Dudley Federation of Tenants and Residents Associations
01384 868010 -- www.dftra.org.uk -- info@dftra.org.uk
www.facebook.com/dudleyfed -- www.twitter.com/DudleyFed -- www.instagram.com/dudleyfed

Acceptable Usage Policy for IT systems and data

1. Introduction

This Acceptable Use Policy (AUP) is designed to protect Dudley Federation of Tenants and Residents Associations (DFTRA), our employees, volunteers, members and other partners from harm caused by the misuse of our IT systems and our data. Misuse includes both deliberate and inadvertent actions. The purpose of this policy is to establish acceptable and unacceptable use of electronic devices and network resources at DFTRA in conjunction with its established culture of ethical and lawful behaviour, openness, trust, and integrity.

The repercussions of misuse of our systems can be severe. Potential damage includes, but is not limited to, malware infection (e.g. computer viruses), legal and financial penalties for data leakage, and lost productivity resulting from network downtime.

All board members and staff at DFTRA are responsible for the security of our IT systems and the data on them and must manage them responsibly to maintain the confidentiality, integrity, and availability of its information assets. As such, all employees must ensure they adhere to the guidelines in this policy at all times. Should any employee be unclear on the policy or how it impacts their role they should speak to the Chairperson, Organisation Manager or the DFTRA Board as a whole.

2. Definitions

“Users” refers to everyone who has access to any of DFTRA’s IT systems. This includes permanent employees and also temporary employees, volunteers, members, visitors, and partners.

“Systems” means all IT equipment that connects to the corporate network or access corporate applications. This includes, but is not limited to, desktop computers, laptops, smartphones, tablets, printers, data and voice networks, networked devices, software, electronically-stored data, portable data storage devices, third party networking services, telephone handsets, video conferencing systems, and all other similar items commonly understood to be covered by this term.

3. Scope

This is a universal policy that applies to all Users and all Systems. This policy covers only internal use of DFTRA’s systems, assets owned or leased by DFTRA, or to devices that connect to the network or reside at the DFTRA offices.

Board members at DFTRA who monitor and enforce compliance with this policy are responsible for ensuring that they remain compliant with relevant local legislation at all times.

4. Use of IT Systems

DFTRA’s systems exist to support and enable the organisation. A small amount of personal use is, in most cases, allowed. However it must not be in any way detrimental to users own or their colleagues productivity and nor should it result in any direct costs being borne by DFTRA other than for trivial amounts (e.g., an occasional short telephone call).

DFTRA trusts volunteers and employees to be fair and sensible when judging what constitutes an acceptable level of personal use of the company’s IT systems. If employees or volunteers are uncertain, they should consult the Chairperson or the DFTRA board.

Dudley Federation of Tenants and Residents Associations
01384 868010 -- www.dftra.org.uk -- info@dftra.org.uk
www.facebook.com/dudleyfed -- www.twitter.com/DudleyFed -- www.instagram.com/dudleyfed

Any information that is particularly sensitive or vulnerable must be encrypted and/or securely stored so that unauthorised access is prevented (or at least made extremely difficult). However, this must be done in a way that does not prevent–or risk preventing–legitimate access by all properly-authorised parties.

DFTRA can monitor the use of its IT systems and the data on it at any time. This may include (except where precluded by local privacy laws) examination of the content stored within the email and data files of any user, and examination of the access history of any users.

DFTRA reserves the right to regularly audit networks and systems to ensure compliance with this policy.

5. Data Security

If data on DFTRA's systems is classified as confidential this should be clearly indicated within the data and/or the user interface of the system used to access it. Users must take all necessary steps to prevent unauthorised access to confidential information.

Users are expected to exercise reasonable personal judgement when deciding which information is confidential.

Users must not send, upload, remove on portable media or otherwise transfer to a non-DFTRA system any information that is designated as confidential, or that they should reasonably regard as being confidential to DFTRA, except where explicitly authorized to do so in the performance of their regular duties.

Users must keep passwords secure and not allow others to access their accounts. Users must ensure all passwords comply with DFTRA's safe password policy.

Users who are supplied with computer equipment by DFTRA are responsible for the safety and care of that equipment, and the security of software and data stored it and on other DFTRA systems that they can access remotely using it.

Because information on portable devices, such as laptops, portable data storage devices (USB sticks), tablets and smartphones, is especially vulnerable, special care should be exercised with these devices: sensitive information should be stored in encrypted folders only. Users will be held responsible for the consequences of theft of or disclosure of information on portable systems entrusted to their care if they have not taken reasonable precautions to secure it.

All workstations (desktops and laptops) should be secured with a lock-on-idle policy active after at most 10 minutes of inactivity. In addition, the screen and keyboard should be manually locked by the responsible user whenever leaving the machine unattended.

Users who have been charged with the management of those systems are responsible for ensuring that they are at all times properly protected against known threats and vulnerabilities as far as is reasonably practicable and compatible with the designated purpose of those systems.

Users must at all times guard against the risk of malware (e.g., viruses, spyware, Trojan horses, rootkits, worms, backdoors) being imported into DFTRA's systems by whatever means and must report any actual or suspected malware infection immediately.

Dudley Federation of Tenants and Residents Associations
01384 868010 -- www.dftra.org.uk -- info@dftra.org.uk
www.facebook.com/dudleyfed -- www.twitter.com/DudleyFed -- www.instagram.com/dudleyfed

6. Unacceptable Use

All employees should use their own judgment regarding what is unacceptable use of DFTRA's systems. The activities below are provided as examples of unacceptable use, however it is not exhaustive. Should an employee need to contravene these guidelines in order to perform their role, they should consult with and obtain approval from their manager before proceeding.

- ✕ All illegal activities. These include theft, computer hacking, malware distribution, contravening copyrights and patents, and using illegal or unlicensed software or services. These also include activities that contravene data protection regulations.
- ✕ All activities detrimental to the success of DFTRA. These include sharing sensitive information outside the company, such as member information, as well as defamation of the organisation.
- ✕ All activities for personal benefit only that have a negative impact on the day-to-day functioning of the business. These include activities that slow down the computer network (e.g., streaming video, playing networked video games).
- ✕ All activities that are inappropriate for DFTRA to be associated with and/or are detrimental to the company's reputation. This includes pornography, gambling, inciting hate, bullying and harassment.
- ✕ Circumventing the IT security systems and protocols DFTRA has put in place.

7. Enforcement

DFTRA will not tolerate any misuse of its systems and will discipline anyone found to have contravened the policy, including not exercising reasonable judgment regarding acceptable use. While each situation will be judged on a case-by-case basis by the DFTRA Board, employees and volunteers should be aware that consequences may include the termination of their employment or position as a Director.

Use of any of DFTRA's resources for any illegal activity will usually be grounds for summary dismissal, and DFTRA will not hesitate to cooperate with any criminal investigation and prosecution that may result from such activity.

Updated and agreed by the DFTRA board on: 10th June 2024.

Next review due by: July 2026.