POLICY

COMPUTING AND COMMUNICATION ACCEPTABLE USE POLICY

Pumps United Computing and Communication Acceptable Use Policy aims to protect the integrity of our information system's assets by outlining the expected acceptable use. This policy applies to all of Pumps United's employees, contractors and other workers (employees) who require or have access to our information systems and internet (the Network) in order to perform their role.

Employees that access the Network via resources provided by Pumps United must demonstrate sound judgement whilst using the network, in particular but not limited to:

- Limiting personal use when accessing the internet and email facilities to ≤5% only.
- Personal use must not interfere with the Pumps United's security or work priorities.
- Information disseminated, received or accessed remains the property of and controlled by Pumps United at all times.
- The storage of any of Pumps United's information on personal or non-Pumps United devices, including laptops, and storage devices is prohibited.
- Ensure the protection of assigned assets including, but not limited to, desktops, laptops, monitors, dumb terminals, tablets and telephones.
- The use of applications and Network resources is only permitted to authorised employees.
- Download and / or installation of software must be authorised and installed by Management or employees under their direction.
- Requirements for after hour's access to the Network must be authorised by Management.
- Employees must maintain password security and ensure confidentiality.
- Screens should be locked when employees are away from their desk for extended periods of time to avoid unauthorised access to the Network or sensitive documents.
- Protection of data and the privacy of personal information stored on Network devices.

Pumps United employees must not use the Network:

- For any unlawful or prohibited purposes.
- To provide access to others either deliberately, or through failure to secure access to the Network devices, for example, through failure to lock their device when away from their desk.

The Group does not permit inappropriate use of the Network and associated devices, including:

- Procuring or transmitting material that goes against the Group's policies and philosophies, e.g. pornographic material.
- Transmittal of spam via email, SMS / MMS or voice mail.
- Use of the Group's email and / or IP address to engage in conduct that is disrespectful or goes against the Group's policies and philosophies, e.g. bullying and harassment.
- Conducting non-Group business on the Group's resources.
- Conducting or supporting illegal actions that could compromise the reputation and integrity of the Group.
- Monitoring of email content and server usage may be conducted as deemed appropriate by the Executive Management.

Pumps United's Senior Management Team is responsible for the effectiveness of our management systems, encompassing all professional services undertaken for our clients.

Chief Executive Officer
Pumps United Pty Ltd
01/09/2017