IT and Communications policy

About this policy

- This policy outlines the standards employees and volunteers must observe when using the food banks IT and communications systems.
- Breach of this policy will be dealt with under our Problem Solving Procedure.

Equipment security and passwords

- You are responsible for the security of the IT equipment whilst you are using it and you must not allow it to be used by anyone other than in accordance with this policy.
- You should use passwords on all food bank IT equipment. Passwords must be kept confidential.
- You must only log on to the IT systems using the log in details given to you by *your Main Contact*. You must not use another person's log in details or share your username and password with other employees and volunteers *without permission from your Main Contact.*
- You must log out and shut down the computer at the end of each day / your session.

Systems and data security

- You should not destroy, delete or modify existing systems, programmes, information or data (except as authorised *by your Main Contact* in the proper performance of your duties).
- You must not download or install software from external sources without authorisation from *your Main Contact*.
- You must not attach any device or equipment including mobile phones, tablet computers or USB storage devices to our systems without authorisation from *your Main Contact*.
- 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 *your Main Contact* if you suspect the IT equipment may have a virus.

Email

- Adopt a professional manner and observe appropriate etiquette when communicating with others by email.
- Always use our standard email signature
- 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 the food bank computer which you would not want a third party to read
- 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 or

- Send messages from another person's email address (unless authorised *by your Main Contact*) or under an assumed name
- Use your own personal email account to send or receive emails relating to the running and operations of the food bank. Only use the email account we have provided for you.

Using the internet

- Internet access is provided primarily for the running and operating of the food bank.
- 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.

Monitoring

- Our systems enable us to monitor telephone, email, voicemail, internet and other communications. As part of the running of the food bank, 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 searched made) as reasonably necessary in the interests of the running of the food bank, including for the following purposes (this list is not exhaustive):

- 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.

Prohibited use of our systems

Misuse or excessive personal use of our telephone or email system or inappropriate internet use will be dealt with under our Problem Solving procedure. Misuse of the internet can in some cases by 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 food banks
- A false and defamatory statement about any person or organisation
- Confidential information about us, employees or volunteers or the people who use the food banks (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.

Approved & Issued:	Reviewed:	Next Review:
10th March 2021	10th May 2023	May 2024