**Software/Application Policy**

# Policy Statement

***<Company Name>*** will ensure the acceptable use of software by all users of the Council’s computer equipment or Information Systems.

# Purpose

The purpose of this document is to state the software policy of ***<Company Name>***. All existing ***<Company Name>*** policies apply to your conduct with regard to software, especially (but not limited to) the following [amend list as appropriate]:

* Email Policy.
* Internet Acceptable Usage Policy.
* IT Access Policy.
* Remote Working Policy.

# 

# Scope

This document applies to all the employees of the ***<Company Name>***, contractual third parties and agents of the organization who have access to Information Systems or information used for ***<Company Name>*** purposes.

# Definition

This policy should be applied at all times when the ***<Company Name>’*s** computer equipment or Information Systems are used.

# Risks

***<Company Name>*** recognizes that there are risks associated with users accessing and handling information in order to conduct business. This policy aims to mitigate the following risks:

* [List appropriate risks relevant to the policy – e.g. the non-reporting of information security incidents, inadequate destruction of data, the loss of direct control of user access to information systems and facilities etc.].

Non-compliance with this policy could have a significant effect on the efficient operation of the Council and may result in financial loss and an inability to provide necessary services to our customers**.**

# 

# Applying the Policy

## Software Acquisition

All software acquired by ***<Company Name>*** must be purchased through the [Name a department – e.g. Procurement Department]. Software may not be purchased through user corporate credit cards, petty cash, and travel or entertainment budgets. Software acquisition channels are restricted to ensure that ***<Company Name>*** has a complete record of all software that has been purchased for ***<Company Name>’s*** computers and can register, support, and upgrade such software accordingly. This includes software that may be downloaded and/or purchased from the Internet.

Under no circumstances should personal or unsolicited software (this includes screen savers, games and wallpapers etc.) be loaded onto a ***<Company Name>*** machine as there is a serious risk of introducing a virus.

## Software Registration

The ***<Company Name>*** uses software in all aspects of its business to support the work carried out by its employees. In all instances, every piece of software is required to have a license and the Council will not condone the use of any software that does not have a license. Software must be registered in the name of ***<Company Name>*** and the department in which it will be used. Due to personnel turnover, software will never be registered in the name of the individual user. The [Name a department – e.g. IT Helpdesk] maintains a register of all ***<Company Name>*** software and will keep a library of software licenses. The register must contain:

1. The title and publisher of the software.
2. The date and source of the software acquisition.
3. The location of each installation as well as the serial number of the hardware on which each copy of the software is installed.
4. The existence and location of back-up copies.
5. The software product's serial number.
6. Details and duration of support arrangements for software upgrades.

Software on Local Area Networks or multiple machines shall only be used in accordance with the license agreement.

***<Company Name>*** holds licenses for the use of a variety of software products on all Council Information Systems and computer equipment. This software is owned by the software company and the copying of such software is an offence under the Copyright, Designs and Patents Act 1988, unless authorized by the software manufacturer.

It is the responsibility of users to ensure that all the software on their computer equipment is licensed.

## 

## Software Installation

Software must only be installed by the [Name a department – e.g. IT Helpdesk] once the registration requirements have been met. Once installed, the original media will be [insert council storage procedure here – e.g. kept in a safe storage area maintained by the IT Helpdesk]. Software may not be used unless approved by the [Name a role – e.g. Head of Department], or their nominated representative. Shareware, Freeware and Public Domain Software are bound by the same policies and procedures as all other software. No user may install any free or evaluation software onto the ***<Company Name>’s*** systems without prior approval from Information Services [or equivalent department].

## Software Development

All software, systems and data development for the organization is to be used only for the ***<Company Name>*** purpose.

Software must not be changed or altered by any user unless there is a clear business need. All changes to software should be authorized before the change is implemented. A full procedure should be in place and should include, but not be limited to, the following steps [amend as appropriate or replace with your own procedure]:

1. The software asset’s owner should approve change requests affecting a software asset.
2. All change requests should consider whether the change is likely to affect existing security arrangements and these should then be approved.
3. A record should be maintained of agreed authorization levels.
4. A record should also be maintained of all changes made to software.
5. Changes to software that have to be made before the authorization can be granted should be controlled.

## Personal Computer Equipment

***<Company Name>*** computers are organization’s-owned assets and must be kept both software legal and virus free. Only software acquired through the procedures outlined above may be used on ***<Company Name>*** machines. Users are not permitted to bring software from home (or any other external source) and load it onto ***<Company Name>*** computers. Generally, organization-owned software cannot be taken home and loaded on a user's home computer if it also resides on a ***<Company Name>’s*** computer. If a user needs to use software at home, [insert organization procedure here – e.g. purchase a separate package and record it as a an organization-owned asset in the software register].

## Software Misuse

***<Company Name>*** will ensure that Personal Firewalls are installed where appropriate. Users **must not** attempt to disable or reconfigure the Personal Firewall software. It is the responsibility of employees to report any known software misuse to the appropriate personnel[Name a role – e.g. Head of Department].

According to the Copyright, Designs and Patents Act 1988, illegal reproduction of software is subject to civil damages and criminal penalties. Any ***<Company Name>***’**s** user who makes, acquires, or uses unauthorized copies of software will be disciplined as appropriate under the circumstances. ***<Company Name>*** does not condone the illegal duplication of software and will not tolerate it.

# Policy Compliance

If any user is found to have breached this policy, they may be subject to ***<Company Name>’s*** disciplinary procedure. If a criminal offence is considered to have been committed further action may be taken to assist in the prosecution of the offender(s).

If you do not understand the implications of this policy or how it may apply to you, seek advice from [name appropriate department].

# Policy Governance

The following table identifies who within ***<Company Name>*** is Accountable, Responsible, Informed or Consulted with regards to this policy. The following definitions apply:

* **Responsible** – the person(s) responsible for developing and implementing the policy.
* **Accountable** – the person who has ultimate accountability and authority for the policy.
* **Consulted** – the person(s) or groups to be consulted prior to final policy implementation or amendment.
* **Informed** – the person(s) or groups to be informed after policy implementation or amendment.

# 

# Review and Revision

This policy will be reviewed as it is deemed appropriate, but no less frequently than every 12 months. Policy review will be undertaken by [Name an appropriate role].

# Key Messages

* All software acquired must be purchased through the [Name a department – e.g. Procurement Department].
* Under no circumstances should personal or unsolicited software be loaded onto a Council machine.
* Every piece of software is required to have a licence and the Council will not condone the use of any software that does not have a licence.
* Unauthorised changes to software **must not** be made.
* Users are not permitted to bring software from home (or any other external source) and load it onto Council computers.
* Users **must not** attempt to disable or reconfigure the Personal Firewall software.
* Illegal reproduction of software is subject to civil damages and criminal penalties.