KINETIKA
DESIGN THAT MOVES

119 Artist Studios
High House Production Park
Purfleet-on-Thames
Essex RM19 1AS

01708 202844
info@kinetika.co.uk
www.kinetika.co.uk

IT Acceptable Use Policy

Updated July 2025
Next review due September 2026

1. Introduction

This IT Acceptable Usage Policy covers the security and use of all Kinetika's information and IT equipment. It also includes the use of email, internet, voice and mobile IT equipment. This policy applies to all Kinetika's freelancers and contractors (referred to as 'individuals').

This policy applies to all information, in whatever form, relating to Kinetika's business activities worldwide, and to all information handled by Kinetika relating to other organisations with whom it deals. It also covers all IT and information communications facilities operated by Kinetika or on its behalf.

2. Access Control – Individual's Responsibility

Access to the Kinetika IT systems is controlled by User IDs and passwords. All User IDs and passwords are uniquely assigned to named individuals and consequently, individuals are accountable for all actions on Kinetika's IT systems. It if your responsibility to ensure strong, unique passwords are in place and are updated on a regular basis. Best practice suggests passwords are a minimum of 8 characters long with mix of upper and lower, numerical and another symbols.

Individuals must not:

- Allow anyone else to use their user ID and password on any Kinetika IT system.
- Leave their user accounts logged in at an unattended and unlocked computer.
- Use someone else's user ID and password to access Kinetika's IT systems.
- Leave their password unprotected (for example writing it down).
- Perform any unauthorised changes to Kinetika's IT systems or information.
- Attempt to access data that they are not authorised to use or access.
- Exceed the limits of their authorisation or specific business need to interrogate the system or data.
- Connect any non-Kinetika authorised device to the Kinetika network or IT systems.
- Store Kinetika data on any personal equipment.
- Give or transfer Kinetika data or software to any person or organisation outside Kinetika without the authority of Kinetika.

The Operations Director will give direction on the extent and limits regarding IT systems and data.

ARTS COUNCIL ENGLAND
Supported using public funding by
ARTS COUNCIL ENGLAND

3. Devices

As all freelancers and contractors at Kinetika use their own equipment, it is the individual's responsibility to ensure any device accessing Kinetika files and systems are secure. This includes laptops, personal devices and mobile phones which can access email or files.

Care should be taken to ensure devices are encrypted, that password/PIN protection is in place, security updates are regularly applied, and that unnecessary software is disabled or removed on personal devices

It is an expectation that all equipment will have antivirus software installed to detect and remove any virus automatically. Kinetika has anti-virus licences available for use. If you require this, please speak to the Operations Director in the first instance.

There are several threats to ICT systems that can result in the damage of equipment, loss of computer-based information or the disclosure of information to unauthorised third parties. These threats can influence the continuity of our Organisation or cause us to fail in our duties under the Data Protection Act. Please see Appendix A for more detailed breakdown on the potential threats.

4. File Storage

The File Storage Guide documents the primary method of file storage which is Microsoft Sharepoint. At no point should files be saved locally onto individuals own computers or onto other cloud storage systems, as these files remain the property of Kinetika.

Individuals must not:

- Store files on their personal computers
- Store files onto other online cloud systems such as Dropbox and Google Drive without express permission

5. Storage Devices

Storage 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. Only Kinetika authorised mobile storage devices with encryption enabled must be used, when transferring sensitive or confidential data.

6. Clean Desk and Clear Screen Policy

To reduce the risk of unauthorised access or loss of information, Kinetika expects a clear desk and screen policy as follows:

- To protect sensitive information, all confidential materials are to be removed from a workspace and locked away when the items are not in use or an individual leaves their workstation.
- Filing cabinets containing restricted or sensitive information must be kept closed and locked when not in use or when not attended.
- Keys used to access restricted or sensitive information must not be left at an unattended desk.
- Computers must be logged off/locked or protected with a screen locking mechanism controlled by a password when unattended.

- Care must be taken to not leave confidential material on printers or photocopiers.
- All business-related printed matter must be disposed of using confidential waste bins or shredders.

7. Working Off-site

It is accepted that devices will largely reside off-site and we ask that the following controls be applied:

- Equipment and media must not be left unattended in public places and not left in sight in a car.
- Laptops must be carried as hand luggage when travelling.
- Care should be taken in public places to protect against loss or compromise of information.
- Ensure your wi-fi connection is secure, using a VPN if needed.

8. General Data Protection Regulation (GDPR)

We expect all members of the core Kinetika team to undertake data protection training.

Kinetika provide an online course to give a complete foundation on the principles, roles, responsibilities and processes under the Regulation, which is followed by a short test. The test can be retaken multiple times until you pass, ensuring a clear understanding of the Regulation and the organisation's compliance obligations.

If you have recently undertaken similar training for another organisation, please provide a copy of this. If you require access to the training module, please ask the Operations Director to setup your username and password.

9. Internet and email Conditions of Use

Use of Kinetika internet and email is intended for business use. Personal use is permitted where such use does not affect the individual's business performance, is not detrimental to Kinetika in any way, not in breach of any term and condition of engagement and does not place the individual or Kinetika in breach of statutory or other legal obligations.

All individuals are accountable for their actions on the internet and email systems.

Individuals must not:

- Use the internet or email for the purposes of harassment or abuse.
- Use profanity, obscenities, or derogatory remarks in communications.
- Access, download, send or receive any data (including images), which Kinetika considers offensive in any way, including sexually explicit, discriminatory, defamatory or libellous material.
- Use the internet or email to make personal gains or conduct a personal business.
- Use the internet or email to gamble.
- Use the email systems in a way that could affect its reliability or effectiveness, for example distributing chain letters or spam.
- Place any information on the Internet that relates to Kinetika, alter any information about it, or express any opinion about Kinetika, unless they are specifically authorised to do this.
- Send unprotected sensitive or confidential information externally.
- Forward Kinetika mail to personal email accounts (for example a personal Hotmail account).

- Make official commitments through the internet or email on behalf of Kinetika unless authorised to do so.
- Download copyrighted material such as music media (MP3) files, film and video files (not an exhaustive list) without appropriate approval.
- In any way infringe any copyright, database rights, trademarks or other intellectual property.
- Download any software from the internet without prior approval of the IT Management Company.
- Connect Kinetika devices to the internet using non-standard connections.

10. Telephony (Voice) Equipment Conditions of Use

Use of Kinetika voice equipment is intended for business use. Individuals must not use Kinetika's voice facilities for sending or receiving private communications on personal matters, except in exceptional circumstances. All non-urgent personal communications should be made at an individual's own expense using alternative means of communications

Individuals must not:

- Use Kinetika's voice for conducting private business.
- Make hoax or threatening calls to internal or external destinations.

Accept reverse charge calls from domestic or International operators, unless it is for business use.

11. Monitoring and Filtering

All data that is created and stored on behalf of Kinetika is the property of Kinetika.

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. Kinetika has the right (under certain conditions) to monitor activity on its systems, including internet and email use, to ensure systems security and effective operation, and to protect against misuse. Any monitoring will be carried out in accordance with audited, controlled internal processes, under current legislation.

All breaches of information security policies will be investigated. Where investigations reveal misconduct, disciplinary action may follow in line with Kinetika disciplinary procedures.

12. Actions upon Termination of Contract

All Kinetika equipment and data, for example laptops and mobile devices including telephones, smartphones, USB memory devices and CDs/DVDs, must be returned to Kinetika at termination of contract.

All Kinetika data or intellectual property developed or gained during the period of employment remains the property of Kinetika and must not be retained beyond termination or reused for any other purpose.

13. Incident Reporting

IT security breaches, phishing attempts, or data loss should be immediately reported to **Agile Computers | 01494 452000** | **service@agilecomputers.co.uk**.

Appendix A - Protection against ICT Threats

There are several threats to ICT systems that can result in the damage of equipment, loss of computer-based information or the disclosure of information to unauthorised third parties. These threats can influence the continuity of our Organisation or cause us to fail in our duties under the Data Protection Act.

The major threats include:

· Virus infection.

Viruses are software programs written with the express intent of bypassing Computer Security. Virus software can delete files, make it impossible for the PC to connect to the Internet or even cause physical damage to the equipment. They can be written as a separate program or as instructions to other software such as Microsoft Word or Excel. Anti-virus software can search for known types of virus and (if kept up to date) can offer protection against this threat.

· 'Break-in' over the internet

When a computer is connected to the Internet it may be possible for another computer to access information on the connected PC. This is generally known as 'hacking' and may involve cracking passwords or bypassing security systems on the PC. Firewall Software can protect this threat. It is also important that, where possible, the operation system and office software are updated with any available 'security patches' from the manufacturer and that password protection is being used effectively.

· Software with unknown functions

Some software has 'unadvertised features' which can (for example) collect information from a PC and send it over the Internet. This type of program is sometimes known as a 'Trojan Horse'. Whilst often used to collect marketing information they can be designed for more sinister purposes, such as recording all keystrokes from a keyboard to identify passwords and bank account details. Whilst Anti-Virus and Firewall software can assist, it is also important only to buy trusted software from reputable sources.

· Attachments to email

Virus and other rogue software can be attached to email messages and often seek to bypass security by persuading the user to 'unzip' or open a file or to run a piece of software. To achieve this, they have to build up user confidence in the authenticity of the instruction to open or run the dangerous attachment. This is often achieved by the virus attaching itself to a message from a known party, or by falsely identifying a message as being from a trusted source such as a Bank or an Anti-Virus company. Anti-Virus software helps, but the policies below also seek to minimise the risks.

· Hoax Warnings

Tricksters sometimes try to persuade users to undertake actions that will cause later problems. An example would be suggesting that a file has a virus and should be deleted when, in fact, that file is essential to Microsoft Windows. Policies and staff training offer protection against this type of hoax.

In view of the above individuals are expected to:

1. Maintain up-to-date Virus software on all PCs
2. Ensure that security patches to PC and Apple Operating Systems are kept up to date on all machines that are connected to the internal network in the building. If the machine no longer received updates due to the Manufacturer (Microsoft or Apple) no longer supplying them it should not be connected to the internal network at all.
3. Refrain from unsuitable use of computer equipment and to protect the organisation against virus and other threats