IT Acceptable Use Policy

Table of Contents

[Background 3](#_Toc17190286)

[Purpose 3](#_Toc17190287)

[Definitions 3](#_Toc17190288)

[Acceptable Use Policy 4](#_Toc17190289)

[Physical Security 4](#_Toc17190290)

[Cyber Security 5](#_Toc17190291)

[Information Security 5](#_Toc17190292)

[Mobile Security 5](#_Toc17190293)

[Responsibilities 6](#_Toc17190294)

[Non-Compliance With This Policy 6](#_Toc17190295)

[Appendix A 7](#_Toc17190296)

[Appendix B 7](#_Toc17190297)

[IT Acceptable Use Assessment 11](#_Toc17190298)

# Background

**[Describe The Background Of Why An Acceptable Use Policy Has Come About.]**

The **[Business Name]** acknowledges the need to provide guidance to users of information technology (IT) systems on what is acceptable and what is not acceptable use of IT systems for **[Business Name]**.

Therefore, the **[Business Name]** is establishing this Acceptable Use Policy to support **[Business Name]** and describe the controls in place for monitoring and surveillance of personnel that **[Business Name]** may undertake on [Business Name] owned systems and equipment.

# Purpose

**[Describe What The Intent Of This Document Will Be.]**

This document sets forth the Acceptable Use for all **[Business Name] users**. It establishes the business rules and guidelines for consistency and compliance in demonstrating the acceptable use of information technology (IT) systems used within **[Business Name]**

# Definitions

**[Define Any Terms That Are Used Throughout This Document.]**

|  |  |
| --- | --- |
| Terms | Definition |
| IT Asset | **IT Asset** refers to anything (tangible or intangible) that has value to an organisation, including, but not limited to, a computing device, IT system, IT network, IT circuit, software (both an installed instance and a physical instance), virtual computing platform (common in cloud and virtualised computing), and related hardware (e.g., locks, cabinets, keyboards), as well as people and intellectual property (including software). |
| Confidential Information | Includes all information relating to **[Business Name]** or operational interests, methodology and affairs, trade secrets, financial information, internal hiring and training information including salaries and bonus programs, **[Business Name]** policies and procedures and any information marked as being confidential |
| Prohibited Use | Includes any unreasonable non-business use and, in particular, accessing, sending, viewing, downloading, storing or printing:* Offensive or illegal material, including but not limited to, items of pornography or any inappropriate materials that have the potential to offend another person or group of people. Examples of inappropriate material would include naked people or people involved in inappropriate acts that are likely to offend a reasonable person;
* Information with the potential to harass or cause harm to any other person; examples would include discriminatory or racist material in the form of jokes, pictures or photos etc.;
* Information whilst using an alias to use the internet or e-mail, including sending an anonymous message.;
* Confidential Information that the User is not authorised to use or access; an example would include payroll information or personal information in relation to another User if such access is not authorised.; and
* Using ICT Equipment or services to gain unauthorised access to computer systems or attempts to circumvent security controls or loopholes. This includes the creation and execution of software to discover security vulnerabilities and or loopholes
 |
| Reasonable Personal Use | Means non-business-related use such as:* Occasional short e-mail exchanges with family members or friends;
* Brief visits to non-business-related sites (e.g. news, shopping or social media) during work breaks;
 |
| **Portable Storage Devices** | Means portable or removable devices and media that are capable of storing data.Examples of Portable Storage Devices include USB memory sticks, SD Cards and USB hard drives |
|  |  |

# Acceptable Use Policy

**[Describe The Details Of The Policy.]**

All **[Business Name]** will be provided with the necessary IT equipment to perform their job role. The standards for equipment and services are set by **[Business Name]** and may change when appropriate.

**[Business Name]** will provide Portable Storage Devices if required. Non-**[Business Name]** Portable Storage Devices pose a risk to the business. Users must take all reasonable precautions to ensure that the use of Non-**[Business Name]** Portable Storage Devices does not compromise **[Business Name]** cyber security. The **[Business Name]** IT department can scan Portable Storage Devices for viruses, malware and other cyber security threats prior to the use of Non-**[Business Name]** Portable Storage Devices

## Physical Security

Users must take all reasonable precautions to protect the physical security of IT equipment issued to them.

Users must:

* Use any protective accessories (e.g. cases, covers and screen protectors) issued with equipment
* Avoid using public Wi-Fi hotspots to connect **[Business Name]** IT equipment in public spaces

Users must not:

* Leave equipment unattended in a public areas
* Leave equipment visible in an unattended parked vehicle
* Let equipment be used by anyone other than another **[Business Name]** employees
* Damage or misuse equipment
* Install unauthorised software programs on IT equipment issued to them without authorisation from the IT department.

## Cyber Security

Access to **[Business Name]** systems generally requires the use of a username (or e-mail address) and password. Users are encouraged to use a passphrase that is easy to remember but hard for an attacker to guess (Please see Appendix A for information on creating a passphrase)

Users must:

* Take all reasonable precautions to protect their username (or e-mail address) and password/passphrase from misuse
* Lock their computer before leaving it unattended
* Report any suspicious activity and cyber incidents

Users must not:

* Share, write down or otherwise disclose their password/passphrase
* Use their **[Business Name]** username or e-mail address for anything not business related
* Open attachments or click links in an e-mail message without checking to verify the source. (Please see Appendix B for information on checking to verify email source)

## Information Security

Users must:

* Take all reasonable precautions to protect the Confidential Information of **[Business Name]**
* Comply with all laws and regulations relating to intellectual property rights (including copyright, trade mark, design, patents, process or any other property capable of legal protection).

Users must not:

* Leave printouts or portable media containing private information on their desk and should be locked in a drawer to reduce the risk of unauthorised disclosure.
* Post any corporate or private or sensitive information, such as credit card numbers, passwords or other private information via email or on public sites, including social media sites.

## Mobile Security

Users must:

* Report loss or damage of a mobile device to the IT department as early as possible
* Enforce a passcode on their mobile device
* Lock their device when not in use
* Avoid using public Wi-Fi hotspots to connect mobile devices in public spaces

Users must not:

* Have conversations of a business confidential nature in public spaces
* Connect mobile devices to public Wi-Fi
* Leave their mobile device unattended

# Responsibilities

**[List Who Is Responsible For The Policy.]**

Users must respect the rights of other users, respect the integrity of the systems and related physical resources and observe all relevant laws, regulations and contractual obligations. It is the responsibility of the user to check information before transmission to ensure that it is not defamatory, libellous or misleading.

As the IT equipment and services are the property of **[Business Name], [Business Name]**may access, review, audit, intercept and copy any electronic data created, stored, transmitted, received or printed on its equipment or services at any time.

As system access is based on a username (or email-address), Users will be held accountable for any usage attributed to their own username (or e-mail address) unless all reasonable measures have been taken to prevent fraudulent use of their username (or e-mail address) including complying with this Policy.

Users must comply with the Policy Guidelines.

Users must comply with any reasonable requests by **[Business Name],** in relation to investigation into potential breaches of this Policy.

Users must successfully complete the *IT Acceptable Use Assessment*. Until they have done so they will not be provided with IT equipment or services.

# Non-Compliance With This Policy

**[Business Name]** acknowledges that inadvertent and unintended breaches of this policy may occur and encourages users to report policy breaches as soon as possible to their Supervisors or the IT Department.

Systematic and/or deliberate non-compliance with this Policy however may lead to disciplinary action, up to and including termination of employment (where the User is also an Employee).and may result in prosecution under applicable laws and users may be held accountable under any applicable law, policy, procedures, or workplace agreements

Supervisors are responsible for monitoring and acting upon compliance with this Policy.

Supervisors are responsible for ensuring that all Users complete the *IT Acceptable Use Assessment* and submit this to the IT Department for review and approval

Supervisors are responsible for disciplinary or other appropriate action where a User breaches this Policy.

# Appendix A

**Passphrases**

For many years’ humans have been taught to create complex passwords that have been increasingly difficult to remember, however computers have found it extremely easy to guess passwords by continually trying until they succeed. The speed in which a computer can try to guess a password can now take from milliseconds to hours to correctly guess which has forced us to either create longer and more complex passwords which are impossible to remember, or we need to try a different approach.

Instead of creating a long and complex password that is difficult to remember, the method which was put forth by security expert Bruce Schneier back in 2008 is to turn a sentence into your password.

The sentence should be personal and memorable to you as it is more likely that you will remember it rather than writing it down and storing it in an unsecure location.

Here are some examples of sentences that can be turned in to passwords and the approximate time it would take to guess these passphrases.

* I love to drink coffee (25 centuries to guess)
* The crows are the best team (174,871,509 centuries to guess)
* The power are the best team (4,600,217 centuries to guess)
* Bye bye miss american pie (89,706,509 centuries to guess)
* Lucy's birthday is in april (106,112 centuries to guess)

As you can see using a sentence is easier to remember but really difficult for a computer to guess. Try coming up with your own personal and memorable sentence and use it as your password it helps you and **[Business Name]** stay safe.

# Appendix B

**How To Spot A Phishing Email – (Adapted from 5 ways to detect a phishing email)**

Phishing is one of the most longstanding and dangerous methods of cyber crime. Despite what people think they know about phishing, they consistently fall victim. According to Verizon’s 2019 Data Breach Investigations Report, 32% of all cyber attacks involved phishing.

1. **The Message Is Sent From A Public Email Domain**

No legitimate organisation will contact you from an address that ends ‘@gmail.com’. Not even Google.

With the exception of independent workers, every organisation will have its own email domain and company accounts. For example, emails from Google will read ‘@google.com’.

If the domain name (the bit after the @ symbol) matches the apparent sender of the email, the message is probably legitimate. The best way to check an organisation’s domain name is to type the company’s name into a search engine. This makes detecting phishing seem easy, but cyber criminals have plenty of tricks up their sleeves to deceive you.

***Top tip: Look at the email address, not just the sender***

Many of us don’t ever look at the email address that a message has come from. Your inbox displays a name, like ‘IT Governance’, and the subject line. When you open the email, you already know (or think you know) who the message is from and jump straight into the content. When crooks create their bogus email addresses, they often have the choice to select the display name, which doesn’t have to relate to the email address at all.

They can therefore use a bogus email address that will turn up in your inbox with the display name Google. But criminals rarely depend on their victim’s ignorance alone. Their bogus email addresses will use the spoofed organisation’s name in the local part of the address.

Take this example of a phishing email mimicking PayPal:



This is a nearly flawless scam email. It uses PayPal’s logo at the top of the message, it is styled professionally, and the request is believable. But as much as it attempts to replicate a genuine email from PayPal, there’s one huge red flag: the sender’s address is ‘paypal@notice-access-273.com’.

A genuine email from PayPal would have the organisation’s name in the domain name, indicating that it had come from someone at (@) PayPal. That PayPal isn’t in the domain name is proof that this is a scam. Alas, simply including PayPal anywhere in the message is often enough to trick people. They might glance at the word PayPal in the email address and be satisfied, or simply not understand the difference between the domain name and the local part of an email address.

1. **It Includes Suspicious Attachments Or Links**

Phishing emails come in many forms, but the one thing they all have in common is that they contain a payload. This will either be an infected attachment that you’re asked to download or a link to a bogus website that requests login and other sensitive information.

**What is an infected attachment?**

An infected attachment is a seemingly benign document that contains malware. In a typical example, like the one below, the phisher claims to be sending an invoice:



It doesn’t matter whether the recipient expects to receive an invoice from this person or not, because in most cases they won’t be sure what the message pertains to until they open the attachment.

When they open the attachment, they’ll see that the invoice isn’t intended for them, but it will be too late. The document unleashes malware on the victim’s computer, which could perform any number of nefarious activities.

We advise that you never open an attachment unless you are fully confident that the message is from a legitimate party. Even then, you should look out for anything suspicious in the attachment. For example, if you receive a pop-up warning about the file’s legitimacy or the application asks you to adjust your settings, then don’t proceed.

Contact the sender through an alternative means of communication and ask them to verify that it’s legitimate.

**Suspicious links**

You can spot a suspicious link if the destination address doesn’t match the context of the rest of the email. For example, if you receive an email from Netflix, you would expect the link to direct you towards an address that begins ‘netflix.com’.

Unfortunately, many legitimate and scam emails hide the destination address in a button, so it’s not immediately obvious where the link goes to.



In this example, you would probably know that something was suspicious if you saw the destination address in the email. Unfortunately, the rest of the message is pretty convincing, and you might click the link without giving it a second thought.

To ensure you don’t fall for schemes like this, you must train yourself to check where links go before opening them. Thankfully, this is straightforward: on a computer, hover your mouse over the link and the destination address appears in a small bar along the bottom of the browser.

On a mobile device, hold down on the link and a pop-up will appear containing the link.

Source: Luke Irwin – 5 Ways To Spot A Phishing Email (<https://www.itgovernance.co.uk/blog/5-ways-to-detect-a-phishing-email>)

# IT Acceptable Use Assessment

**IT ACCEPTABLE USE ASSESSMENT**

User Name:

Department:

**Question 1 – IT Security**

Which of the following are Rights and Obligations under this policy?

|  |  |  |  |
| --- | --- | --- | --- |
| a) | The information stored on my computer belongs to me and the organisation can’t view, copy or delete it without my permission? | True | False |
| b) | All information stored on **[Business Name]** IT systems is and remains the property of **[Business Name]?** | True | False |
| c) | **[Business Name]** IT systems are provided primarily for business use? | True | False |
| d) | B and C? | True | False |

**Question 2 – IT Security**

|  |  |  |  |
| --- | --- | --- | --- |
| a) | It’s okay for me to share my password with someone I trust? | True | False |
| b) | I need to lock my computer when I leave it unattended? | True | False |
| c) | It’s okay for me to leave my laptop on the back seat of my car when I park in the street in front of my house? | True | False |
| d) | I need to let the IT department know as soon as I think there might be a virus on my computer? | True | False |
| e) | Non-compliance with this policymay lead to disciplinary action up to and including termination of employment? | True | False |

**Question 3 – Removable Devices**

|  |  |  |  |
| --- | --- | --- | --- |
| a) | If I am in a hurry to transfer a file that I need for work from my removable device, it is OK to plug it into my work computer first and then have the device scanned by the IT-Department? | True | False |
| b) | Serious breaches of the *Removable Device – Acceptable Use Policy* could result in termination of my employment? | True | False |
| c) | It is OK for me to lend a friend a USB stick that contains company sensitive information? | True | False |
| d) | It is OK for me to share inappropriate videos or content with my co-workers via a removable device as long as it has been scanned by the IT-Department? | True | False |
| e) | Before copying any company Confidential Information onto a USB stick I need approval to do so from my direct Supervisor or another appropriately authorised Manager? | True | False |
| f) | If I suspect that another Employee is in breach of this policy I should report the incident to my Manager? | True | False |

**Question 4 - Email and Internet Use**

|  |  |  |  |
| --- | --- | --- | --- |
| a) | All messages composed, sent, or received on the electronic mail system are and remain the property of **[Business Name]?** | True | False |
| b) | **[Business Name]** cannot access my e-mail or internet usage conducted on its equipment or systems because this information is my private property? | True | False |
| c) | I must not open attachments or click links in an e-mail message if I am unsure of the source? | True | False |
| d) | It is OK for me to sharing inappropriate videos or content with my co-workers via email? | True | False |

**Question 5 – Cyber Security**

|  |  |  |  |
| --- | --- | --- | --- |
| a) | It is OK for me to write down my password? | True | False |
| b) | It is OK for me to use someone else’s username and password as long as they have given me permission? | True | False |
| c) | I should not open attachments or click on links in e-mails unless I am sure of the source? | True | False |
| d) | It is OK for me to occasionally use news and social media sites during work breaks? | True | False |
| e) | It is OK for me to have a long e-mail conversation with a friend using **[Business Name]** email system? | True | False |
| f) | Is it OK for me to use e-mail or internet for non-business use? | True | False |

Employee Signature:

Date: / /

**ICT DEPARTMENT USE only**

The IT Department must confirm that the User has demonstrated an understanding of this Policy by answering the questions correctly.

Where a User has demonstrated this, the users Manager and IT must sign off below and a copy must be retained by the IT Department (and placed in the Employee’s personnel file where the User is also an Employee).

Where a User has not demonstrated the requisite understanding, the User must be directed to the area of the policy that they must review and complete the Understanding Assessment again.

Manager, Name:

Manager, IT Signature:

Date: / /