# Computer and Information Security Policy

## Purpose

* 1. The purpose of this Policy is to protect the data and information that [Company Name] stores and to mitigate the risk of unauthorised access to the information.

## Privacy Officer

* 1. The Privacy Officer for [Company Name] is [Privacy Officer’s Name].
	2. This Policy should be read in conjunction with the Privacy Act 2020.

## Scope

* 1. This Policy covers the security and use of all [Company Name]’s information and IT equipment. It also includes the use of email, internet, voice and mobile IT equipment.
	2. This Policy applies to all [Company Names]’s employees, contractors and agents (“Individuals”).
	3. This Policy applies to all information, in whatever form, relating to [Company Name]’s business activities, and to all information handled by [Company Name] relating to other people and organisations with whom we deal.

## Computer Access Control

* 1. Access to the [Company Name] IT systems is controlled by the use of User IDs and passwords. All User IDs and passwords are to be uniquely assigned to named Individuals and consequently, Individuals are accountable for all actions on the [Company Name]’s IT systems.
	2. Individuals must not:
		1. Allow anyone else to use their User ID and password on any [Company Name] IT system.
		2. Leave their user accounts logged in at an unattended and unlocked computer.
		3. Use someone else’s user ID and password to access [Company Name]’s IT systems.
		4. Leave their password unprotected (for example, writing it down).
		5. Perform any unauthorised changes to [Company Name]’s IT systems or information.
		6. Attempt to access data they are not authorised to use or access.
		7. Exceed the limits of their authorisation or specific business need to interrogate the system or data.
		8. Connect any non-[Company Name] authorised device to the [Company Name] network or systems.
		9. Store [Company Name] data on any non-authorised [Company Name] equipment.
		10. Give or transfer [Company Name] data or software to any person or organisation without the authority of [Company Name].
	3. Line managers must ensure that Individuals are given clear direction on the extent and limits of their authority with regard to IT systems and data.

## Internet and Email Conditions of Use

* 1. Use of [Company Name] internet and email is intended for business use.
	2. Personal use is permitted where such use:
		1. Does not affect the Individuals’ business performance.
		2. Is not detrimental to [Company Name] in any way.
		3. Is not in breach of any term or condition of employment.
		4. Does not place the Individual or [Company Name] in breach of statutory or other legal obligations.
	3. All Individuals are accountable for their actions on the internet and email systems.
	4. Individuals must not:
		1. Use the internet or email for the purposes of harassment or abuse.
		2. Use profanity, obscenities, or derogatory remarks in communications.
		3. Access, download, send or receive any data (including images), which [Company Name] considers offensive in any way, including sexually explicit, discriminatory, defamatory or libellous material.
		4. Use the internet or email to make personal gains or conduct a personal business.
		5. Use the internet or email to gamble.
		6. Use the email systems in a way that could affect its reliability or effectiveness, for example distributing chain letters or spam.
		7. Place any information on the Internet that relates to [Company Name], alter any information about it, or express any opinion about [Company Name], unless they are specifically authorised to do this.
		8. Send unprotected sensitive or confidential information externally.
		9. Forward [Company Name] mail to personal (non-[Company Name]) email accounts (for example a personal gmail account).
		10. Make official commitments through the internet or email on behalf of [Company Name] unless authorised to do so.
		11. Download copyrighted material such as music media (MP3) files, film and video files (not an exhaustive list) without appropriate approval.
		12. In any way infringe any copyright, database rights, trademarks or other intellectual property.
		13. Download any software from the internet without prior approval of the IT Department/Management.
		14. Connect [Company Name] devices to the internet using non-standard connections.

## Clear Desk and Clear Screen Policy

* 1. In order to reduce the risk of unauthorised use or loss of information, [Company Name] enforces a clear desk and screen policy as follows:
		1. Personal or confidential information must be protected using security features provided (for example, secure print on printers).
		2. Computers must be logged off/locked or protected with a screen locking mechanism controlled by a password when unattended.
		3. Care must be taken to not leave confidential material on printers or photocopiers.
		4. All business-related printed matter must be disposed of using confidential waste bins or shredders.

## Working Offsite

* 1. It is accepted that laptops and mobile devices will be taken offsite.
	2. The following controls must be applied:
		1. Working away from the office must be in line with [Company Name]’s remote working policy.
		2. Equipment and media taken offsite must not be left unattended in public places and not left in sight in a car.
		3. Laptops must be carried as hand luggage when travelling.
		4. Information should be protected against loss or compromise when working remotely (for example at home or in public places). Laptop encryption must be used.
		5. Particular care should be taken with the use of mobile devices such as laptops, mobile phones, smartphones and tablets. They must be protected at least by a password or a PIN and, where available, encryption.

## Mobile Storage Devices

* 1. Mobile devices such as memory sticks, CDs, DVDs and removable hard drives must be used only in situations when network connectivity is unavailable or there is no other secure method of transferring data.
	2. Only [Company Name] authorised mobile storage devices with encryption enabled must be used, when transferring sensitive or confidential data.

## Software

* 1. Employees must use only software that is authorised by [Company Name] on [Company Name] computers.
	2. Authorised software must be used in accordance with the software supplier's licensing agreements.
	3. All software on [Company Name] computers must be approved and installed by the [Company Name] IT department.
	4. Individuals must not:
		1. Store personal files such as music, video, photographs or games on [Company Name] IT equipment.

## Viruses

* 1. [Company Name] has implemented centralised, automated virus detection and virus software updates within [Company Name].
	2. All PCs have antivirus software installed to detect and remove any virus automatically.
	3. Individuals must not:
		1. Remove or disable anti-virus software.
		2. Attempt to remove virus-infected files or clean up an infection, other than by the use of approved [Company Name] anti-virus software and procedures.

## Telephony (Voice) Equipment Conditions of Use

* 1. Use of [Company Name] voice equipment is intended for business use.
	2. Individuals must not use [Company Name]’s voice facilities for sending or receiving private communications on personal matters, except in exceptional circumstances.
	3. All non-urgent personal communications should be made at an Individual’s own expense using alternative means of communications.
	4. Individuals must not:
		1. Use [Company Name]’s voice for conducting private business.
		2. Make hoax or threatening calls to internal or external destinations.
		3. Accept reverse charge calls from domestic or International operators, unless it is for business use.

## Actions upon Termination of Contract

* 1. All [Company Name] equipment and data, for example laptops and mobile devices including telephones, smartphones, USB memory devices and CDs/DVDs, must be returned to [Company Name] at termination of contract.
	2. All [Company Name] data or intellectual property developed or gained during the period of employment remains the property of [Company Name] and must not be retained beyond termination or reused for any other purpose.

## Monitoring and Filtering

* 1. All data that is created and stored on [Company Name] computers is the property of [Company Name] and there is no official provision for individual data privacy, however wherever possible [Company Name] will avoid opening personal emails.
	2. IT system logging will take place where appropriate, and investigations will be commenced where reasonable suspicion exists of a breach of this or any other policy.
	3. [Company Name] has the right (under certain conditions) to monitor activity on its systems, including internet and email use, in order to ensure systems security and effective operation, and to protect against misuse.

## Breaches

* It is your responsibility to report suspected breaches of security policy without delay to the Privacy Officer, your line management, the IT department, the information security department or the IT helpdesk.
* All breaches of information security policies will be investigated.
* Where investigations reveal misconduct, disciplinary action may follow in line with [Company Name] disciplinary procedures and the Employment Relations Act 2000.