IT Acceptable Use Policy

Policy: IT001 – IT Acceptable Use

Owner: Board

Version: IT001 v1

Published Date: 03/01/2023

Next review: 03/01/2025

Contents

1. Policy Statement

This Policy sets out the obligations of Delamode Group, and its subsidiaries, whose correspondence address is 700 Avenue West, Skyline 120, Great Notley, Braintree, Essex, UK, CM77 7AA (the "COMPANY") regarding acceptable use of IT services and assets.

2. Purpose

The purpose of the Policy is to ensure employees, contractors and agents are clear on the acceptable use of IT assets (COMPANY data, IT systems, IT equipment, mobile devices, software, IT services and licenses).

3. Objectives

The Policy objectives

This policy explains the behaviours we expect from all IT users when it comes to working with COMPANY IT systems and data. To achieve this, we will explain the rules in these key areas

a. What's an IT asset?
b. What's acceptable and what's not acceptable when using COMPANY IT assets?
c. Can I purchase IT assets and when should I return IT assets?
d. Can I use company-provided IT assets for personal matters?
e. What are the rules on mobile devices?
f. What are the rules on using personally owned mobile devices?
g. What are the rules on storing and transferring data? and
h. How should I manage my passwords?
i. What's acceptable and what's not acceptable when using company email and internet?
j. What are the rules on social media?
k. What must I consider when remote working?
l. What must I consider when working from home?
m. What's our clear desk policy?
n. When and what should I report if I see a security issue?

4. What is an 'IT asset'?

An 'IT asset' includes, but is not limited to, COMPANY data, IT systems, IT equipment, mobile devices, software, IT services and licenses.

If you work on a desktop PC, or have a COMPANY provided laptop or mobile phone these are clear examples of IT assets. Other less obvious examples include the information in business application (Sage, FCL, Access Xsped), software license, or the server it resides upon.

5. What is acceptable behaviour when using COMPANY 'IT assets'

We expect you to follow these positive practices

a. IT assets must be used responsibly for business purposes.
b. Respect the confidentiality and privacy of other IT users.
c. Take responsibility for safeguarding and securing the IT assets.
d. Protect the integrity and confidentiality of data created, modified, or owned on our IT assets.
e. Where possible prevent the loss, falsification and or misuse of our data whilst using our IT assets; and
f. Adopt a clear desk approach to working.

6. What is not acceptable behaviour when using COMPANY 'IT assets'

Unless it's part of your job and you're authorised to do so, we expect you not to do any of the following using COMPANY 'IT assets'.

a. Browsing the private files or accounts of others. (Unless you have the correct permissions)
b. Breaching confidentiality, copyright, or legislation.
c. Procuring or transmitting material that is offensive or in violation of any applicable bullying, sexual harassment, discrimination, or workplace policies.
d. Using of online gambling.
e. Intentionally introducing malicious applications, such as malware and computer viruses into COMPANY IT assets.
f. Using COMPANY IT assets for fraudulent purposes.
g. Executing any form of network monitoring which, for example, intercepts data.
h. Attempting to defeat or bypass any security measures.
i. Unauthorised installation, modification, removal or disposal of any software or hardware.
j. The connection of any non-company owned mobile device to the COMPANY network; and Connectivity of any non-company owned storage device to any company owned device.

7. Can I purchase IT assets?

Because of the increasing cyber-risk and regulatory burden all software (including web-based subscription services) and hardware assets are procured through the IT department. This helps us to ensure assets are procured to corporate standards and processes. By ensuring that only approved IT assets are permitted to be purchased, installed, or used, we reduce our risk.

8. When should I return IT assets?

We expect all IT users in possession of company-provided IT assets and data to return them on termination of employment, termination of contract or when requested by their line manager. All IT users must ensure that any assets, including the data stored on them are left in an accessible and usable state by the COMPANY after they have left. This includes ensuring that email accounts have been prepared for access by others by removing any personal emails to ensure GDPR compliance.

Furthermore, we expect our line managers to proactively retrieve all tangible IT assets from their staff before their final working day and return them to IT for reuse and subscription licenses/access are removed

9. Can I use COMPANY provided IT assets for personal matters?

Yes, but with some rules... The company allows IT users the occasional personal use of company IT assets. The following rules must be followed.

Personal use must

a. Not have a negative impact on work or working relationships with colleagues.
b. Not have a negative impactive to company IT services
c. Be confined to your own time (i.e., before/after business hours, during lunch or breaks)
d. Not be used for commercial purposes not related to the COMPANY business.
e. Not store personal data especially data that would impact the performance of IT Assets or put the company of risk of GDPR fines (personal photos, password details, bank details etc,)

10. What are the rules on using mobile devices?

Our definition of a mobile device is any piece of equipment that can be taken off- premises and that can be used to remotely access or process COMPANY data.

We use mobile devices routinely in our business to access IT systems including email, file storage and business applications. The types of devices used include, but are not limited to, mobile phones, tablets, and laptops. It's vital that we ensure the physical security of mobile device at-all-times.

For employees allocated a mobile phone the following apply

a. All phones must have PIN set to prevent unauthorised access

b. Company-owned smartphones are property of the COMPANY and must be treated, used, and safeguarded as such. If an employee damages or loses a company-issued smartphone, the employee must notify the IT Support immediately and log a police report in event of theft. If a phone is lost, the employee will be issued with a spare phone from stocks held, any replacement phone will be paid for by department.

c. Any service minutes/data allowance that are "included" in the monthly plan are property of the COMPANY

d. Staff using corporately provided mobile devices are expected to limit personal data use to a minimum and, unless authorised, are not permitted to use premium mobile data services including.
    a. International roaming
    b. Premium rate numbers
    c. SMS voting and payment schemes
    d. Gambling and competition sites
    e. Music or Video streaming services

e. Staff are responsible for monitoring mobile device data usage and taking appropriate action to manage their spend, if any usage results in a significant overspend and it is proven to be no-business use you will be required to pay back the difference.

f. Phones provided by the company must have the provided cases and covers in place at all times, if damage is caused by either missing the employee may be liable for repair costs

g. When a phone is returned to the company access passwords must be provided to the phone to ensure it can be reused. If not, the employee will be charged the full cost to replace the phone

11. What are the rules for use of Personal Devices?

The COMPANY does not currently operate a Bring Your Own Device policy (BYOD), but the company does permit staff to use their own computers, smartphones, or other devices for limited work purposes such as email or teams.

a. If you use a personal computer, you must ensure it has suitable antivirus.
b. We expect at a minimum that all mobile devices containing COMPANY data must be protected from unauthorised access by an authentication method such as a pin, password, or unique identifier.
c. No third-party equipment is to be connected to the COMPANY internal network without prior approval and review of the Local IT Support team.

12. What are the rules on storing and transferring COMPANY data?

To ensure the company does not breach copyright or licensing laws, no personal media (such as music or movies) must be stored or played on the company systems. No privately owned or purchased software must be installed or used on COMPANY systems.

Confidential and Employee Sensitive data must not be stored on IT systems without appropriate controls to prevent unauthorised access.

The use of removable media, such as USB external drives and SD Cards, must be approved by the IT group, and the storage medium should only be used to transfer or store company owned data where no other more secure solution is available; The storage device must be encrypted. OneDrive should be sufficient in nearly all cases to share data.

Under no circumstances

a. Should company confidential or personal data be stored on non- company owned removable media.
b. Should company data be copied, stored, or transferred to any non- company approved applications, websites, or cloud service solutions, such as DropBox, Google Drive, etc.

13. How should I manage my passwords?

Passwords are an important protection for user accounts and a poorly chosen password may result in the compromise of company systems. We expect you to be responsible for following these password practices.

a. Use strong passwords, including combinations of letters, numbers, and special characters.
b. Use Multifactor authentication where available, it is mandatory for Microsoft 365 access
c. Change passwords periodically, typically at least every three months.
d. If you suspect that your account has been compromised, change your password, and notify IT Support immediately.
e. Ensure all passwords for administrative accounts are different from other accounts and have multifactor authentication
f. You should never enter or share your company account details and password; this includes to the help desk or IT support.
g. Only click on a password reset link when you have requested the link via the service website or logon screen.
h. Do not reuse, share, or write down credentials or passwords.
i. Do not enter passwords on a computer, device, IT service that you do not trust.
j. Insert both user credentials and passwords into the same message or document. They must be sent or stored separately

14. What's acceptable behaviour when using company email and internet?

We all need to remain vigilant of receiving malicious emails or browsing suspect websites. If you see one of these threats immediately report it to IT support

The following behaviour is expected when it comes to using our email and internet systems

a. COMPANY branding guidelines for email signatures must be complied with.
b. Email messages must be treated like any other form of correspondence and the content and language used must be professional and consistent with established company practices; and
c. Email must only be used in contract negotiations with appropriate authorisation from those with authority, and it must be made clear when email correspondence is not legally binding by marking it subject to contract.
d. You should only use your email account to register for external services for legitimate business use. We can see with the monitoring solutions that we receive emails from eBay and Spotify for example.
e. If you do need to register for an external service with your company email account, you should never use the same password that you use to logon to email or other internal IT systems.
f. If an email you receive from a trusted sender is different to the normal correspondence; especially if they are asking for personal details or the message contains a link or attachment you should call the sender to verify it is correct, alternatively log a call with your IT support desk to investigate.

15. What are the rules on social media?

Only those personnel officially designated by the COMPANY have the authorisation to speak on behalf of the company using social networking sites. However, we appreciate you may have professional networks and leverage social media as part of your role. If you are using social media, the following high-level principles must be followed

a. Do not bring the COMPANY name or brand into disrepute.
b. You are personally responsible for the content you publish
c. Unless expressly authorised to do so, do not create, or contribute to any social networking site pages using our customer names, brands, or logos under; and
d. Copyright, fair use and financial disclosure laws must be followed.

16. What must I consider for remote working?

Remote working can be of significant benefit and is sometimes necessary to achieve our goals. While we appreciate the advantages, we need to ensure security is maintained.

When travelling, you must always carry any IT assets as hand luggage. While using company-owned devices to remotely connect to the company network, you must ensure the computer being used is not also connected to any other un-trusted network. As a rule, do not connect to public networks if you are uncertain of their legitimacy.

Ensue all data is backed up regularly either using OneDrive or other storage solutions provided by the COMPANY.

17. What must I consider when working from home?

Working from home is now far more common, below are specific IT guidelines to read in conjunction with the Hybrid working from home policy.

You must ensure you always have sufficient internet bandwidth and internal access to conduct video conference calls and other company COMPUTER based activities.

Have good working knowledge of Microsoft teams, be available during working hours and clearly mark when you are not available.

IT can provide support on company supplied equipment but will not support personal devices (printers for example) or any issues with your internet support provider. If you lose internet connectivity you will be expected to attend the office.

You follow health and safety best practice for your home working environment.

Full IT support will only be provided in normal office business hours, the latest hours agreed with the business can be provided by your local IT support.

Comply with all aspects of the acceptable use, especially security

18. What's our clear desk policy?

The company has a clear desk and clear screen directive, which aims to reduce the risks to our data. We expect papers and printed media to be stored out of sight in cabinets or furniture when not in use, especially outside of working hours.

Personal data and confidential data must be locked when not required, especially when the office is vacated.

19. How should I protect my devices?

The COMPANY recognises there is a risk of unauthorised access to information and systems should computers remain unlocked. There is also a potential for sensitive data to be viewed if left on screen. Desktop computers, laptops and mobile devices must not be left logged on and unlocked when unattended; the device must be protected by locking or by logging off even for 1 minute.

When sending company confidential or personal information to a printer, a PIN code should be used to protect the printed copy from being viewed by unauthorised individuals.

If PIN functionality is not available, the user should take all practical precautions to avoid the printed copy from being viewed by unauthorised.

20. When and how should I report a security issue?

a. You should report any observed or suspected information security weaknesses, breaches, or contraventions of this policy as quickly as possible to IT support.

b. We ask that you report rather than try to fix, prove, or test a suspected security weakness as this could be interpreted as a potential misuse, cause damage or even destroy useful evidence.
c. All information security incidents or any breaches of this policy should be reported to IT Support or IT management These include, but are not limited to:
    i. The loss or theft of any company data, mobile device, computer, or hardware equipment.
    ii. The transfer or access of data by those who are not entitled to receive it.
    iii. Attempts to gain unauthorised access to company data or IT systems.
    iv. Changes to data or IT system hardware, firmware or software without the company's knowledge, instruction, or consent; and
    v. Unwanted disruption or denial of service to any company IT system.

d. Should evidence suggest that negligence has led to a breach of policy or where the reporting of such breaches has not been followed, action may be taken under the COMPANY Disciplinary Procedure.
e. The company reserves the right to monitor and investigate any activities when there is a perceived threat to company information, resources, business performance or suspicion of abuse, in line with our regulatory obligations

21. Trust your instincts

If something feels wrong or too good to be different, it probably is... We ask that you

a. Don't click or provide usernames/password
b. Report issues to IT Support
c. Send questions and ideas to the Group IT Director

22. Associated Policies

a. Hybrid Working
b. IT Security
c. Data Protection

23. Relevant Training (Click on link)

a. Microsoft Teams

b. Microsoft OneDrive (File sharing)

c. Health and Safety Working from Home

d. Cyber Security

Document Control	
Function Owner	IT
Policy Owner	Board
Policy Approval Route	Operating Board > Audit Committee > Board
Published date	
Version Number	1
Effective date	
Next review date	

Version History	
Key Changes	Effective Date
Initial launch	01/01/2023