IT Acceptable Use Policy

1. Purpose

The purpose of this policy is to protect Glad Group's interests, assets and reputation. It aims to prevent misuse, unauthorised access and other behaviours that could compromise Glad Group's information and information systems. It outlines the appropriate usage in an effective, safe, ethical and lawful manner.

2. Scope

The IT Acceptable Use policy applies to all Glad Group entities as outlined below:

- **Glad Group Pty Ltd** | ABN 62 092 928 115
- Glad Security Pty Ltd trading as **Glad Group Services** | ABN 99 122 097 590
- **Glad Maintenance Pty Ltd** | ABN 85 127 522 481
- **Auxus Pty Ltd** | 12 655 147 292
- Stratium Global Pty Ltd trading as **Unifyd Technology** | 55 627 094 366
- **Australian Protective Services Pty Ltd** | 47 610 471 424

This policy applies to all employees, consultants, contractors and outsourced service providers (users) performing work for and behalf of Glad Group.

3. Policy Statement

This policy has been developed in alignment with the following:

- Glad Group's statutory and organisational responsibility to ensure confidentiality, integrity and availability of Glad Group information and information systems
- Compliance with the Workplace Surveillance Act 2005, Privacy Act 1988, the Notifiable Data Breaches Scheme and The Australian Privacy Principles
- Reduction of cyber security threats and risk of legal action related to technology use

Use of Glad Group information and information system assets must be ethical, efficient, lawful, economic and aligned with Glad Group's Code of Conduct and other relevant policies and procedures. All users that are in possession of or have access to Glad Group information or information system assets must take all reasonable steps to protect those assets against loss, damage or destruction. This relates to physical and electronic files, documents and records, as well as equipment.

Users have a direct responsibility for maintaining a reasonable level of security when working at any location, considering the circumstances and potential risks of working outside Glad Group's premises including customer locations.

3.1. Coverage

Information and information systems cover computing, collaboration and communications facilities, including telephones, facsimiles, mobile devices, computers, laptops, tablets, printers, photocopiers, email, internet access, network applications, web services and similar resources. Information and information systems encompass facilities, technology, application systems and data.

It applies to all information and information system assets owned, leased or outsourced by Glad Group at all its business locations, customers sites and private residences, regardless of format or storage device and whether shared or allocated to individuals.

3.2. Usage

Acceptable use of Glad Group information systems includes work performed for business purposes in an efficient, economical, lawful and ethical manner. The most common security problems and breaches related to access and use are:

- Forgotten, guessed, shared or misused passwords

© COPYRIGHT GLAD GROUP (ALL RIGHTS RESERVED)

- Information not stored securely
- Unauthorised changes being made to computers or the network
- Installing unauthorised equipment or software
- Use of systems for unreasonable private purposes

Users are responsible for the following when using Glad Group Information Systems:

- All activities that originate from their account
- All information sent from, requested, solicited or viewed from their account
- Information placed on a computer using their account

Users must not use the Information Systems and Services for the following activities:

- The creation or transmission of any material or data that could reasonably be deemed abusive, offensive, defamatory, obscene or indecent
- The creation or transmission of material that could reasonably be deemed likely to harass, intimidate, harm or distress
- The unauthorised transmission of material that is labelled confidential or commercial in confidence
- Deliberate unauthorised access to facilities or services

3.3. User Access

To enable user access to information and information systems the following must occur:

- The user's Manager and/or Senior Management must lodge a request for user access to the IT department on support@gladgroup.com.au or via the IT Request Form within Glad Academy where applicable
- Managers must ensure access is provided on the principle of least possible privilege and need to know basis
- Managers must notify the IT department to remove staff access upon departure from Glad Group

3.4. Password Management

- Users must ensure passwords are complex enough to ensure they cannot be guessed easily or misused
- Users must never share their account and password with anyone, including but not limited to colleagues, managers, customers, support staff, family members or friends.
- Users are accountable for all activities performed within their accounts

3.5. Email

Emails created in the course of employment are business records of Glad Group and may be monitored and audited by appropriately authorised Glad Group personnel.

- Email content must not be detrimental to, nor adversely affect, the reputation or operations of Glad Group, its employees or customers.
- Users are responsible and accountable for their use of email and for the format and content of email sent by them.
- Unsolicited, discouraged emails and emails that are in breach of Glad Group's Code of Conduct must not be forwarded and must be deleted. Reasonable steps must be taken to prevent a re-occurrence.

3.6. Internet

© COPYRIGHT GLAD GROUP (ALL RIGHTS RESERVED)

Glad Group provides information systems for business purposes. Unnecessary or unauthorised internet usage can severely compromise Glad Group.

- Internet usage must be used primarily for business purposes
- Glad Group reserves the right to monitor and record internet usage and web browsing activity of all its technology, including computers, laptops, tablets and mobile devices
- Internet usage must not be detrimental to, nor adversely affect, the reputation and operations of Glad Group, its employees or customers.

3.7. Communication and Collaboration Platforms

Communication and collaboration platforms include, but are not limited to, instant messaging, SMS and MMS, Microsoft Teams, chat functions, social media platforms, web-based applications and any other electronic method used to communicate, share information or conduct Glad Group business, whether accessed through Glad Group equipment or personal devices.

These platforms form part of Glad Group's Information Systems where they are used for work-related purposes and must be used in an efficient, lawful, ethical and secure manner and in accordance with Glad Group's policies and procedures.

Users are responsible for the following when using communication and collaboration platforms for Glad Group business:

- Ensuring that all communications are professional, appropriate and consistent with the Glad Group Code of Conduct
- Only sharing Glad Group information with authorised persons and through approved channels
- Taking reasonable steps to protect confidential and commercially sensitive information
- Ensuring that records relating to Glad Group business are retained in approved Glad Group systems where required

Users must not:

- Use personal messaging, social media or other non-approved platforms to store or transmit Glad Group confidential or commercially sensitive information without authorisation
- Create, send or forward content that is offensive, discriminatory, defamatory, misleading, threatening or otherwise in breach of Glad Group policies or any applicable law
- Establish unofficial work-related communication groups or distribution lists that bypass approved Glad Group systems or governance requirements
- Delete, alter or remove any communication or record that may be required for an investigation, legal proceedings, audit or business record without authorisation

Where personal devices are used to access or conduct Glad Group business, users must ensure that Glad Group information is appropriately protected and must comply with any security, access and monitoring requirements.

All work-related communications created, sent or received using these platforms in the course of employment or engagement with Glad Group are considered Glad Group business records and may be accessed, monitored and retained in accordance with this policy and applicable legislation.

3.8. Reasonable Private Use

Reasonable private use is permitted provided it is infrequent, brief and does not intrude on work time, impact service delivery, incur costs, or create an exposure for Glad Group to viruses, legal liability, or embarrassment.

3.9. What Access or Use is Not Acceptable

© COPYRIGHT GLAD GROUP (ALL RIGHTS RESERVED)

It is prohibited to create, send, access or store information that:

- Could damage the reputation of Glad Group
- Involves or could lead to unlawful victimisation, discrimination, harassment or vilification
- Is sexually suggestive, offensive, obscene, threatening, abusive or defamatory
- Is used for operating a private business unrelated to Glad Group
- Is deliberately misleading or deceptive
- Is encrypted without the approval of your manager and IT Department and does not comply with Glad Group encryption standard
- Violates any State or Federal law or regulation
- Infringes copyright or other intellectual property rights
- Impersonates another user, their email account or any other service
- May hinder productivity (such as forwarding chain emails)
- May damage or impair information technology assets, (for example sending a virus or downloading music or videos, use of chat rooms), either intentionally or unintentionally
- Is for non-business purposes (such as games, music, personal pictures and videos) other than what is permissible under reasonable private use
- Could potentially destabilise Glad Group systems
- Has a negative impact on network resources. For example, video and radio broadcasts over the network is restricted to business use.

3.10. Intellectual Property and Licensing

Electronic communications, documents and computer software is easily copied and increases the risk of intellectual property infringements. Any software that needs to be installed on any Glad Group equipment must be authorised in writing by IT and the manager.

Users must not:

- Copy software which is licensed to Glad Group, unless authorised under the license arrangements
- Download and/or install free or non-Glad Group licensed software on any Glad Group equipment

3.11. Protecting Information and Equipment

Users must take reasonable steps to ensure that information and equipment are appropriately protected and physically secured. This especially applies when using portable equipment (such as laptops, tables and mobile devices. Glad Group equipment that has been lost or stolen must be reported immediately to IT.

3.12. Access to Personal Files and Removal of Unacceptable Material

Glad Group may, without notice or user approval, investigate, replicate and/or remove any illegal or unacceptable material from its sites and computing resources. All users should be aware that their use of Glad Group resources, especially for personal purposes is conditional on this right of access by management as part of investigations. Use of Glad Group systems is subject to lawful monitoring in accordance with applicable legislation.

3.13. Compliance

This compliance section is relevant and enforceable across all IT Policies.

© COPYRIGHT GLAD GROUP (ALL RIGHTS RESERVED)

Glad Group treats misuse of its information systems seriously. Violations of the conditions of use may result in temporary or indefinite withdrawal of access, disciplinary action including termination of employment and/or demand for reimbursement to Glad Group.

In the case of misuse, user access my be withdrawn following a written request from the Manager or Senior Management of the controlled entity or affiliate.

Misuse or unauthorised use of Glad Group Information Systems may constitute an offence under the Criminal Code Act 1995 and/or other state and federal legislations and regulations.

Users must immediately report any suspected or actual data breach, phishing attack, cyber incident or loss of information. Reports will be treated as confidential.

4. Related Policies, procedures and guidelines

- Glad Group Code of Conduct
- Confidentiality Policy
- Mobile Device and Service Usage Policy
- Social Media Policy
- Workplace Surveillance Policy

5. Contact for questions

People and Culture, gladacacemy@gladgroup.com.au

6. Log of change

Date	Amendments	Authorised by	Revision
May 2019	New Policy	**Nick Iloski**	1
March 2026	General Policy Updates	**Ann Shanahan**	2

Authorised By:

Riccardo Furnari

National Technology & Transformation Manager

© COPYRIGHT GLAD GROUP (ALL RIGHTS RESERVED)