

Use of Email, Intranet, Internet and Voicemail Policy

This policy applies to all full time and part time employees, contractors and temporary staff of the A1 Group who have access to our systems for email (both internal and external), our intranet, browsing the internet and voicemail. It also applies to the way in which you use these systems when you are off-site. The policy may change from time to time, and such changes will be communicated to you.

The A1 Group maintains systems which provide email, intranet, internet and voicemail services for the purpose of assisting in the conduct of A1 Group business. Messages sent through email or the internet, the data on A1 Group computers and messages contained on voicemail are the sole property of the A1 Group.

Communications via, and any messages stored on, these systems, are business records of the A1 Group. They can therefore be used (for or against us) in court cases or administrative proceedings. You are strongly urged to take the same care using these systems as when writing and sending business letters.

Purpose

This policy covers the procedures for access to email, voicemail, intranet and internet services and the rules governing their use.

Administration

The Director and HR Consultant administer this policy and the procedures within it.

Email

Email is as common as the telephone - it is a very effective way to communicate within a geographically diverse organisation such as the A1 Group. The purpose of email is to improve communication between all levels of the organisation, regardless of geography. It is also an excellent means of distributing A1 Group news, information, results and policy announcements.

Since email is a core part of our infrastructure, its proper use should be encouraged wherever appropriate, but its purpose should never be undermined. It is fast becoming an effective way of communicating with our business partners by the implementation of gateways to other email systems.

Email falls into the indirect cost category and sometimes its use is taken for granted - it is perceived to be always available and free of charge. However, although there is no direct cost associated with each message sent, there is a cumulative cost in terms of usage of the available network bandwidth. It is the responsibility of the Director to make sure that the appropriate capacity is available to enable effective use of email. It is also the responsibility of every user to make sure that they are using the system to its best effect.

Care should be taken when using email because email messages are perceived to be less formal than paper-based communication and there is a tendency to be lax about their content. Bear in mind that all expressions of fact, intention and opinion via email can be held against you and/or A1 Group in the same way as verbal and written expressions or statements. Do not include anything in an email which you cannot or are not prepared to account for. It is good practice to re-read each email in hard copy before sending it. An email cannot be retrieved once it is despatched.

Email messages which have been deleted from the system can be traced and retrieved. Therefore, all persons having a part in creating or forwarding any offending email can be identified. Emails, both in hard copy and electronic form, are admissible in a court of law.

Conduct when using email

The main reason for the existence of the A1 Group email system is for A1 Group business. However, we recognise that from time to time you will need to use the system for personal use – subject to the conditions on use set out in this policy, A1 Group allows you to use the system for a reasonable amount of personal emails, but please do not abuse this facility.

Email (whether business or personal) must not be used for:

- Accessing, downloading, distributing or sending pornographic or obscene materials.
- The communication or printing of material in breach of copyright laws
- Any communications which may be or are abusive, defamatory, obscene, offensive, vulgar, threatening or harassing. *This could include abusive or bullying behaviour and such matters as sexual or racial comments or images, or indeed anything which could offend someone on the basis of their race, sex, age, religion, nationality, disability or sexual orientation*
- Posting statements about A1 Group or data for which A1 Group is responsible
- Sending chain letters
- Copying electronic files without permission
- Using A1 Group equipment or resources to violate any law or to perform any unethical business acts
- Attempting to obtain unauthorised access into any computer
- Using email to transfer large file attachments (over 5MB in size) and where possible attachments should be zipped (compressed). Contact your manager for alternatives to using email to share files
- Forwarding email to yourself or to another person by use of agents (for example, to your private email account) which requires a Director's prior consent. Furthermore, forwarding individual emails to your private email account, such as Hotmail, is not encouraged
- Sending or posting confidential materials to any unauthorised person, inside or outside A1 Group
- Releasing viruses, worms, Trojan horses, or similar programs by sending attachments of unknown origin
- Taking deliberate actions such as creating 'email storms' to make a computer system or network unavailable to other users

Further, the system should not be used for matters such as social announcements.

Email Signatures

You may have noticed the facility to add a 'signature' to your email messages.

Name | Job Title | Primary Phone | Mobile Phone

Please use the default font type and colour and note that scanned images and graphics should not be used.

Please note the following:

- All information to be placed on one line. Do not include email address
- Do not include quotes or tag lines of any kind except A1 Group approved tag line may be added in a second line after the Name/Details line
- Do not include graphics or environment/printing reminders

All the above is in an effort to reduce the amount of paper/toner/ink used should an email be printed.

The email system is provided by A1 Group for business use, and you are required to adhere to the guidelines above for the sending of corporate external emails.

Misuse of Email

As with all communications both internally and externally, you should ensure that you are professional and courteous at all times. Misuse of the systems may lead to disciplinary action which may result in your dismissal. Some examples of misuse are:

- Accessing, downloading, distributing or sending pornographic or obscene materials
- The communication or printing of material in breach of copyright laws or using our systems to try to gain unauthorised use of third party systems
- Any communications which may be or are abusive, defamatory, obscene, offensive, vulgar, threatening or harassing. This could include abusive or bullying behaviour and such matters as sexual or racial comments or images, or indeed anything which could offend someone on the basis of their race, sex, age, religion, nationality, disability or sexual orientation

The A1 Group may override any individual passwords or require you to disclose them to facilitate access to these systems. To ensure compliance with this policy A1 Group reserves the right to access the systems at any time without notice and to monitor their use.

The Internet

The A1 Group internet access facilities provide:

- Access to the World-wide Web (www) for browsing
- Internet mail service through our email system

The above points dealing with email apply equally to internal emails and external internet emails.

Access to Internet browsing for individuals will be allowed for all employees, subject to adhering to the policies defined in this document.

This policy applies to all the above methods of accessing the internet, whether in work hours or for personal use or not.

Conduct when using the Internet

The following are examples of activities which could result in revocation of Internet access privileges and/or disciplinary action:

- The use of inflammatory, obscene or other inappropriate comments (these may result in a complete shutdown of A1 Group to the Internet, with A1 Group being held legally liable)
- Activities that incur additional costs to A1 Group or interfere with employees' work performance
- Profit-making activities that accrue to the employee.
- Unlawful activities, including sending or receiving copyrighted materials in violation of copyright laws or license agreements
- Sending or receiving sexually explicit or offensive messages, cartoons or jokes, ethnic slurs, racial epithets or any other statement or image that might be construed as harassment, disparagement or libel
- Sending A1 Group proprietary or confidential materials to anyone not entitled to know or possess them

You should not use or install any instant messaging (IM) software at all. IM software, such as AOL or MSN, is inherently insecure and can introduce viruses to our IT systems.

You may not use the A1 Group internet - or any other mechanism to obtain any third party software without the explicit permission of the Director. This particularly applies to any free or open source software. Even if there is no apparent immediate charge for the software you may not download or use it or incorporate any portion of it in your work. Use of free or open source software can expose the A1 Group to significant obligations and liabilities and must be expressly approved in writing by a Director.

Whilst the Internet offers the potential of immense rewards, it also contains serious risks. Anyone and everyone can have access to the Internet. As users of the Internet, employees must:

- Ensure that they act as responsible users and do not engage in activities that will annoy or offend A1 Group electronic neighbours
- Ensure that they are careful and professional in what type of information is sent and accessed over the Internet

Employees should disclaim speaking for A1 Group, where appropriate. Personal opinions posted on bulletin boards must be accompanied by a disclaimer that clearly indicates the opinions expressed are the originators only and are not the opinion of A1 Group. Employees should be aware that their posting might well be forwarded around the world and that when using A1 Group system to post a message, A1 Group name may be carried along with it.

Any A1 Group presence on the Internet such as Home Pages or Web Servers will be controlled and administered by the A1 Group Directors. Building home pages or web servers with any reference to A1 Group is not authorised.

Although the Internet represents a valuable information resource for legitimate business and technical research and information sharing, it also presents a significant opportunity for abuse, lost employee productivity and potential liability for both A1 Group and the employee. Inappropriate, illegal or indiscreet uses and activities of any kind will reflect on A1 Group and on A1 Group personnel.

Protection of the A1 Group network and computer systems is A1 Group's number one priority: thus security measures protecting its network will override all other considerations.

For this reason, the following restrictions will apply:

- Unless and until adequate security and encryption technologies are available, the Internet is not a method for remotely connecting to the A1 Group network
- Some Internet functions will be unavailable
- The tools available to access the Internet will be limited to those tools that do not compromise the security of our network

General

The Internet is not secure. Where there is a more secure communication method available (i.e. proprietary direct connect email gateways between A1 Group clients and A1 Group Outlook email system), then employees must use it.

As all employees are responsible for keeping A1 Group proprietary information confidential, they should not send any confidential information through the Internet. Once information enters the Internet there are no guarantees as to how many copies of it may be produced, where it will end up, how long it will remain there, or who may read it. Further, please remember that all our confidential information needs to be treated carefully, such as local replicas of databases which might hold confidential data.

To prevent computer viruses, no employee may download software or computer files from the Internet without the prior permission of the Director. Further, no additional software (e.g. from CD-ROMs) may be loaded onto hard drives without the prior permission of the Director.

Before using any downloaded software, employees should verify that the licensing agreement indicates whether it can be used for commercial purposes. Employees will be



held personally responsible for any infringement of licensing agreements for software which they have loaded.

The Internet is not 'owned' by anyone. The A1 Group Directors do not have the ability to positively identify problems, trace missing mail, know why a device in the Internet is not responding or fix or change anything in the Internet. Therefore, depending on the nature of the problem, the A1 Group Directors will unfortunately be unable to help in certain instances. There are absolutely no guarantees that Internet services will work properly. The A1 Group Directors can only ensure that A1 Group systems are functioning correctly.

Mail on the Internet is essentially a store and forward mechanism, outside A1 Group ability to control. It does not have the ability to let employees know if their email was received by the intended party. In addition, timely delivery of email cannot be guaranteed. It may take moments, it may take days. It may not happen. It may go to someone unintended. These problems are not known to be widespread but on the other hand are not completely rare. It is the employees' responsibility to ensure that their Internet email is received by the intended party.

The A1 Group Internet services will be under constant probe and attack from the outside by persons attempting to access our systems. There will be times when it will be necessary to shut these services down for extended periods of time to protect A1 Group network and systems, or to repair damage, or to stop email floods from consuming A1 Group network. If employees have critical business requirements for the Internet that cannot be interrupted it will be necessary for them to install a standalone Internet service to use during these outages. Contact the Directors for more information.

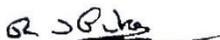
Compliance Monitoring

To ensure that employees are adhering to their responsibilities, A1 Group reserves the right to monitor to whom employees are sending email and from whom employees are receiving email and to examine the content of suspected email messages if it is suspected that this policy is being broken. The A1 Group also reserves the right to monitor employee's use of the Internet, both for email and browsing, voicemail and the intranet.

This may be done without employees' consent or knowledge, but will only be done with the consent of their Director. All such instances will be reported to the Director. Any breach of this policy may result in disciplinary action.

Revision

The Company will make all employees aware of this Company Policy.

Signed: 

Date: 1/1/24

Russell Pike - **Managing Director A1 Group**

Next Review date 1st January 2025