#FBF696 trading as Norwich OUTPOST

IT Policy

1. Purpose
2. Policy Statement
3. Organisation Responsibilities
4. Internet Access
5. Subject Access Requests
6. Legal requirements

Issue date: 30/05/2020
Review date: 30/05/2021

1. Purpose

The purpose of this document is to define our IT policy and applies to all employees and volunteers of OUTPOST regardless of status or length of service in relation to the IT usage in the organisation.

This policy is for guidance only and does not form part of the contract of employment or voluntary service.

2. Policy statement

The organisation is required to ensure that all users of the organisation's information systems are aware that their use of the facilities by the Steering Committee.

Information systems means but is not limited to all of the organisation’s computer systems or equipment including hardware, software, data and removable media e.g. CDs, DVDs, USB pen drives. It also includes access to email and internet facilities and telephones.

European and UK legislation allows the monitoring of systems and network traffic without consent for legitimate purposes such as but not limited to:

- Policing regulatory compliance.
- Safeguarding the integrity of the organisation’s Information Technology Infrastructure.
- Fault investigations and Incident handling.
- Authorised Law enforcement requests.
- Preventing or detecting crime, unauthorised use, unauthorised disclosures of the organisation’s confidential information or the use of unlicensed software.
- Preventing or detecting the transmission of inappropriate material.
- Enabling the proper performance of business matters during an individual's absence from work.
- Recording evidence of transactions.

Monitoring may be manual and may take the form of spot checks, audits or filtering of communications and collation of usage data.

All internet data that is composed, transmitted and/or received by the organisation's computer systems is considered to belong to the organisation and is recognised as part of its official data. It is therefore subject to disclosure for legal reasons or to other appropriate third parties.

The equipment, services and technology used to access the Internet are the property of the organisation and the organisation reserves the right to monitor Internet traffic and monitor and access data that is composed, sent or received through its online connections.

Emails sent via the organisation email system should not contain content that is deemed to be offensive. This includes, though is not restricted to, the use of discriminatory, vulgar or harassing language/images. All sites and downloads may be monitored and/or blocked by the organisation if they are deemed to be harmful and/or not productive to business.

Any breaches of this policy may result in disciplinary action up to and including summary dismissal in the case of serious breaches.

3. Organisation Responsibilities

The organisation will ensure that it complies with all necessary and relevant legislation and regulation in relation to the monitoring of its information systems. Authorised organisation personnel including but not limited to the Steering Committee and Trustees.

3.1. Respect the privacy of others.

- Not use or disclose information realised in the monitoring process for purposes other than those for which the process was approved.
- Safeguard information collected in the monitoring process.
- Destroy information collected in the monitoring process when it is no longer required.

4. Internet Access

Access to the Internet is available to all employees and volunteers. Access to certain sites may be monitored, blocked and/or restricted at the organisation’s discretion, without prior notification to users. Unacceptable use of email and the internet by employees and volunteers includes, but is not limited to:

- Sending, posting or viewing discriminatory, harassing, or threatening messages, footage or images on the Internet.
- Copying inappropriate material and/or attachments to other users.

- Using the organisation’s systems to perpetrate any form of fraud and/or software, film or music piracy.
- Stealing, using, or disclosing someone else's password without authorisation.
- Downloading, copying or pirating software and electronic files that are copyrighted
  or without authorisation
- Hacking into unauthorised websites.
- Sending or posting information that is defamatory to the organisation, its services, colleagues and/or customers and suppliers.
- Introducing malicious software onto the organisation’s network and/or jeopardising the security of the organisation's electronic communications systems.
- Sending or posting chain letters, solicitations, or advertisements not related to business purposes or activities.
- Passing off personal views as representing those of the organisation.
- Breaching copyright and licensing laws when composing e-mails and attachments.
- Sending commercially sensitive or confidential information by e-mail without prior
  approval from a line manager or other appropriate member of management.
- Sending personal identifiable information (including but not limited to employees
  and volunteers) except to serve a specific business purpose and only to internal email addresses.
- Gaining access to e-mails addressed to other users.

5. Subject Access Requests

Any individual is entitled to make a request to obtain copies of any personal information relating to them and held by the organisation either in paper or electronic format.