IT Acceptable Use Policy

Purpose and Scope

The IT Acceptable Use Policy outlines acceptable use of Information Technology (IT) resources, services, and systems. It is the responsibility of every IT User to adhere to the IT Acceptable Usage Policy at all times.

Definitions

Company – Refers to Pabulum Limited.

External Email - Any email destination that is not a Company address.

Generic Account – Any login account that is shared or is not tied to a specific individual.

Interactive Accounts – Any account where the user of the account must type in the password of the account to log in.

IT Services – As provided by Forge Dynamic for the purpose of delivering IT support services as described in the Company's Service Level Agreement and Forge Dynamic's Terms of Business.

IT Devices – Including but not limited to computers and servers, phones and wireless handheld devices including mobile devices, cell phones, smart phones, tablets and iPads provided to the IT User by the Company

Mobile IT Devices - Refers to any ICT equipment that is taken away from the office and used off-site.

IT Resources – Including but not limited to network connectivity, software and applications, files, file shares, and other intellectual property obtained electronically provided to the IT User by the Company.

IT User - Any individual utilising IT resources, services, and systems, whether an employee or non-employee (i.e. customer, vendor, contractor, etc.).

Messaging Systems – Including but not limited to electronic communication mediums such as email, instant messaging, blogs, social media, text, and SMS messages.

Named User - Unique identifier (ID) and password assigned by Forge Dynamic.

Phishing - Any attempt to obtain confidential information from Internet users, typically by sending an e-mail that looks as if it is from a legitimate organisation.

Removable Media and Storage Devices – Including but not limited to USB's, DVD's, thumb drives, removable hard drives, wireless handheld devices and MP3 players, etc.

1.0 User Responsibility

1.1 Authorised Use

The use of any IT Device and/or IT Resource is a privilege and must be used for business purposes only, except where restricted by local law.

- Information residing on IT Devices should be for business purposes only as prescribed by the Company:
- The large size of multi-media files can impact business operations (i.e. increase backup or restore times and cause processing delays), therefore it is the IT User's responsibility to manage multimedia files and ensure those stored on IT Devices are for Company use only.
- IT Users are responsible for deleting all "inappropriate" material (i.e. defamatory, obscene, discriminatory, harassing, etc.).
- If detected, non-business-related files and information may be deleted as permitted by the laws of the country of operation.
- IT Devices are not to be used for personal gain or profit, or to represent you as someone else.
- IT Users may not use other User Passwords, Interactive, Named User IDs or accounts, or attempt to capture or guess other User's passwords.
- An interactive generic account may only be used by authorised IT Users.

1.2 Privacy

User data may be subject to access by authorised personnel in the Company or Forge Dynamic.

1.3 Protecting IT Devices and Information

Follow established procedures for protecting information and managing passwords, please refer to the Password Usage Policy for guidance.

IT Users should not attempt to access operating systems, files, security systems, or administrative systems where they haven't been given the authorisation to do so, including:

- Using electronic mail, data, programmes, or other information sources that are not authorised by the Company.
- Connecting unauthorised networking devices to Company IT Devices and IT Resources.
- Attempting to connect a router, switch, or hub to Company IT Devices and IT Resources to create a network for your work group or department.

IT Users must not alter or delete internal security controls or configurations on IT devices. IT Users are responsible for properly securing all IT devices while not in use, as follows:

- Do not leave IT Devices in clear view in unattended vehicles or in hotel rooms.
- Do not leave IT Devices in a vehicle overnight.
- Do not leave IT Devices (i.e. computers, mobile devices, removable media and storage devices) unattended or unsecured while away from your assigned work space or while traveling.

1.4 Reporting an Information Technology Incident

Information security is everyone's responsibility and potential risks, loss, or weakness must be reported. Any breach, misuse, loss or theft of a Company IT Device, IT Resource, and/or information must be reported immediately to it@pabulum-catering.co.uk.

1.5 Applicable Laws

IT Users must obey all laws in effect in the country of operation, including but not limited to: copyright, trade secret, patent, software licensing and use, secure device use, other hardware use, and intellectual property laws.

1.6 Requesting IT Support Services

All IT Services must be requested through the Forge Dynamic Helpdesk on 0203 411 3852 or email to it@pabulum-catering.co.uk.

2.0 IT Device Use

2.1 IT Devices

Employees must utilise a Company provided computer to access the Company owned IT systems or other business related systems required to support their roles. Other IT Users are only allowed to access IT resources and other Company systems as prescribed by the Company. In addition:

- The relocation or re assignment of IT Devices must be done by Forge Dynamic.
- Company owned IT devices no longer in use and that are to be decommissioned must be notified to Forge Dynamic.
- Donating or gifting of Company owned, decommissioned IT Devices is not permissible. Forge Dynamic will collect and dispose of all decommissioned IT Devices in compliance with the appropriate laws.

2.1.1 Data Protection and Security

- Do not set up your personal email address on the device.
- Do not link up, download, or otherwise access personal third-party apps or services, such as Dropbox or other storage; on-demand TV; other media streaming services.
- Usage of any social media accounts must be aligned to the Social Networking Policy.
- Staff must set a complex password on their mobile device such as phone and tablets.
- You must not jailbreak your device, or otherwise hack, tamper or attempt to fix the device in any way, if the device requires support, then please contact the Forge Dynamic Helpdesk.

2.1.2 User Responsibility

- Your Mobile IT Device (Laptop) must be transported in a suitably protective case (such as a sleeve, or padded backpack), this will be provided by the company.
- Handle your device with care and respect. Do not throw, damage, place heavy items on, or intentionally drop your device.
- Do not keep or leave your Mobile IT Device unattended in vehicles.
- Keep your device safe and secure at all times. You should know where your device is at all times.

2.1.3 Lost, Damaged, or Stolen Devices

- If your Mobile IT Device becomes lost or has been stolen, report it to the Forge Dynamic Helpdesk immediately.
- If your device has become damaged, report it to Forge Dynamic, and Forge Dynamic will liaise with the user to arrange collection of the device if necessary.
- You must not carry out repairs on any company-owned device.
- You must not solicit any individual or company to repair a company owned device on your behalf.

2.1.4 Equipment Return or Purchase by Departing Employees

Phones, tablets, or other mobile devices provided by the Company for employee use are the property of the Business and must be returned upon an employee's departure e.g. end of employment. These devices are valuable assets and may be needed by a new employee filling the open position. If assigned devices - including charging cable and power adapter - are not returned prior to departure, the value of any missing equipment will be deducted from the employee's final pay.

2.1.5 Replacement of Stolen or Damaged Devices

Employees are responsible for the safety and care of the devices provided to them. If a device is stolen or damaged in a way that renders it unusable and repair is not available (or is more expensive than a replacement device), funding for the repairs or replacement will be handled as follows:

Repair or replacement will be funded by the employee's department, it will be at the discretion of the Head of the Department or Finance Director as to whether to seek costs from the individual to cover all or a percentage of the costs for the damages or loss dependent on how this event occurred. All damages and losses must be reported to the Forge Dynamic Helpdesk.

If an employee is assigned multiple devices, this policy applies to all devices, collectively, not each device, individually.

2.1.6 Safeguarding

- Anyone found trying to access another staff member's device or associated content will be subject to disciplinary action.
- If a device is found, report to the Forge Dynamic Helpdesk immediately.
- Do not take photographs of others without their express permission.
- You are strictly forbidden from using your device to create, store, access, view, download, distribute, send, upload inappropriate content or materials.
- You are forbidden from utilising your device to partake in illegal activities of any kind.
- Do not use your device to post images, movies, or audio to a public facing part of the internet, without the express permission of all individuals imaged/recorded. Where this includes colleagues, refer to them and their Manager, and ensure that full permission has been received.
- Your device/s and any content are subject to routine and ad-hoc monitoring by Forge Dynamic. You must surrender your device upon request by any member of staff.

2.1.7 Personal Use

- Your Mobile IT Device is not permitted for personal use. It has been provided for work-related use only. Any non-work-related activities which have occurred additional costs will be reported, and these costs can be asked to be covered by the individual.
- Do not grant access to anyone, unless expressly authorised to do so by your Manager.
- Staff are prohibited to take or store personal photos/videos on devices as these may be seen by colleagues.
- If there is a request to use your devices abroad or for personal use, then a written request and agreement from a Director is required.

2.2 Data Storage and Removable Media

Company Data must be stored on the relevant OneDrive for Business, SharePoint Team Site or file server where it is backed up and secure.

Data stored on non-Company provided IT Devices and IT Resources may not be recoverable by Forge Dynamic in the event of failure/loss.

Individuals requiring removable media and storage devices to support their job function or where legitimate business reasons exist, must use an encrypted storage device as recommended by Forge Dynamic.

2.3 Software

A standard set of software has been provided on each employee's computer. Hardware and software that is provided by the Company must not to be modified or removed, except by Forge Dynamic.

Freeware, open sourced software, or trialware from any source may not be used without prior authorisation from the Company and where appropriate Forge Dynamic.

2.4 Intranet / Internet Use

Access to the Intranet and/or Internet is for business use, any personal use of the internet should follow the principal of "reasonable" usage, on your own time and/or outside of normal working hours.

3.0 Electronic Messaging Systems

3.1 Electronic Messaging Systems Use

Company provided messaging systems (e.g. Whatsapp, Skype) are for use by authorised IT Users on Company supplied equipment.

Personal use of Company provided messaging systems should follow the principal of "reasonable" usage, on your own time and/or outside of normal working hours.

IT users may only subscribe to automated newsletters or news group mail listings that are business or job related.

3.2 Company Email System Use

Messages having no business purpose must not be propagated using Company messaging systems:

- Video, audio clips or other file attachments, chain letters or unsolicited "junk" mail if received, should be deleted immediately.
- Sending or forwarding of Restricted information to any non-authorised email system is strictly prohibited.
- Do not archive emails outside of the Messaging System.
- IT Users must use best endeavours to minimise the exposure of their email accounts to malicious attacks:
    - Do not give out your Company email address to websites for non-business purposes.
    - Do not open spam mail attachments or click on provided links.
    - Do not reply to spam or junk mail.
    - Minimise the number of approved senders in your spam manager applications.

3.2.1 E-Mail Distributions

Internal e-mail distribution lists may not receive external email unless agreed and signed off from the business.

4.0 IT Passwords and Access

Password requirements are determined by the type of IT Device or IT Resource for which access is being granted.

4.1 Account Lock Out

All IT Users must lock their computer screen when they walk away from their computer:

- An unlocked or unattended computer can be accessed by unauthorised personnel who could compromise or access information on the computer or elsewhere on the network (i.e. File shares).
- If an account has a succession of 10 unsuccessful attempts to log in, the account will be locked out.

4.2 Account Reuse

All account IDs once deprovisioned cannot be reassigned. This applies to:

- Interactive and non-interactive accounts
- Internal and cloud service accounts

5.0 Exception to Policy

There may be business reasons to allow exceptions to this policy and the Company retains the right to make such exceptions as necessary and in accordance with applicable regulatory or legal statutes.

6.0 Non-Compliance

The consequences for policy violations will vary depending on the nature of the violation and are at the discretion of the Company, however all IT Users should be aware that failing to adhere to the Acceptable IT Usage Policy may result in disciplinary action.

Nelson Williams
Managing Director
(*This policy will be reviewed in August 2023*)

IT Acceptable Use Policy

I confirm that I have read and agree to the terms of the Pabulum IT Acceptable Use Policy.

Signed: _____

Name:

Job Title:

Date: _____