







ICT Acceptable Use Policy (AUP)

Policy Number	I.4	**Review Cycle**	**3 year**	**Reviewer**
Date Created	01/07/2009	**Review Date(s)**	01/07/2015	Operations Lead
Original Author	Operations Lead/ CEO		01/07/2018	Admin and Finance Lead / CEO
			01/07/2021	Admin and Finance Lead / CEO
			01/07/2024	
			01/07/2027	

ACCEPTABLE USE POLICY FOR ICT SYSTEMS

1. Introduction

This Acceptable Use Policy (AUP) for IT Systems is designed to protect APTCOO, our employees, customers and other partners from harm caused by the misuse of our IT systems and our data.

Everyone who works at APTCOO is responsible for the security of our IT systems and the data on them. As such, all employees must ensure they adhere to the guidelines in this policy at all times. Should any employee be unclear on the policy or how it impacts their role they should speak to their manager.

2. Definitions

“Users” are everyone who has access to any of APTCOO’s IT systems. This includes permanent employees and also temporary employees, contractors, agencies, consultants, suppliers, learners, service users, customers and business partners.

“Systems” means all IT equipment that connects to the corporate network or access corporate applications. This includes, desktop computers, laptops, smartphones, tablets, printers, data and voice networks, networked devices, software, electronically-stored data, portable data storage devices, third party networking services, telephone handsets, video conferencing systems, and all other similar items commonly understood to be covered by this term.

3. Use of IT Systems

All data stored on APTCOO’s systems is the property of APTCOO. Users should be aware that the company cannot guarantee the confidentiality of information stored on any APTCOO system except where required to do so by local laws.

APTCOO’s systems exist to support and enable the business. A small amount of personal use is, in most cases, allowed. However it must not be in any way detrimental to users own or their colleagues productivity and nor should it result in any direct costs being borne by APTCOO other than for trivial amounts. APTCOO trusts employees to be fair and sensible when judging what constitutes an acceptable level of personal use of the company’s IT systems. If employees are uncertain they should consult their manager.

Any information that is particularly sensitive or vulnerable must be encrypted and/or securely stored so that unauthorised access is prevented. However this must be done in a way that does not prevent or risk preventing access to authorized parties. APTCOO can monitor the use of its IT systems and the data on it at any time. This may include (except where precluded by local privacy laws) examination of the content stored within the email and data files of any user, and examination of the access history of any users. APTCOO reserves the right to regularly audit networks and systems to ensure compliance with this policy.

4. Data Security

If data on APTCOO's systems is classified as confidential this should be clearly indicated within the data and/or the user interface of the system used to access it. Users must take all necessary steps to prevent unauthorised access to confidential information.

Users are expected to exercise reasonable personal judgement when deciding which information is confidential.

Users must not send, upload, remove on portable media or otherwise transfer to a non APTCOO system any information that is designated as confidential, or that they should reasonably regard as being confidential to APTCOO, except where explicitly authorised to do so in the performance of their regular duties.

Users must keep passwords secure and not allow others to access their accounts. Users must ensure all passwords comply with APTCOO's safe password policy.

Users who are supplied with computer equipment by APTCOO are responsible for the safety and care of that equipment, and the security of software and data stored it and on other APTCOO systems that they can access remotely using it.

Because information on portable devices, such as laptops, tablets and smartphones, is especially vulnerable, special care should be exercised with these devices: sensitive information should be stored in encrypted folders only. Users will be held responsible for the consequences of theft of or disclosure of information on portable systems entrusted to their care if they have not taken reasonable precautions to secure it.

Staff must not to use their own personal equipment during contracted working hours, nor should personal equipment be brought onto APTCOO premises. Should there be a need for a member of staff to bring their personal equipment onto site, this should be with express permission of their line manager.

All workstations (desktops and laptops) should be secured with a lock-on-idle policy active after at most 10 minutes of inactivity. In addition, the screen and keyboard should be manually locked by the responsible user whenever leaving the machine unattended.

Users must at all times guard against the risk of malware (e.g., viruses, spyware, Trojan horses, rootkits, worms, backdoors) being imported into APTCOO's systems by whatever means and must report any actual or suspected malware infection immediately.

5. Unacceptable Use

All employees should use their own judgment regarding what is unacceptable use of APTCOO's systems. The activities below are provided as examples of unacceptable use. Should an employee need to contravene these guidelines in order to perform their role, they should consult with and obtain approval from their manager before proceeding.

- All activities detrimental to the success of APTCOO. These include sharing sensitive information outside the company, such as research and development information and customer lists, as well as defamation of the company.

- All activities for personal benefit only that have a negative impact on the day-to-day functioning of the business (e.g. streaming video, playing networked video games and using social media including Facebook and Twitter).

- All activities that are inappropriate for APTCOO to be associated with and/or are detrimental to the company's reputation. This includes gambling, bullying and harassment.

- Circumventing the IT security systems and protocols which APTCOO has put in place.

6. Enforcement

APTCOO will not tolerate any misuse of its systems and will discipline anyone found to have contravened the policy, including not exercising reasonable judgment regarding acceptable use. Each situation will be judged on a case-by-case basis.

Appendix 1

Distribution/ Access: All Staff

RECORD OF CHANGES

DATE	AUTHOR	PROCEDURE	DETAILS OF CHANGE
3rd July 2017	MG	Additional information added	'Learners' and 'Service Users' added to paragraph 2 – Definitions under 'Users'.
3rd July 2017	MG	Additional information added	Paragraph 5 – 'Data Security' – additional paragraph providing clarity on the use and access of personal IT equipment.

Appendix 2

EMPLOYEE RECORD OF HAVING READ THE POLICY

Title of Policy: ICT – Acceptable Use Policy (AUP)

I have read and understand the principles contained in the named policy.

PRINT FULL NAME	SIGNATURE	DATE