this is appropriate.
- A risk assessment will be carried out
- The Director will hold a central list of all usernames and passwords.
- The Director will maintain oversight of all service-specific online spaces.

What should remain confidential?

- Staff should not indicate a political allegiance on Beetroot Consulting social networking sites/ or any online communication where they are representing Beetroot Consulting.
- Staff should not reveal confidential information about Beetroot Consulting's businesses, its staff, clients or service users.

Staff responsible for managing and updating the business's social media channels or websites should not use them to:

- contact friends
- communicate personal information
- promote themselves, if they work in a self-employed capacity alongside working for Beetroot Consulting.
- Promote other organisations, if employed by another employer alongside Beetroot Consulting.
- Make defamatory statements about organisations/individuals. This would include any statement which could be considered to harm reputation, or cause a person to lose their professional standing.

Quoting statements from other sources

- Action can be taken against a company for repeating libellous information. Check carefully information from other sources that you intend to publish is accurate and factual.

Use of photos/comments/videos of staff and service users

- Social networking sites allow photographs, videos and comments to be shared with thousands of other users. However it may not always be appropriate to share work-related information in this way. Before uploading photographs, videos or comments ensure:
- Any social media tools used in the course of our work with children, young people and vulnerable adults must be risk assessed in advance

Responding to negative comments

Beetroot Consulting will always try not to remove negative comments/criticism. Instead we will respond to legitimate criticism.

- Staff should report any negative/offensive/derogatory comments to their manager and the Director who will work with the business/charity to agree a response.

18. IT Equipment

Staff are responsible for business IT equipment when in their care and should not allow friends, family members, or members of the public to use Business IT equipment except as part of running a service.

It is the responsibility of all staff with laptops, mobile phones and portable IT equipment (such as projectors, external hard drives.) to ensure that equipment is stored securely when not in use (overnight, when offices are closed for example.) Staff with laptops and responsibility for portable IT equipment should ensure they are locked away when they are not present.

No confidential information should be copied or stored on portable IT equipment unless in exceptional circumstances outlined in Data Protection and the Information Security policies.

Tampering with PCs, telephones, cables or other computer equipment should not be done without first contacting the Director.

19. Purchasing new/replacement IT equipment

All new IT equipment requests should be approved by the Director

20. Sustainability and Redundant IT equipment

All redundant IT equipment should be returned to the Director team who will verify it, remove all documents and dispose of it via an approved recycle company. The company provides quarterly reports helping BC understand

21. IT Procedures

All Beetroot Consulting business staff or suppliers have a Google Workspace logon and an email address.

Google workspace enables remote working. All staff logging in from off-site locations should take precautions to ensure that the network is not accessed or viewed by unauthorised persons. Off-shore access to the network requires approval by the Director.

22. Beetroot Consulting websites

Beetroot Consulting has one main business-wide website.

The business website contains information about every service the business delivers. Should you wish to request changes to this information, please contact the Director at info@beetrootconsulting.org

23. Monitoring

Beetroot Consulting has the right to monitor employee's use of communication systems. Beetroot Consulting reserves the right to monitor, intercept and review, without any further notice, staff activities using company IT resources and communication systems.

24. Breach of this policy

Breach of this policy will be dealt with under the HR policy. Disciplinary action can be taken regardless of whether a breach is committed during working hours and regardless of whether Beetroot Consulting's equipment or facilities are used for the purpose of committing the breach.

Serious breaches of this policy (such as posting of material or comments that are derogatory about the company or its employees, or that involve sensitive material) may be treated as gross misconduct and could result in dismissal.

Any member of staff suspected of committing a breach of this policy will be required to co-operate with investigations which may involve handing over passwords and log in details.