Barking & Dagenham Giving

IT Protocols, policy and procedures

Originally published April 2024 by Magie Dang

Last updated July 2024 by Magie Dang

Barking & Dagenham
Giving

Contents

1. Purpose

The purpose of this IT policy is to start documenting and establishing the guidelines and procedures for the secure and efficient use of information technology resources within our organisation. It aims to ensure the confidentiality, integrity, and availability of data, protect against unauthorised access or use, and promote responsible and ethical IT practices. As such it is an evolving document that will continuously be updated as work progresses. This policy applies to all employees, contractors, and third-party users who have access to our organisation's IT resources, including but not limited to computer systems, networks, software, and data.

2. Acceptable Use

- All users must use IT resources responsibly, ethically, and in compliance with applicable laws and regulations.
- Users should not engage in any activities that may disrupt or compromise the integrity, availability, or confidentiality of IT resources.
- Unauthorised access, use, or distribution of sensitive information is strictly prohibited and will be considered a breach of GDPR.

3. Security

- Users must protect their login credentials and not share them with others.
- All devices connected to the organisation's network must have up-to-date antivirus software and security patches.
- All devices must be registered with the IT department to ensure that access is strictly employees. Any google access from unregistered devices must be removed from the network and a regularly check in with the IT/operations department will be enforced for security measures,
- Users should report any suspected security incidents, vulnerabilities, or breaches to a member of management immediately.
- Regular security awareness training should be provided to educate users about potential threats and best practices.

4. Password Management

- Users must adhere to the strong password policy (8+ characters, 1 number, 1 special character) for all applications and where prompted to enforce 2 factor authorisation.
- Passwords must be updated regularly in compliance with the application software's security policy in order to protect and defer security breaches

5. Data Management

- Users must adhere to data classification and handling policies to ensure the confidentiality, integrity, and availability of data.
- Access to sensitive data should be granted on a need-to-know basis, and appropriate access controls should be implemented.
- Regular data backups should be performed to prevent data loss, and backup integrity should be verified periodically.
- Personal data should be handled in accordance with applicable privacy laws and regulations.

6. Software and Hardware

- Only authorised software and hardware should be installed and used on organisation-owned devices.
  Acceptable software applications:

  Canva
  Google workspace/chrome
  Monday
  Sage
  Slack
  Wordpress
  Mailerlite

- Users should not attempt to bypass or disable any security measures implemented on IT resources.
- External storage devices are permitted for use with permission from the management team.
- Proper inventory management of hardware and software assets should be maintained.

7. Internet and email usage

- Internet and email usage should be for business purposes only and personal use should be limited and in compliance with organisational policies.
- Users should not visit or download content from unauthorised or potentially malicious websites.
- Users should exercise caution when opening email attachments or clicking on links from unknown sources, as they may contain malware or phishing attempts.

8. Incident Response

- An incident response plan should be established to address and mitigate any IT security incidents promptly.
- Users should be aware of the reporting procedures for security incidents and should report any incidents or suspicious activities immediately.
- The IT department should conduct regular incident response drills and review and update the incident response plan as needed.
- In the event of loss of any BDG registered devices, users must promptly sign out of the registered device through either another device or alert the operations team to evoke admin privileges to proceed. The CEO and operations manager must also be notified immediately to follow insurance procedures.

9. Monitoring and enforcement

- The organisation reserves the right to monitor and audit IT resources to ensure compliance with this policy.
- Violations of this policy may result in disciplinary action, up to and including termination of employment or legal consequences.