IT AND SOCIAL MEDIA POLICY

STANLEY GROUP

MAY 2023

Stanley Group

Internet, Email and Social Media Usage Policy and Guidelines

Introduction

1. This policy sets out the obligations and expectations on employees of Stanley Group including contractors and temporary staff, who use the Company's IT facilities. These facilities are provided to assist with day to day work. It is important that they are used responsibly, are not abused, and that individuals understand the legal, professional and ethical obligations that apply to them.

Authorisation

2. No person is allowed to use Company IT facilities who has not previously been authorised to do so by the Company IT Department or their Line Manager. Unauthorised access to IT facilities is prohibited and may result in either disciplinary action or criminal prosecution.

Legislation

3. All users shall comply with all current relevant legislation. This includes (but may not be restricted to) the following:

Data Protection Act 1998 / the General Data Protection Regulations (GDPR)

4. Any personal information on an individual which the Company holds is covered by this legislation. This includes emails too. If you receive a subject access request you should refer this immediately to your line manager.

5. Users need to be sure that they are not breaching any data protection rules when they store or use information and when they write and send emails. This could include but is not limited to:

    - Using data which has not been kept up-to-date.
    - Passing on or processing personal information about an individual without their consent.
    - Keeping personal information longer than necessary.
    - Sending personal information outside the country.
    - Including password(s) to encrypted files within the same medium as the attachments

6. If any breach of data protection rules is discovered such as the leaking or hacking of personal or sensitive data, this should be reported immediately to your line manager, and any immediate action should be taken to close down such leaks. Your line manager will ensure this is properly investigated and the appropriate reporting actions taken if necessary.

Computer Misuse Act 1990

7. This Act makes it an offence to try and access any computer system for which authorisation has not been given.

Copyright Design and Patents Act 1988

8. Under this Act it is an offence to copy software without the permission of the owner of the copyright.

Defamation Act 1996

9. Under this Act it is an offence to publish untrue statements which adversely affect the reputation of a person or group of persons.

Terrorism Act 2006

10. This Act has makes it a criminal offence to encourage terrorism and/or disseminate terrorist publications.

Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000.

11. This allows for any organisation to monitor or record communications (telephone, internet, email, and fax) for defined business-related purposes.

Responsibilities

12. All Users are expected to act in a manner that will not cause damage to IT facilities or disrupt IT services. Any accidental damage or disruption must be reported to the IT department or your line manager as soon as possible after the incident has occurred. Users are responsible for any IT activity which is initiated under their username.

Use of the Internet

13. Use of the Internet by employees is encouraged where such use is consistent with their work and with the goals and objectives of Stanley Group in mind. Reasonable personal use is permissible subject to the following:

- Users must not participate in any online activities that are likely to bring Stanley Group into disrepute, create or transmit material that might be defamatory or incur liability on the part of the Company, or adversely impact on the reputation of the Company.
- Users must not visit, view or download any material from an internet site which contains illegal or inappropriate material. This includes, but is not limited to, pornography (including child pornography), obscene matter, race hate material, violence condoning messages, criminal skills, terrorism, cults, gambling and illegal drugs.
- Users must not knowingly introduce any form of computer virus into the Company's computer network.
- Personal use of the internet must not cause an increase or significant resource demand, e.g. storage, capacity, speed or degrade system performance.
- Users must not "hack into" unauthorised areas.
- Users must not download commercial software or any copyrighted materials belonging to third parties, unless such downloads are covered or permitted under a commercial agreement or other such licence and approved by the Company.
- Users must not use the Internet for illegal or criminal activities, such as, but not limited to, software and music piracy, terrorism, fraud, or the sale of illegal drugs.
- Users must not use the internet to send offensive or harassing material to other users.
- Use of the internet for personal reasons (e.g. online banking, shopping, information surfing) must be limited, reasonable and done only during non-work time such as lunch-time.
- Use of gambling sites, online auction sites and other such inappropriate websites is **not** permissible. If you are in any doubt, you should confirm with your line manager whether a site is permissible or not before accessing the site.
- Staff may face disciplinary action or other sanctions (see below) if they breach this policy.

Use of Email / Instant messaging

14. Messages sent or received on the Company email / IM system form part of the official records of Stanley Group; they are not private property. The Company does not recognise any right of employees to impose restrictions on disclosure of such messages within the Company. These may be disclosed through legal obligations, as part of legal proceedings (e.g. tribunals), and as part of disciplinary proceedings. Users are responsible for all actions relating to their IT account including username and password, and should therefore make every effort to ensure no other person has access to their account.

15. When using Company email / messaging systems, users must:

- ensure they do not unnecessarily disrupt the Company's wider IT systems or cause an increase for significant resource demand in storage, capacity, speed or system performance e.g. by sending large attachment to a large number of internal recipients.
- ensure they do not harm the Company's reputation, bring it into disrepute, incur liability on the part of the Company, or adversely impact on its image.

- not seek to gain access to restricted areas, without authorisation, of the network or other “hacking activities”; this is strictly forbidden.
- not use the system for the creation, retention or distribution of disruptive or offensive messages, images, materials or software that include offensive or abusive comments about ethnicity or nationality, gender, disabilities, age, sexual orientation, appearance, religious beliefs and practices, political beliefs or social background. Employees who receive emails / messages with this content from other employees of the Company should report the matter to their line manager or supervisor.
- not send emails / messages that might reasonably be considered by recipients to be bullying, harassing, abusive, malicious, discriminatory, defamatory, and libellous or contain illegal or offensive material, or foul language.
- not upload, download, use, retain, distribute, or disseminate any images, text, materials, or software which might reasonably be considered indecent, obscene, pornographic, or illegal.
- not engage in any activity that is likely to
    - Corrupt or destroy other users’ data or disrupt the work of other users
    - Waste staff effort or Company resources, or engage in activities that serve to deny service to other users
    - Be outside of the scope of normal work-related duties – for example, unauthorised selling/advertising of goods and services
    - Affect or have the potential to affect the performance of damage or overload the Company system, network, and/or external communications in any way
    - Be a breach of copyright or license provision with respect to both programs and data, including intellectual property rights
- not send non-business-related chain letters or joke emails from a Company account.

16. Staff who receive improper email from individuals inside or outside the Company, should discuss the matter in the first instance with their line manager or supervisor.

17. Personal use of a Stanley Group email / message account is **strongly discouraged**.

Email Good Practice

18. The Company has good practice guidelines for dealing with email when staff are out of the office for longer than three days. When activating the "out of office" facility messages should name an alternative member of staff for correspondents to contact if necessary. This will ensure that any important messages are picked up and dealt with within required timescales.

19. During periods of absence when highly important emails are anticipated, the employee (or manager) should make arrangements for notification and access by another appropriate member of staff.

20. Where sensitive and confidential information needs to be sent via email for practical reasons, please be aware that email is essentially a non-confidential means of communication. Emails can easily be forwarded or archived without the original sender’s knowledge. They may be read by persons other than those they are intended for.

21. Users must exercise due care when writing emails to avoid being rude or unnecessarily terse. Emails sent from the Company may be interpreted by others as Company statements. Users are responsible for ensuring that their content and tone is appropriate. Emails often need to be as formal and businesslike as other forms of written correspondence.

22. Users should delete all unsolicited junk mail, and in the process of archiving emails, users should ensure inappropriate material is not archived.

23. The Company provides a current and up to date automatic virus checker on all networked computers. However, caution should be used when opening any attachments or emails from unknown senders. Users must best endeavour to ensure that any file downloaded from the internet is done so from a reliable source. It is a disciplinary offence to disable the virus checker. Any concerns about external emails, including files containing attachments, should be discussed with the IT / Line Manager.

Use of Social Media

24. Many Stanley Group employees will already be using social media in their personal lives. When you are not at work, it is, of course, entirely up to you to decide whether and how you choose to create or participate in a social media space or any other form of online publishing or discussion. This is your own business. The views and opinions you express are your own.

25. However, if you identify yourself as an employee of the Company or as being associated with it in any way, you must be mindful of this when participating in social media. We have a responsibility to make you aware that, even where you don't intend it, you can harm the company's business and reputation when using social media in a personal capacity, and that breaching this policy outside of work can still result in disciplinary action.

Legitimate Access to Prohibited Material

26. There may be circumstances where users feel that the nature of their work means that they are required to access or use material prohibited under this policy. If so, this should be discussed with the Line Manager concerned **before** any access is initiated. The Company is legally responsible for the content and nature of all materials stored on/accessed from its network.

Remote Users

27. Users may sometimes need to use Company equipment and access the Company network while working remotely, whether from home or while travelling. The standards set out in this document apply to Company employees whether or not Company equipment and resources are being used.

Monitoring

28. All resources of Stanley Group, including computers, tablets, phones, external drives, USB drives, email, voicemail etc. are provided for legitimate use. If there are occasions where it is deemed necessary to examine data beyond that of the normal business activity of the Company then, at any time and without prior notice, the Company maintains the right to scrutinise any systems and inspect and review all data recorded in those systems. This will be undertaken by authorised staff only. This examination helps ensure compliance with internal policies and the law. It supports the performance of internal investigations and assists in the management of information systems.

Penalties for Improper Use

29. *Withdrawal of facilities*
    Users in breach of these regulations may have access to Company IT facilities restricted or withdrawn.

30. *Disciplinary Action*
    Breaches of these regulations may be dealt with under the Company's disciplinary procedures. It may lead to termination of employment from the Company.

31. *Breaches of the law*
    Where appropriate, breaches of the law will be reported to the police.