



IT & SYSTEMS POLICY

POLICY CONTROL

Version	Description	Date	Approval
0.1	IT & Systems Policy	21 March 2024	
1.0	Board approval	11 June 2024	Board
Next Review:		June 2027	
Owner:		Foodbank Manager – Zoe Nixon	

LINKED POLICIES & DOCUMENTS

Privacy Policy
Data Protection Policy
Communications Policy
Social Media Policy

APPENDICES

IT & SYSTEMS POLICY

1. INTRODUCTION

This policy outlines the standards staff members must observe when using Newquay Foodbank's IT and communications systems.

Newquay Foodbank is registered with the Information Commissioner as a Data Controller (ref A8753034) and is also a Data Processor on behalf of the Trussell Trust. All staff members are required to read and understand the Data Protection Policy that should be read in conjunction with this IT & Communications Policy.

The term "staff members" is used in Newquay Foodbank's policies to refer to any employees, volunteers, trustees or contractors that are 'working' for the Foodbank. "Foodbank visitors" is the term used to describe Foodbank beneficiaries.

2. WHO THIS POLICY APPLIES TO

This policy applies to all Newquay Foodbank staff members who have access to Foodbank owned IT equipment eg laptops; phones; email addresses and access to IT systems such as SharePoint or DCS.

3. EQUIPMENT & PASSWORDS

You are responsible for the security of all IT equipment whilst you are using it and must not allow it to be used by anyone other than in accordance with this policy.

You must use passwords on all Foodbank IT equipment & passwords must be kept confidential and not recorded anywhere.

You must only log on to the IT systems using the log in details specifically allocated to you by your Foodbank Manager. You must not use another person's log in details or share your username and password with other staff members.

You must log out and shut down all IT equipment at the end of each day / your session.

When accessing systems that utilise a generic or shared account and password – eg social media platforms or a session account, you must only change the password in exceptional circumstances. Changes should be advised to financeadmin@newquayfoodbank.co.uk in order for the Master Password Manager to be updated and ensure other users are made aware.

4. SYSTEMS & DATA SECURITY

You should not destroy, delete or modify existing systems, programmes, information or data (except as authorised by the Foodbank Manager in the proper performance of your duties).

You must not download or install software from external sources without authorisation from the Foodbank Manager.

You must not attach any device or equipment including mobile phones, tablet computers or USB storage devices to our systems without authorisation from the Foodbank Manager.

You should exercise particular caution when opening unsolicited emails from unknown sources. If an email looks suspicious do not reply to it, open any attachments or click any links in it.

Inform the Foodbank Manager if you suspect the IT equipment may have a virus.

5. EMAIL

All staff members must adopt a professional manner and observe appropriate etiquette when communicating with others by email.

Remember that email can be used in legal proceedings and that even deleted emails may remain on the system and be capable of being retrieved.

You must not send abusive, obscene, discriminatory, racist, harassing, derogatory, defamatory, pornographic or otherwise inappropriate emails.

You should not:

- Send or forward private emails on Foodbank computers
- Send or forward chain mail, junk mail, cartoons, jokes or gossip
- Contribute to system congestion by sending trivial messages or unnecessarily copying or forwarding emails to those who do not have a real need to receive them
- Send messages from another person's email address
- Use your own personal email account for any emails that may include confidential information regarding Foodbank visitors. Only use the email account we have provided for you.

6. INTERNET USE

Internet access is provided primarily for the running and operating of the Foodbank. You should not use Foodbank IT equipment to access the internet for personal use.

You should not access any web page or download any image or other file from the internet which could be regarded as illegal, offensive, in bad taste or immoral. Even web content that is legal in the UK may be in sufficient bad taste to fall within this prohibition. As a general rule if any person might be offended by the contents of a page, or if the fact that our software has accessed the page or file might be a source of embarrassment if made public, then viewing it will be a breach of this policy.

We may block or restrict access to some websites at our discretion.

7. MONITORING

Our systems enable us to monitor telephone, email, voicemail, internet and other communications. As part of the running of the Foodbank, our telephone and computer systems may be continually monitored by automated software or otherwise.

We reserve the right to retrieve the contents of email messages or check internet usage (including pages visited and searches made) as reasonably necessary in the interests of the running of the Foodbank, including but not limited to, the following purposes:

- To monitor whether the use of the email system or the internet is legitimate and in accordance with this policy
- To find lost messages or to retrieve messages lost due to computer failure
- To assist in the investigations of alleged wrongdoing
- To comply with any legal obligation.

8. PROHIBITED USE OF OUR SYSTEMS

Misuse or personal use of our telephone or email system or inappropriate internet use will be dealt with under our Disciplinary procedure. Misuse of the internet can in some cases be a criminal offence.

Creating, viewing, accessing, transmitting or downloading any of the following material will amount to gross misconduct:

- Pornographic material
- Offensive, obscene or criminal material or material which is liable to cause embarrassment to us or to our partners or to people coming to Foodbanks
- A false and defamatory statement about any person or organisation
- Confidential information about us, staff members or Foodbank visitors (except as authorised in the performance of your role)
- Unauthorised software
- Any other statement which is likely to create any criminal or civil liability (for you or us)
- Music or video files or other materials in breach of copyright.

9. STATUS OF THIS POLICY

This policy does not form part of the formal contract of employment, but it is a condition of employment that staff members will abide by the rules and policies made by Newquay Foodbank from time to time.

Compliance is the responsibility of all staff members.

Any breach of this policy may lead to disciplinary action being taken, or even a criminal prosecution. Any questions or concerns about the interpretation or operation of this policy should be taken up with the Foodbank Manager.

10. REVIEW

This policy and its implementation will be reviewed at least every three years, or where significant change occurs.

