EMAIL, INTERNET AND SOCIAL MEDIA POLICY

1. SCOPE

This policy applies to all employees of the Swain Group.

2. AIM

To provide a clear set of principles and guidelines in relation to the use of e-mail, The Internet, social media and databases within the Company.

3. POLICY STATEMENT

Our IT and communications systems are intended to promote effective communication and working practices. This policy outlines the standards you must observe when using these systems, when we will monitor their use, and the action we will take if you breach these standards.

A variety of equipment is provided to employees to allow them to undertake their roles effectively such as laptops, mobile phones and tablets. Whilst being essential business equipment, these devices are also capable of harming the company's IT and communications systems, reputation, employees, customers and third parties if they are abused or used in a manner which is contrary to this Policy. Similarly, the use of such personally owned devices is also capable of causing damage or harm if used contrary to this Policy.

By giving employees access to its IT systems the Company places a great amount of trust that they will be used in a business context, i.e. in any activity that assists the employee in performing their role.

While the Company recognises that limited personal use will occur (as it does with the telephone system), instances of abuse, misuse, or malicious conduct will be treated seriously and dealt with under the Company's Disciplinary Policy. Limited personal use should not impact productivity and work performance and personal use is always subject to the terms of this Policy.

The Company expects that its contractors, agency workers, customers and suppliers will equally abide by this policy and respect the standards it adopts.

4.0 RESPONSIBILITIES

4.1 Employees

- Ensure the rules contained in this and any other related policy are adhered to.
- Refer to this policy if uncertain about any aspect of the company's expectation regarding the use of e-mail, internet or databases.

4.2 Managers

- Ensure that all employees who are given access to e-mail, internet or databases as part of their role abide by this policy.
- Ensure the rules contained in this and any other related policy are adhered to.

5.0 MONITOR AND CONTROL

The IT Department monitoring systems that search email, social media and internet usage. Monitoring is undertaken on a routine, random or targeted basis. Should it uncover serious instances of e-mail and/or Internet abuse, the employees concerned will be subject to disciplinary action.

The company reserves the right, where appropriate, for any employee's e-mail system to be intercepted and vetted at any time, by their Line Manager, the Human Resources or IT Departments. This is for the purpose of monitoring, record keeping, to find lost messages, or to retrieve messages lost due to computer failure, prevention and detection of crime, investigating or detecting the unauthorised use of the company's systems or ascertaining compliance with company practices and procedures and other wrongful acts.

While the Company respects the privacy and trust of individuals, monitoring and vetting is undertaken to ensure compliance with the Company's legal obligations and is necessary for the purposes of legitimate business practice and interests.

It must be noted that even information that has been deleted can still on occasions be retrieved and traced.

6.0 E-MAIL

Appropriate and professional language must be used in all e-mail messages, both internally and externally. The use of emojis is not permitted. As soon as an e-mail is sent, it is no longer under the sender's control; the message may end up in the public domain or be read by someone else unintentionally. For the purposes of defamatory actions, the sending can amount to publication and result in liability sometimes in several jurisdictions at once, depending on where it is received.

Remember, that just like correspondence, e-mail communications can be admissible as evidence in criminal or other legal proceedings. Care must be taken with regards to content, subject-matter covered and expressions on liability issues or admissions (e.g. that something is or may be our fault). Such factors can subsequently be used as evidence in court and can be contractually binding.

6.1 E-mail Usage

Messages, data, programmes or files must not be transmitted or, as far as possible received, that could cause or potentially cause hardware, software or network failure and/or the destruction of data.

The Company prohibits employees to participate in "chain" e-mails, jokes or to spend an inordinate amount of time organising non-Company related social events via e-mail or any other 'messaging' system (e.g. Instant Messenger).

With regards to personal e-mails, employees must take care not to abuse the system.

Attachments sent to external sources should be avoided unless they are business critical. Confidential or business sensitive e-mails and attachments should be password protected and/or encrypted.

Clearly, the receipt of e-mails is beyond anyone's control; however, the subsequent cascading of messages is entirely the employee's responsibility. E-mails containing material of an unprofessional or inappropriate nature must be deleted at source. Instances where such e-mail messages are passed on will be treated seriously.

It is unacceptable to send persistent, aggravated or intimidating e-mail/instant messages to another person, whether a fellow employee or not. The Company views these as unacceptable and such cases will be treated seriously.

E-mail accounts assigned to a person should not be used by another to send or receive messages unless they are given specific authorisation to do so. Where authorisation is provided, mail forwarding or delegation facilities should be adopted.

The use of "generic" accounts to access e-mail databases is not permitted unless authorised by the IT Department. All e-mail activity must be traceable to an individual by name.

E-mail messages must not be forwarded "automatically" using agents or forwarders to any external e-mail address.

Company internal e-mail messages should not be forwarded to an external address, unless for a specific business requirement. This is particularly important when messages contain confidential or sensitive information, particularly when the recipient may not be under a confidentiality obligation.

Any e-mail sent externally to Internet forums, such as mailing lists or news groups, should not advertise, promote, present or otherwise make statements about the company, its products or services. They must not include photos of company vehicles and equipment.

Subscriptions to any Internet web sites should be avoided. Company e-mail addresses should NOT be used to subscribe to any non-business-related material.

The Company e-mail service must be the only system used to send and receive business related communications. The use of any external e-mail systems for this is not permitted.

6.2 E-mail Maintenance

Checks must be carried out on mailboxes to ensure that the content and size of the mailbox does not exceed individual limits set.

Archiving of e-mails to an archive mailbox must be performed if the mailbox cannot be kept below limits set. Space for archiving mailboxes will be made available where possible on servers. Archive mailboxes held on local PC's are the responsibility of the individual to ensure its integrity and backup.

Large attachments should not be exchanged using the e-mail systems. Doing so can cause serious delays to all other e-mails in the system and can affect the networks being used by other systems.

Mailboxes should not be used as a mechanism for storing and indexing e-mail attachments.

7.0 INTERNET WEB BROWSING

The Internet must only be used to obtain information that is key to the performance of an employee's role whether this is in the office or via a Company provided secure VPN connection. Access to the Internet from Company equipment can only be conducted through approved connection methods.

The Company prohibit employees from using the Internet during working time to:

- Purchase products via the Internet for personal use.
- Use or purchase "smart" mobile phone applications (APPS) for personal use (recreational browsing).
- Download or install software from external sources without authorisation from their Line Manager. This includes software programs, instant messaging programs, screensavers, photos, video clips and music files. Incoming files and data should always be virus-checked by the IT Department before they are downloaded. If in doubt, they should seek advice from the IT Department.
- Apply for jobs outside the organisation or for forwarding a CV via Internet e-mail to the extent that it affects an individual's productivity.

The following examples are deemed inappropriate personal use categories. Sites and APPS within these categories should not be visited in either Company or personal time using company equipment.

Attempts to access these contents will be monitored:

- Adult/Sexually Explicit
- Criminal Activity
- Gambling/Online Auctions/Games
- Hacking
- Illegal drugs
- Intimate Apparel & Swimwear
- Intolerance & Hate
- Personals & Dating
- Phishing, Fraud and Theft
- Spyware
- Tasteless & Offensive
- Violence & Weapons
- Streaming Media

Whilst it is recognised that the Internet contains a wealth of information, some of it may be inaccurate, out of date or libellous. Employees using the Internet should bear this in mind when using it in the context of their work and take reasonable steps to validate the authenticity of such information.

8.0 SOCIAL MEDIA

Social Media portals such as Facebook, YouTube or Twitter offer opportunities to exchange opinions, thoughts, and experiences with other users, friends, colleagues and clients on a global scale.
Employees using these types of media must not post photos of company vehicles and equipment OR make any negative/defamatory comments about the company, its employees, customers, supplier, contractors etc.

8.1 Personal Use

Using the Company's Network, IT resources, communication systems and the use of company equipment such as PCs, and "smart" mobile phones for personal use is prohibited during working hours. Access may be blocked and attempts to access these may be monitored. In addition, the following must not be accessed from the Company's network:

- Online radio
- Audio and video streaming
- Instant messaging.

The company respects employees' rights to a private life. However, employees should be aware that any content posted on the internet is in the public domain.

The following sections of this Policy provide employees with common sense guidelines and recommendations for using social media responsibly and safely at work or in their own time to:

8.2 Protecting the Company's Reputation

All employees are responsible for protecting our business reputation. Employees must not post disparaging or defamatory statements about:

- Other employees
- Our organisation
- Our clients
- Suppliers and vendors
- Other affiliates and stakeholders
- Photos of any company vehicles or equipment.

Employees should avoid social media communications that might be misconstrued in a way that could damage our business reputation, even indirectly.

Posts or comments about sensitive business-related topics, such as our performance are not permitted. Even if you make it clear that your views on such topics do not represent those of the organisation, your comments could still damage our reputation.

Employees should make it clear in social media postings that they are speaking on their own behalf.

Employees are personally responsible for what they communicate in social media. Remember that what you publish might be available for a long time to a potentially large and varied audience including the organisation itself, future employers and social acquaintances. Keep this in mind before you post content.

If you disclose your affiliation as an employee of the Company, you must also state that your views do not represent those of your employer. You should also ensure that your profile and any content you post are consistent with the professional image you present to clients and colleagues.

If you are uncertain or concerned about the appropriateness of any statement or posting, refrain from making the communication until you discuss it with your Line Manager.

If you see content in social media that disparages or reflects poorly on our organisation or our stakeholders, you should contact your Line Manager or the IT Department.

8.3 Respecting Intellectual Property and Confidential Information:

Employees should not do anything to jeopardise company information, confidential information and intellectual property using social media.

The contact details of business contacts made during the course of your employment are regarded as our confidential information, and as such you will be required to delete all such details from your personal social networking accounts, such as Facebook accounts or LinkedIn accounts, on termination of employment.

In addition, employees should avoid misappropriating or infringing the intellectual property of other companies and individuals, which can create liability for the organisation, as well as the individual author.

Do not use our logos, brand names, slogans or other trademarks, or post any of our confidential or proprietary information without prior written permission.

To protect yourself and the organisation against liability for copyright infringement, where appropriate, reference sources of information you post or upload and cite them accurately.

If you have any questions about whether a post or upload might violate anyone's copyright or trademark, ask the IT department.

8.4 Respecting Colleagues, Clients, Partners and Suppliers:

Do not post anything your colleagues or our customers, clients, business partners, suppliers, vendors or other stakeholders would find offensive, including discriminatory comments, insults or obscenity.

Do not post anything related to your colleagues or our customers, clients, business partners, suppliers, vendors or other stakeholders without their written permission.

Clause 8.1 of this policy applies regardless of whether the social media is accessed using the Company's IT facilities and equipment or equipment belonging to you or any other employee.

Employees may be required to remove internet postings which are deemed to constitute a breach of this policy. Failure to comply with such a request may result in disciplinary action.

8.5 Business Use

Our company is often the subject of discussion on the social media sites. Everyone who comments on the Company shapes the company's image in the public eye.

- The Company will provide access upon request, to employees that can demonstrate a business need to use social media.
- If your duties require you to speak on behalf of the organisation in a social media environment, you must still seek approval for such communication from your manager.
- If you are contacted for comments about the organisation for publication anywhere, including in any social media outlet, direct the inquiry to the Managing Director's office.
- Do not deliberately or unwittingly give a third-party access to a database or information contained on it, whether they are an employee or an external person.
- It is strictly prohibited to pass on any information to a competitor or person who may then cause detriment or derive a competitive advantage over the Company.

9.0 COMPANY EQUIPMENT

9.1 Passwords

Users must comply with the following rules regarding passwords:

- Passwords are confidential, remain personal and should never be disclosed to any other person apart from the IT Department.
- They must not be kept on paper or any computer media, unless these can be stored securely. Passwords should not be distributed via unencrypted e-mail.
- They must be changed whenever disclosed or when there is any indication of possible system or credential compromise.
- Passwords used for access to Company assets must not be re-used for any non-work usage (e.g. for access to a private mailbox, a private computer or access to any website on the Internet).

9.2 Software/Hardware

Only approved software that is correctly licensed to the Company may be used and is required to be purchased through the IT Department.

To get software installed users must contact the IT Department.

Users should be aware that non authorized hardware including but not limited to disk drives, tape drives, USB-sticks, CDROM/DVD writers or network adapters such as wireless LAN cards, could introduce risks.

All hardware installation or modification is therefore also restricted to the IT Department.

9.3 Security

Equipment connected to the Company Network via a LAN cable must have any Wireless devices turned off to prevent simultaneous access to other networks.

To ensure secure disposal or re-use of equipment containing sensitive or classified data, the user must contact the IT Department for further instructions.

Users must lock or log out of their workstation when they temporarily leave their desks. Users must ensure that they have properly logged out of all systems before they leave the premises for the day.

No person can try to explore or test a suspected weakness without appropriate authorisation. Testing weaknesses is interpreted as a misuse of the system.

10. POLICY BREACHES

Breaches of this policy may result in disciplinary action up to and including dismissal. Disciplinary action may be taken regardless of whether the breach is committed during working hours or not, and regardless of whether Company equipment or facilities are used for the purpose of committing the breach.

11. POLICY REVIEW AND ASSESSMENT

This policy will be reviewed and amended at any time to consider changes to legislation and/or best practice