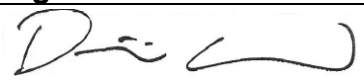
Newcastle West End Foodbank

Information Security and Social Media Policy

Version No.: 2.1
Effective From: 18 November 2020
Review Date: 18 November 2022

Signature:	Signed by:	Position:	Date:
	Rev D Coad	Chairman	17 November 2020

1 Introduction

This policy sets out what is and what is not acceptable behaviour when using the computer facilities within Newcastle West End Foodbank (WEFB) and outwith WEFB, such as the internet, smart phones, social media and networking websites.

2 Scope

This policy applies to all employees, volunteers and anyone engaged WEFB to carry out its services.

Any deviation from this policy may be subject to disciplinary review or other appropriate action.

3 Overview and Definitions

3.1 Information Security

The security of information/data covers three main aspects:

Confidentiality (**C**), i.e. to protect information/data from breaches, unauthorised disclosures, or unauthorised viewing.

Integrity (**I**), i.e. to retain the integrity of the information/data by not allowing it to be modified or deleted maliciously or accidentally.

Availability (**A**), i.e. to maintain the availability of the information/data by protecting it from cyber-attacks, destruction, disruption and denial of service.

In addition to the core principles of **C**, **I** and **A**, information security also relates to the protection of the organisation's reputation. Reputational loss can occur when any of these principles are breached.

"Information/data" can be held in computerised digital form, but also covers information/data held in printed form and hand-written. It is WEFB policy to ensure that the use of documents, computers, mobile computing, mobile communications, portable storage devices, mail, voice mail, voice communications in general, multimedia, postal services and fax machines must be controlled to prevent unauthorized use and to reduce security risks.

3.2 Social Media

Social media is the term used for internet-based applications and web sites which help people keep in touch and enable them to interact. It allows people to share information, ideas and views.

Social media can affect communications amongst managers, employees, volunteers, donors, suppliers and job applicants; how organisations promote and control their reputation; and how colleagues treat one another. It can also distort what boundaries there are between home and work.

Misuse of IT and social media can create issues such as time-theft, defamation, loss of reputation, cyber-bullying, freedom of speech and the invasion of privacy.

4 Legal Considerations

The Human Rights Act 1998 Article 8 gives a 'right to respect for private and family life, home and correspondence'. Case law suggests that employees have a reasonable expectation of privacy in the workplace.

General Data Protection Regulations (GDPR) May 2018 which describes how organisations must collect, handle and store personal information.

The Regulation of Investigatory Powers Act 2000 covers the extent to which organisations can use covert surveillance.

Computer Misuse Act 1990 made it an offence to access any computer to which a person does not have an authorised right to use. The Act introduced three criminal offences:

1. Unauthorised access to computer material.
2. Unauthorised access with intent to commit or facilitate commission of further offences.
3. Unauthorised modification of computer material

5 Roles and Responsibilities

5.1 Chief Executive Officer

The Chief Executive Officer is responsible for the overall management of information security, and should also ensure that all employees and volunteers are trained to understand, implement and maintain the security objectives set out in this policy and as detailed in any work instructions.

5.2 IT Support

The person or persons fulfilling the role of IT support are responsible for operating within the confines of their authorisation in terms of upholding the confidentiality, integrity and access to personal and organisational information/data and not abusing their privileged access rights.

IT support personnel are also responsible for ensuring that any access rights,

applications, tools and equipment provided to staff and volunteers are provided with the appropriate limitations to access rights, profiles and security measures that enables WEFB services to be delivered efficiently and effectively but without compromising security.

5.3 All Staff and Volunteers

Information Security is the responsibility of all staff and volunteers, who are expected at all times to act in a professional and responsible manner whilst conducting WEFB business, in line with WEFB's Code of Conduct. All staff are responsible for information security and remain accountable for their actions in relation to WEFB information and information systems. All employees have a responsibility not to compromise WEFB, e.g. by sending defamatory or harassing electronic mail, or by making unauthorised purchases, and must also be aware that the confidentiality and integrity of information transmitted by E-mail or facsimile may not be guaranteed.

Access by employees to the Internet via computing facilities provided by WEFB is restricted to business use only.

Staff and volunteers granted access to WEFB's information systems must only use their own login IDs, keep their passwords private and must not share usernames or passwords with anyone else. Passwords should also be changed on a regular basis; it is recommended that they are changed every three months. Staff and volunteers should ensure that they understand their role and responsibilities, and that failure to comply with this policy may result in the withdrawal of access rights and/or disciplinary action.

6 Securing Data

The following section outlines the procedures to be used by WEFB to secure essential organisational data. A summary of these procedures is shown in Appendix 1, taken from the National Cyber Security Centre's "Small Charity Guide" (November 2018).

6.1 Backing up "cloud" based applications

Whenever possible WEFB will utilise "cloud" based resources and rely on the provider of those resources to guarantee industry-wide best practice on the reliability and frequency of their data backup and recovery procedures; such resources include Office 365, AdvicePro, Trussell Trust Systems and Volunteer Impact, for the storage of client data, volunteer data and organisational administration data.

When considering the use of cloud-based applications WEFB will use the National Cyber Security Centre's guidance on how to configure, deploy and use cloud services securely (https://www.ncsc.gov.uk/collection/cloud-security).

6.2 Backing up other digital information

Should any other computer-based data not be being supported by cloud-based applications any essential data will be backed up by WEFB staff at least once a week. The backups, whether on a USB, on a separate drive or a separate computer,

will be restricted so that they:

- Are not accessible by all staff or volunteers
- Are not permanently connected (either physically or over a local network) to the device holding the original copy.

Ideally, the backup copies will be held off-site in a different physical location from the original copy.

6.3 Lost or stolen devices

The majority of devices include free web-based tools that can mitigate the impact of their loss. Users of WEFB phones, tablets and other devices are encouraged to use these tools which can:

- track the location of the device
- remotely lock access to the device, to prevent other people using it
- remotely erase the data stored on the device
- retrieve a back up data stored on the device.

6.4 Use of Wi-Fi Hotspots

WEFB staff and volunteers undertaking WEFB business are not allowed to connect to the Internet using unknown or unsecured Wi-Fi hotspots, instead they should use a 3G or 4G mobile network, or a Virtual Private Network (VPN) provided by a reputable service provider.

6.5 Protection from Malware

Malware, i.e. malicious software, is software or web content that can harm the charity, usually through the deployment of viruses, which are self-copying programs that infect legitimate software. In order to protect against malware will carry out the following steps.

- Install and activate antivirus software on all computers, laptops and tablets.
- Prevent the download or installation of any unauthorised software applications from unknown vendors/sources. Third party applications downloaded onto WEFB phones or computers must be approved by the CEO and only downloaded from manufacturer-approved stores, such as Google Play or Apple App Store.
- Ensure that operating systems on all WEFB devices are always kept up to date with the latest versions from software developers, hardware suppliers and vendors. Operating systems, programs, phones and apps will be set to “automatically update” wherever this is an option.
- Replace devices and operating systems when suppliers end their support for older models/versions and updates are no longer be available.

- Use “firewalls” to create a “buffer zone” between the WEFB network and external networks.
- Raise awareness of malicious emails and scams to prevent phishing attacks trying to gain access to sensitive data.

7 WEFB Social Media Core Values

The following sets out the core values that WEFB will deploy in the online social media community:

7.1 Transparency in every social media engagement.

WEFB does not condone manipulating the social media flow by creating “fake” destinations and posts designed to mislead followers and control a conversation. Every web site, Twitter “account”, or other online destination that is ultimately controlled by WEFB or its associates must make that fact known to users and must be authorised according to applicable internal protocols in order to track and monitor WEFB’s online presence. WEFB also requires bloggers and social media influencers to act with transparency and honesty in all their dealings.

7.2 Protection of our clients’ privacy.

This means that all staff and volunteers should be conscientious regarding any Personally Identifiable Information (PII) that WEFB collects, including how we collect, store, use, or share that PII, all of which should be done pursuant to WEFB’s Personal Data Protection Policy

7.3 Protection of staff privacy.

WEFB will balance the need for monitoring staff safety and behaviour with their right to privacy.

7.4 Protection of job applicants’ privacy.

WEFB will be mindful of all legislative and regulatory requirements protecting the privacy of any job applicants and will not put pressure on applicants to grant access to online social media accounts nor make any unauthorised access to online social media accounts.

7.5 Copyright

WEFB and its associates will respect all copyrights, trademarks, rights of publicity, and other third-party rights in the online social media space, including user-generated content (UGC).

7.6 Responsibility in use of technology.

WEFB personnel will not use or align WEFB with any organisations or web sites that deploy the use of excessive tracking software, adware, malware or spyware.

7.7 Maintaining Best Practice

WEFB will utilise best practices, including listening to the online community, and compliance with applicable regulations to ensure that these online social media principles remain current and reflect the most up-to-date and appropriate standards of behaviour.

8 Staff and Volunteers' Use of Online Social Media

There's a big difference between speaking "on behalf of WEFB" and speaking "about" WEFB. This set of principles refers to those personal or unofficial online activities where staff and volunteers might refer to WEFB.

8.1 Adhere to the Code of Conduct and other applicable policies.

All WEFB staff and volunteers are subject to the Code of Conduct in every public setting. In addition, other policies, including the Personal Data Protection Policy, govern staff and volunteers' behaviour with respect to the disclosure of information; these policies are applicable to all personal activities online, as well as the unauthorised removal or copying of personal or organisational information/data.

8.2 Staff and volunteers are responsible for their actions.

Staff and volunteers should be aware that anything that they post online or email that can potentially tarnish WEFB's image will ultimately be their own responsibility. WEFB encourage staff and volunteers to participate in online social media, but urge all personnel to do so properly, exercising sound judgement and common sense.

8.3 Pass on compliments and criticism.

Even if staff and volunteers are not official online spokespersons for WEFB, they are recognised as one of WEFB's most vital assets for monitoring social media. If staff or volunteers come across positive or negative remarks about WEFB or its associates, e.g. the Trussell Trust, online that they believe are important, they should consider sharing them by forwarding them to the person tasked with WEFB Public Relations.

8.4 Senior Officer(s) respond to negative posts.

If staff or volunteers come across negative or disparaging emails/posts about WEFB or its associates, or see third parties trying to spark negative conversations, unless they are an authorised online spokesperson, they should avoid reacting to the post(s) themselves. Staff and volunteers should pass the email(s)/post(s) along to the appropriate spokesperson trained to address such comments.

8.5 Be conscious when mixing business and personal lives.

Online a person's personal and business personas are likely to intersect. WEFB respects the free speech rights of all of its associates, but likewise they must remember that clients, colleagues, donors and supporters often have access to the online content they post or email. Staff and volunteers are required to keep this in mind when publishing information online that can be seen by more than friends and family, and know that information originally intended just for friends and family can be

forwarded on. Staff and volunteers must never to disclose non-public information of WEFB (including confidential information), and be aware that taking public positions online that are counter to WEFB's interests might cause conflict.

9 Online Spokespeople/Representatives

Just as with traditional media, WEFB have an opportunity – and a responsibility – to effectively manage WEFB's reputation online and to selectively engage and participate in social media. The following principles guide how authorised spokespeople should represent WEFB in an online, official capacity when they are speaking on behalf of WEFB:

1. Be trained in the use of Social Media.

2. Follow the Code of Conduct and all other Company policies, i.e. as a representative of WEFB they must act with honesty and integrity in all matters

3. Be mindful that they are representing WEFB. As an official representative, it is important that all posts be respectful of all individuals in accordance with the Equality and Diversity policy and associated legislation.

4. Fully disclose affiliation with WEFB. WEFB requires all associates who are communicating on behalf of WEFB to always disclose their name and their affiliation. It is never acceptable to use aliases, to speak anonymously or otherwise deceive people.

5. Keep records. It is critical that representatives keep records of their interactions in the online social media space and monitor the activities of those with whom they engage. Because online conversations are often fleeting and immediate, it is important to keep track of them when officially representing WEFB. Representatives must be aware that online WEFB statements can be held to the same legal standards as traditional media communications.

6. When in doubt, do not post. Associates are personally responsible for their words and actions, wherever they are. Online spokespeople must ensure that their posts and emails are completely accurate and not misleading, and that they do not reveal non-public information of WEFB.

7. Give credit where credit is due and don't violate others' rights. Representatives must not claim authorship of something that is not theirs. If using another party's content, they must make certain that they are credited for it in the post and that they approve of WEFB utilising their content. Representatives must not use the copyrights, trademarks, publicity rights, or other rights of others without the necessary permissions of the rightsholder(s).

8. WEFB copyright. Any content generated by or on behalf of WEFB will remain the copyright or WEFB, and WEFB will retain the Intellectual Property Rights of, for example, any original artwork, photography, video, music, web content and sound recordings.

9. Be responsible to your work. WEFB understands that associates engage in online social media activities at work for legitimate purposes and that these activities may be helpful to WEFB. However, WEFB encourages all associates to exercise sound judgement and common sense to prevent online social media sites from becoming a distraction at work.

10. Remember that local posts can have global significance. The way that a spokesperson answers an online question might be accurate in some parts of the world, but inaccurate (offensive or even illegal) in others. Representatives should keep that "world view" in mind when participating in online conversations.

11. Know that the Internet is permanent. Once information is published online, it is essentially part of a permanent record, even if a person "removes/deletes" it later or attempts to make it anonymous. If a complete thought, along with its context, cannot be squeezed into a character-restricted space (such as Twitter), it is good practice to provide a link to an online space where the message can be expressed completely and accurately.

10 Equality and Diversity

WEFB is committed to ensuring that the way it provides services to the public and the way staff are treated reflects their individual needs and does not discriminate against individuals or groups on any grounds. This policy has been appropriately assessed.

11 Monitoring and Compliance

WEFB will maintain effective monitoring systems to ensure implementation of this policy, including the following:

Standard/ process / issue	**Monitoring and audit**			
	Method:	**By:**	**Reporting to:**	**Frequency:**
Breaches	Report of Incident	Staff/Volunteers	CEO	As and when incident occurs
Backup of locally held data	Regular Audit	Line Manager	CEO	Monthly

12 Amendments Table

Version	**Effective From**	**Date of Review**	**Changes made**
1			
2	19 November 2019	19 November 2020	Rewrite of Version 1 (undated)
2.1	18 November 2020	18 November 2022	Inclusion of new para 6 on Securing Data.

National Cyber Security Centre
a part of GCHQ

Cyber Security
Small Charity Guide

This advice has been produced to help charities protect themselves from the most common cyber attacks. The 5 topics covered are easy to understand and cost little to implement. Read our quick tips below, or find out more at **www.ncsc.gov.uk/charity** .

Backing up your data

Take *regular* backups of your important data, and *test* they can be restored. This will reduce the inconvenience of any data loss from theft, fire, other physical damage, or ransomware.

- **Identify what needs to be backed up.** Normally this will comprise documents, emails, contacts, legal information, calendars, financial records and supporter or beneficiary databases.
- **Ensure the device containing your backup is *not* permanently connected** to the device holding the original copy, neither physically nor over a local network.
- **Consider backing up to the cloud.** This means your data is stored in a separate location (away from your offices/devices), and you'll also be able to access it quickly, from anywhere.

Keeping your smartphones (and tablets) safe

Smartphones and tablets (which are used outside the safety of the office and home) need even more protection than 'desktop' equipment.

- **Switch on PIN/password protection/fingerprint recognition** for mobile devices.
- Configure devices so that when lost or stolen they can be **tracked**, **remotely wiped** or **remotely locked**.
- Keep your **devices** (and all **installed apps**) **up to date**, using the '**automatically update**' option if available.
- When sending sensitive data, don't connect to public Wi-Fi hotspots - **use 3G or 4G connections** (including tethering and wireless dongles) or **use VPNs**.
- **Replace devices that are no longer supported by manufacturers** with up-to-date alternatives.

Preventing malware damage

You can protect your charity from the damage caused by 'malware' (malicious software, including viruses) by adopting some simple and low-cost techniques.

- **Use antivirus** software on all computers and laptops. **Only install approved software** on tablets and smartphones, and prevent users from downloading third party apps from unknown sources.
- **Patch all software and firmware** by promptly applying the latest software updates provided by manufacturers and vendors. Use the '**automatically update**' option where available.
- **Control access to removable media** such as SD cards and USB sticks. Consider disabling ports, or limiting access to sanctioned media. Encourage staff to transfer files via email or cloud storage instead.
- **Switch on your firewall** (included with most operating systems) to create a buffer zone between your network and the Internet.

Avoiding phishing attacks

In phishing attacks, scammers send fake emails asking for sensitive information (such as bank details), or containing links to bad websites.

- Ensure staff **don't browse the web or check emails** from an account with **Administrator privileges**. This will reduce the impact of successful phishing attacks.
- **Scan for malware** and **change passwords** as soon as possible if you suspect a successful attack has occurred. **Don't punish staff** if they get caught out (it discourages people from reporting in the future).
- Check for obvious signs of phishing, like **poor spelling and grammar**, or **low quality versions** of recognisable logos. Does the sender's email address look legitimate, or is it trying to mimic someone you know?

Using passwords to protect your data

Passwords - when implemented correctly - are a free, easy and effective way to prevent unauthorised people from accessing your devices and data.

- Make sure all laptops, MACs and PCs **use encryption products** that require a password to boot. Switch on **password/ PIN protection** or **fingerprint recognition** for mobile devices.
- **Use two factor authentication (2FA)** for important websites like banking and email, if you're given the option.
- **Avoid using predictable passwords** (such as family and pet names). Avoid the most common passwords that criminals can guess (like *passw0rd*).
- Do not enforce regular password changes; they only need to be changed when you suspect a compromise.
- **Change** the manufacturers' default passwords that devices are issued with, before they are distributed to staff.
- **Provide secure storage** so staff can write down passwords and keep them safe (but not with the device). Ensure staff can reset their own passwords, easily.
- **Consider using a password manager.** If you do use one, make sure that the 'master' password (that provides access to all your other passwords) is a strong one.

For more information go to www.ncsc.gov.uk @ncsc