Future Marine Services

IT & Communications Policy

Overall Aim

The IT and communications systems are intended to protect the Company's legal interests and to promote effective communication and working practices within the organisation by;

- Outlining the standards which must be observed when using these systems, the circumstances in which usage will be monitored, and the action taken in respect of breaches of these standards
- Ensuring all individuals understand the Company's expectations specifically with regards to the use of Company devices, internet, email and social media both at work and outside of working hours
- Ensuring the Company's compliance with data protection legislation such as the General Data Protection Regulations (GDPR) and the Data Protection Act 2018.

Definition

For the purposes of this policy, the Company refers to Future Marine Services (FMS), including any and all associated subsidiary companies, including, but not limited to SafeSTS Ltd, SafeSTS (Asia-Pacific) PTE Ltd, SafeSTS (Mozambique) Ltda, SafeSTS (Middle East) FZE, SafeSTS Servicos do Brazil Ltda and SafeSTS Transfer Technology Ltd.

Scope

This policy applies to all employees, officers, consultants, contractors, casual workers, agency workers and anyone who has access to the Company's IT and communication systems (herein referred to as 'staff' or 'individual').

Misuse of the IT and communications systems can damage the business and the Company's reputation. Breach of this policy may be dealt with under the Disciplinary Procedure and, in serious cases, may be treated as gross misconduct leading to summary dismissal or termination of the engagement.

This policy does not form part of any individual's contract of employment or contract for service and may be amended at any time.

Equipment Security and Passwords

Whilst all equipment remains the property of the Company, staff are responsible for the security and condition of the equipment allocated to or used by them and must sign a Company Equipment Receipt form upon issuance. Any incidences of theft, loss, damage or defect to a Company device must be reported at the earliest opportunity to the Systems Administrator, (currently Anna Koloch, anna@safests.com). Repairs to a Company device are only permitted by a Company approved service provider under advice from the Systems Administrator, repairs conducted by an unauthorised entity are strictly prohibited. Whilst there is insurance cover in place for Company devices, if for any reason a claim is made which the insurance company refuses to pay, then the individual will be required to repay to the Company the cost of the device and any accessories if it is lost, stolen or damaged whilst under the individual's control due to gross negligence or wilful default. Such circumstances may also invoke the Disciplinary Procedure.

Staff must not allow their equipment to be used by anyone other than in accordance with this policy, terminals should be locked or logged off immediately when being left unattended or on leaving the office, to prevent unauthorised users accessing the system. Anyone who is not authorised to access the network should only be allowed to use terminals under supervision or with limited access rights.

Particular care must be exercised in protecting data (which includes personal data, sensitive personal data and business-related data) from loss, unauthorised access, use or disclosure. Please read in conjunction with the Privacy Notice.

Passwords should be used on all IT equipment, particularly items that are taken out of the office. Passwords must be kept confidential and be changed regularly (every 85 days). Staff must not use another person's username and password or make available or allow anyone else to log on using their username and password unless authorised by their Line Manager.

If issued with a laptop, tablet computer, smartphone or other mobile device, Staff must ensure that it is kept secure at all times, especially when travelling. Staff will only be issued one smartphone device at any one time. Passwords and passcodes must be used to secure access to all portable devices. Staff should also be aware that when using equipment away from the workplace, documents may be read by third parties, for example, passengers on public transport.

Staff are forbidden to purchase any IT accessories without prior approval from the System Administrator, to ensure system compatibility.

Upon termination of employment/engagement (for any reason), any equipment allocated to the individual must be returned to the Company (including chargers) and details of all passwords provided to HR. No data is to be deleted from the devices unless agreed with the System Administrator.

Prohibited Use of Personal Devices

The use of personal devices for business purposes gives rise to increased risk in terms of the security of our IT resources and communications systems, the protection of confidential and proprietary information and reputation, and compliance with legal obligations.

Staff are not permitted to use personal devices (such as telephone, tablets, smartphones or computers), to conduct Company business unless they have prior permission from their Line Manager and adhere to security measures put in place (InTune software). Staff should always use Company owned devices for conducting Company business.

Staff who are required to work remotely may be provided with Company mobile devices. In the event of fault or issue with the Company mobile device, this should be reported immediately to the Systems Administrator.

Employees who are discovered contravening this rule may face disciplinary action, up to and including dismissal for gross misconduct under the Disciplinary Procedure, and in the case of a breach of this rule by a contractor, consultant, casual or agency worker, the termination of the engagement. Staff are required to co-operate with any investigation into a suspected breach, which may involve providing us with access to the device and any relevant passwords, login details or itemised billing.

Data Security

Staff should not delete, destroy or modify existing systems, programs, information or data (except as authorised in the proper performance of their duties).

Devices or equipment from unknown sources must not be attached to Company systems without authorisation from the System Administrator. This includes any USB flash drive, MP3 player, tablet, smartphone or other similar device, whether connected via the USB port, Bluetooth, infra-red connection or in any other way.

Staff should not attempt to gain access to restricted areas of the network, or to any password-protected information, except as authorised in the proper performance of their duties.

It is a requirement that all work and data shall be stored on SharePoint , or the Company's other operating systems such as SAP and SafeOps. If any information is stored on SharePoint, at least two members of staff must have access to a particular site/folder. Staff must not save any business related work and/or information on their laptop's C drives or hard-drives of their portable devices. This is to ensure that any data loss is not irrecoverable, to protect personal and business related data from loss, unauthorised access or disclosure and to ensure compliance with our policies and procedures. Random checks and audits will be performed to ensure no Company data is stored on C drives. Failure to adhere to this security measure willusually amount to gross misconduct.

Remote access is allowed via secure methods only. The Company shall provide the only VPN that may be used. Staff must not disclose the VPN password to others.

All incidences of loss or theft of personal data or confidential information should be reported immediately to the System Administrator so that they may be investigated. A data or IT security incident relating to breaches of security and/or confidentiality could range from computer users sharing passwords to the loss or theft of confidential information.

Staff must be particularly vigilant if using Company IT equipment outside the workplace and take such precautions as the Company may require from time to time against importing viruses or compromising system security. The system contains information which is confidential and/or subject to data protection legislation. Such information must be treated with extreme care and in accordance with the Data Protection Policy, Privacy Notices and GDPR.

Computer Software

The Company licences the use of computer software from a variety of outside companies. The Company does not own this software or its related documentation and, unless authorised by the software developer, neither the Company nor any of its staff have the right to reproduce it. To do so constitutes an infringement of copyright.

Staff must not download or install software from external sources without authorisation from the System Administrator. 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 System Administrator before they are downloaded. If in doubt, staff should seek advice from the System Administrator.

Screen sharing software such as Zoom, MS Teams, Join.Me, Team Viewer and GoToAssist is only permitted when necessary in line with an individual's performance of their duties. Staff must always be present during the use of screen sharing software and activity must be monitored to ensure that only relevant screens and information is accessed.

Computer Viruses

The Company monitors all emails passing through the system for viruses. Staff should exercise particular caution when opening unsolicited emails from unknown sources or an email which appears suspicious (for example, if it contains a file whose name ends in .exe). Inform the System Administrator immediately if you suspect your computer may have a virus. The Company reserves the right to delete or block access to emails or attachments in the interests of security. The Company also reserves the right not to transmit any email message.

The Company's computer network makes it vulnerable to viruses and virus protection software has been installed. Therefore, only duly authorised personnel have the authority to load program software onto the network system and re-configuring or disabling the virus protection software is prohibited. Data compatible with the Company's system may be loaded only after being checked for viruses by authorised personnel.

E-mail

Unregulated access increases the risk of staff inadvertently forming contracts through e-mail and increases the opportunity for wrongful disclosure of trade secrets and other confidential information. In addition, carelessly worded e-mails or messages can expose the Company to an action for defamation for libel. As such, e-mails to clients and suppliers must be reviewed prior to sending to ensure appropriate professional formatting, failure to do so is a disciplinary matter and will be dealt with under the Company's disciplinary procedure.

Correspondence with third parties by email should be written as professionally as a letter. Messages should be concise and directed only to relevant individuals. Staff must ensure there is at a minimum one other individual (as appropriate to the subject content) copied in on all email correspondence to reduce the risk of a single point of contact on business matters. Failure to comply with this requirement may result in the application of the Company's disciplinary procedure.

Where possible, emails should be accessed at least once every working day, staff should stay in touch by remote access when travelling in connection with business and use an out of office response when away from the office for more than a day. If an individual is out of the office for any length of time, they are responsible for ensuring that all emails are automatically forwarded on to a designated Company email address, which will be accessible by the Company. On termination of employment/engagement or as otherwise instructed by the Company, all emails will be automatically forwarded on to a designated Company email address.

Staff must not send abusive, obscene, discriminatory, racist, harassing, derogatory, defamatory, pornographic or otherwise inappropriate emails (for example this may include but is not limited to offensive remarks, jokes, pictures or videos sent by e-mail, via social networking websites or blogs). Anyone who feels that they are being, or have been harassed or bullied, or is offended by material received from a colleague via email, should inform HR in accordance with the Anti-Bullying and Harassment Policy.

Staff should take care with the content of all email messages, as incorrect or improper statements can give rise to claims for discrimination, harassment, defamation, breach of confidentiality or breach of contract. The Company has no control over where an email may be forwarded by the recipient. Avoid saying anything which would cause offence or embarrassment if it was forwarded to colleagues or third parties or found its way into the public domain.

Email messages are required to be disclosed in legal proceedings in the same way as paper documents. Deletion from a user's inbox or archives does not mean that an email cannot be recovered for the purposes of disclosure. All email messages should be treated as potentially retrievable, either from the main server or using specialist software.

In general, staff should not:

a) Send, forward or read private emails at work which you would not want a third party to read
b) Send or forward chain mail, junk mail, cartoons, jokes or gossip
c) Contribute to system congestion by sending trivial messages, copying or forwarding emails to those who do not have a real need to receive them, or using "reply all" unnecessarily on an email with a large distribution list
d) Agree to terms, enter into contractual commitments or make representations by email unless appropriate authority has been obtained. A name typed at the end of an email is a signature in the same way as a name written at the end of a letter
e) Download or email text, music or any other content on the internet which is subject to copyright protection, unless it is clear that the owner of such works allows this
f) Send messages from another person's email address (unless authorised) or under an assumed name
g) Send confidential messages via email or the internet, or by other means of external communication which are known not to be secure
h) If an email is received in error the sender should be informed.

Staff must not use own personal email accounts to send or receive email for the purposes of our business. Only use the email account provided by the Company.

Where staff are authorised by the Company to enter into contractual commitments with others, it is a mandatory requirement that all negotiations by email includes a heading ‘Subject to Contract’. This protects the Company from an individual inadvertently creating a legally enforceable contract through a series of emails. Failure to adhere to this requirement will usually amount to gross misconduct.

Further, staff are not allowed to spend time ‘chatting’ by e-mail, MS Teams or any other communication software for personal and private purposes during Company time. Excessive time spent online leads to loss of productivity and constitutes an unauthorised use of the Company’s time.

<u>Writing email instructions summary:</u>

1. Include a clear, direct subject line.
2. Use a professional email address, never use your personal one if you are making contacts on behalf of the company.
3. Think twice before you hit reply all, choose your recipients carefully as not always everyone needs to be copied in.
4. Include your signature, it is important that the client knows your contact details; however when you respond multiple times, signature will take a lot of space; hence it is acceptable to lose it.
5. Use professional salutations.
6. Avoid using exclamation marks.
7. Proofread your email.
8. Ensure all fonts, colours are consistent.
9. Be mindful that people from different cultures email and speak differently.
10. Ensure correct grammatical style is used.

Internet

On Company equipment and devices staff are only permitted to surf the internet for personal and private use, log on to social networking and video sharing or streaming websites including but not limited to, Facebook, , LinkedIn, Instagram, Twitter, , WhatsApp and YouTube or use the Company IT systems to keep a personal weblog ('blog') at designated times during the day. The designated times are either before or after normal working hours and during any lunch break. The Company reserves the right to restrict access to internet websites at any time.

Staff must limit the use of personal devices for personal and private internet use to the above designated times. Unauthorised use outside of the designated times is regarded as misuse of Company time.

Some individuals may be authorised to use their own accounts on sites such as LinkedIn, and WhatsApp for work purposes. In this case, they must receive permission from their Line Manager to do so in Company time and on Company equipment. The Company reserves the right to review audit and monitor their accounts for business purposes (as detailed in this policy).

The use of LinkedIn, and WhatsApp should be reserved for informal communication with clients and/or suppliers only. Any information which may be required to be upheld within a court of law (such as negotiations, complaints, agreements, terms and scopes of work) must be communicated more formally via email, especially for any official or contractual agreements or documents.

For full details on the Company's rules and expectations regarding the use of social media please refer to the Social Media Policy.

Staff should not access any web page or download any image, document or other file from the internet which could be regarded as illegal, offensive, discriminatory, in bad taste or immoral. Even web content which is legal in the UK may be in sufficient bad taste to fall within this prohibition. As a general rule, if any person (whether intended to view the page or not) might be offended by the contents of a page, or if the fact that our software has accessed the page or file might be a source of embarrassment if made public, then viewing it will be a breach of this policy.

Logging on to sexually explicit websites or the downloading and/or circulation of pornography or other offensive, obscene or illegal material constitute gross misconduct offences and render the employee liable to summary dismissal under the Disciplinary Procedure, whilst staff are liable to termination of their engagement.

Computer Games

There are computer games on the network. Staff may only access these outside their normal working hours, for example during lunch breaks. Staff must not install their own games on to work computers.

Training

Any IT related training issued by the Company to Staff to increase security awareness, must be completed within set timeframes. Any Staff identified as being non-compliantwith the training requirements and deadlines will be issued with an NCR and may result in the application of the Company's Disciplinary Procedure.

Phone Usage

The Company's telephone lines and mobile phones, (for staff whose job role requires them to have a Company issued mobile device), are for the exclusive use by staff in connection with the Company's business.

Whilst the Company will tolerate essential personal telephone calls concerning an employee's domestic arrangements, excessive use of Company or personal telephones or mobile phones for personal calls during working hours is prohibited. This includes lengthy, casual chats and calls at premium rates. Not only does excessive time engaged on personal telephone calls lead to loss of productivity, it also constitutes an unauthorised use of the Company's time.

Personal telephone calls should be timed so as to cause minimum disruption to the individual's work and should, as a general rule, only be made during breaks except in the case of a genuine emergency.

Staff should be aware that telephone calls made and received on the Company's telephone network will routinely be monitored to assess staff performance, to ensure client satisfaction and to check that the use of the telephone system is not being abused. The Company receives itemised bills for all Company phones from the service providers. These bills provide details of the number of calls, the length of calls, the cost of calls and the numbers dialled.

If the Company discovers that the Company phone has been used excessively for personal calls, this will be dealt with under the Disciplinary Procedure.

<u>Mobile phones</u>

For staff whose job roles require a mobile phone in order to fulfil their duties, the Company will supply a mobile phone with a charger. The individual is required to purchase a suitable case and charge to the Company on their expenses with proof of purchase.

The Company operates the mobile phone supplied on a monthly contract basis. The package includes a bulk allowance of calls within the UK, company-to-company mobile calls and a data allowance. If there is excessive usage over and above the bulk call allowance, then individual phone usage will be reviewed to identify the nature and location of calls and establish if there has been unnecessary usage.

Calls to satellite phones, overseas mobiles and non-geographic numbers (0845/0945 etc.) do not form part of the Company's bulk call allowance. While it is recognised that calls of this nature are an essential element of the business, staff should be mindful that these calls can be expensive and therefore, before making such calls, should give consideration as to whether it is absolutely necessary or whether an alternative form of contact, such as sending an email, would suffice.

In order to minimise excessive data usage, where possible a secure Wi-Fi connection should be used.

The Company will pay the monthly line rental costs and any call charges incurred in the legitimate business use of the mobile phone. Whenever the monthly bill is unusually high, the individual will be required to check the monthly itemised list of calls received from the mobile phone service provider and declare which calls are personal. The Company reserves the right to request reimbursement for any personal calls incurred in the use of the mobile phone or, subject to approval from the individual, a deduction of the relevant amount from the individual's wages/fees.

The Company reserves the right to request the return of the mobile phone at any time during an individual's term of employment/engagement.

If you have any difficulties using your mobile phone, please contact the Systems Administrator.

Mobile phones and driving

Some staff are occasionally required to travel by vehicle on Company business as part of their duties. Operating a mobile phone whilst driving reduces concentration and increases the likelihood of an accident. It is a criminal offence and the penalty is a fine and points on the driver's licence. Please see below the Company's requirements in relation to using a mobile phone whilst driving on Company business. It applies irrespective of whether the Company-provided mobile phone is used or a personal mobile phone.

The use of hand-held mobile phones or similar hand-held electronic devices whilst driving as part of your duties is strictly prohibited, whether this is to make or receive calls, send or read texts or picture messages or to access the internet or e-mail. Anyone discovered in breach of this rule, may face disciplinary action under the Disciplinary Procedure, in view of the potential health and safety implications.

The vehicle must be pulled over and stopped in a safe place with the engine completely turned off, before using a hand-held mobile phone. A person is regarded as 'driving' for the purposes of the law if the engine is running, even if the vehicle is stationary. This means the hand-held phones must not be used at traffic lights, during traffic jams or at other times when the engine is still running.

A hands-free phone does not require the user to hold it at any point during the course of its operation. A mobile phone that is attached to fixed speakers and does not require the user to hold it whilst in use (for example, because it is stored in a cradle) would be covered, as would a hands-free mobile phone that has voice activation. If the phone needs to be held in the driver's hand at some point during its operation, for example to dial the number or to end the call, it is not hands-free.

If travelling by vehicle is required as part of an individual's duties, the Company will also provide appropriate hands-free mobile equipment to accompany the mobile phone supplied. If a personal mobile phone is used in these circumstances, then the individual must ensure they have the appropriate hands-free equipment for the phone.

However, even with hands-free equipment, driving and conducting a telephone conversation are both attention demanding tasks and all reasonable steps should be taken to ensure these tasks are not carried out at the same time. Whilst driving as part of work duties, any voicemail or call divert facilities available should be made use of, rather than making or receiving 'live' calls, stopping regularly in safe places to check for voicemail messages and to make and return calls. If there is a requirement to make or receive a call whilst driving on Company business with appropriate hands-free equipment, these should be limited to emergency or essential calls and only when it is safe to do so, with any incoming callers being informed that the individual is driving and so the call must be kept short. Please note that the law states that a person can also be prosecuted for using a hands-free device if the person is not in proper control of the vehicle when using the device. The penalty is a fine and points on the driver's licence.

Personal Use of Company Systems

The Company permits the incidental use of the internet, email and telephone systems to send personal emails, browse the internet and make personal telephone calls subject to certain conditions set out in this policy. Personal use is a privilege and not a right. It must not be overused or abused. The Company may withdraw permission for it at any time or restrict access.

Monitoring

The Company systems enable monitoring of telephone, email, voicemail, internet, social media usage and other communications. The Company monitors for business reasons, and in order to carry out legal obligations in its role as an employer, use of Company systems including the telephone and computer systems, and any personal use of them, may be continually monitored by automated software, during routine audits, during periods of leave, in specific cases where misuse is suspected, or otherwise. Monitoring is only carried out to the extent permitted or as required by law as necessary and justifiable for business purposes, and in line with the Company's Privacy Notice.

The Company reserves the right to retrieve the contents of telephone logs, voicemails, instant messages, email messages, social media postings and activities or to check internet usage (including pages visited and searches made) as reasonably necessary in the interests of the business, including for the following purposes (this list is not exhaustive):

- To promote productivity and efficiency
- To ensure the security of the system and its effective operation
- To ensure there is no unauthorised use of the Company's time, for example to check that an individual has not been sending or receiving an excessive number of personal communications or spending an excessive amount of time using social media websites for non-work related activity
- To ensure that all staff are treated with respect and dignity at work, by discovering and eliminating any material that is capable of amounting to harassment under the terms of the Company's AntiBullying and Harassment Policy
- To ensure that inappropriate, restricted or blocked websites are not being accessed by Staff
- To ensure there is no breach of commercial confidentiality
- To monitor whether use of the email system or the internet is legitimate and in accordance with this policy
- To retrieve messages lost due to computer failure
- To assist in the investigation of alleged wrongdoing
- To ensure continuity of service
- To ensure compliance with Company Policies and Procedures
- To comply with any legal obligation.

Prohibited Use of Company Systems

Misuse or excessive personal use of the Company telephone or email system or inappropriate internet use will be dealt with under the Disciplinary Procedure. Misuse of the internet can in some circumstances be a criminal offence. In particular, it will usually amount to gross misconduct to misuse Company systems by participating in online gambling, forwarding chain letters, or by creating, viewing, accessing, transmitting or downloading any of the following material (this list is not exhaustive):

- Pornographic material (writing, pictures, films and video clips of a sexually explicit or arousing nature)

- Offensive, obscene, or criminal material or material which is liable to cause embarrassment to the Company or its clients
- A false and defamatory statement about any person or organisation
- Material which is discriminatory, offensive, derogatory or may cause embarrassment to others (including material which breaches the Equality, Diversity and Inclusion Policy or the Anti-Bullying and Hasrassment Policy)
- Confidential information about the Company, its business, or any of its staff or clients (except as authorised in the proper performance of duties)
- Unauthorised software
- Any other statement which is likely to create any criminal or civil liability (for the Company or the individual)
- Music or video files or other material in breach of copyright
- Storing data on portable devices unless authorised (for security reasons data must only be stored on the network)

Any such action will be treated very seriously and is likely to result in summary dismissal.

Where evidence of misuse is found, the Company may undertake a more detailed investigation in accordance with the Disciplinary Procedure, involving the examination and disclosure of monitoring records to those nominated to undertake the investigation and any witnesses or managers involved in the Disciplinary Procedure. If necessary, such information may be handed to the police in connection with a criminal investigation.

Abuse of the Company's devices is prohibited. Vandalism of the Company's computer network constitutes a potential gross misconduct offence and could render the individual liable to summary dismissal under the Company's Disciplinary Procedure, or the termination of the engagement as applicable.

Related Policies

This Policy should be read in conjunction with the following Company policies and documents:

- Disciplinary Procedure
- Anti-Bullying & Harassment Policy
- Privacy Notice
- Data Protection Policy
- Data Retention Policy
- Information Security Policy
- Social Media Policy
- Employee Privacy Notice

Non-Compliance

Failure to comply with any of the requirements of this policy is a disciplinary offence and may result in disciplinary action being taken under the Company's Disciplinary Procedure. Depending on the seriousness of the offence, it may amount to gross misconduct and could result in summary dismissal or the termination of engagement.

Yvonne Mason, CEO
Future Marine Services Ltd