Acceptable Use of IT Systems and Assets Policy

The purpose of this Acceptable Use of IT Systems and Assets Policy is to define the guidelines and rules for the acceptable use of information and assets within our organisation. It ensures that all employees, temporary staff, contractors, and applicable third parties understand their responsibilities when accessing and utilising information assets.

Acceptable Use of Information Assets:

- Users must comply with all applicable laws, regulations, and organisational policies when accessing or using information assets.
- Information assets should be used for legitimate business purposes only and not for personal gain or unauthorised activities.
- Users must respect intellectual property rights, including copyrights, trademarks, and patents, when using information assets.
- Confidential and sensitive information should be handled with the utmost care, following specific access restrictions.
- Notice of any attempted breaches or concerns should be promptly communicated to the IT Manager - Commuserv.

Acceptable Use of Assets:

- Users must utilise organisational assets, including hardware, software, and network resources, responsibly and for authorised purposes only.
- Assets should not be misused, modified, or shared without proper authorization.
- Users are responsible for the secure handling and protection of assets against loss, theft, or damage.
- Users should not attempt to install unauthorised software, introduce malware, or engage in any activities that compromise the integrity of the assets or network.

Training and Awareness:

- All relevant parties will have access to the documented acceptable use rules.
- Cyber Aware in place to provide ongoing training and awareness for users.

Teleworking:

- When Teleworking, users must ensure the same level of compliance, regulations, and policies/ procedures as they would while on-site.
- Users are responsible for maintaining the security and confidentiality of information assets when accessing them remotely.
- Users should adhere to secure network connections, use approved devices, and follow any additional guidelines or procedures specified for remote work.
- Users must complete a Teleworking Checklist if working from home / on site.

Consequences of Violation:

- Violations of this Acceptable Use Policy may result in disciplinary action, including but not limited to verbal or written warnings, temporary or permanent suspension of system access, termination of employment, and legal actions if necessary.

Review and Revision:
This policy will be periodically reviewed and updated as needed to reflect changes in technology, regulations, or business requirements. Users will be notified of any revisions and will be required to reconfirm their adherence to the policy.

Jim Cunningham
Managing Director

David Stephen
Managing Director