

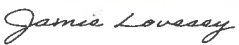

## Electronic Communication & Social Media Usage Policy

---

This Document was written and prepared by J & E Hall Limited. Its use is **CONFIDENTIAL** and must only be used as an internal document. Written authority from a company Director must be obtained prior to circulating this document to any third party

**Document information**

<b>Prepared By:</b>	Jamie Lovesey	<b>Copy No.:</b>	1
<b>Title:</b>	IT Manager		

<b>Reviewed by:</b>	Jamie Lovesey & Andrew Bowden	<b>Authorised by:</b>	Andrew Bowden
<b>Title:</b>	IT Manager/Managing Director	<b>Title:</b>	Managing Director
<b>Signed:</b>		<b>Signed:</b>	

<b>Date of Issue:</b>	08/09/2020	<b>Review Date:</b>	2020
<b>Reference No.:</b>	Information Security Policy	<b>Version No.:</b>	1.0
<b>Supersedes:</b>	0		

<b>Amendment No.</b>	<b>Section No.</b>	<b>Page No.</b>	<b>Paragraph No.</b>	<b>Date</b>	<b>Amended By</b>
1.0				8/9/2020	j.lovesey

---

---

## CONTENTS

<b>1. ELECTRONIC COMMUNICATION &amp; SOCIAL MEDIA USAGE POLICY</b> .....	<b>4</b>
1.1. PURPOSE OF THIS POLICY.....	4
1.2. OVERALL COMPUTER USE.....	4
1.2.1. Password Security.....	4
1.2.2. Computer Usage.....	4
1.2.3. Guest Access Wifi.....	5
1.2.4. Laptop Security.....	5
1.2.5. Virus & Malware protection Software.....	6
1.2.6. Maintaining PCs.....	6
1.2.7. Software Licensing and Copyright.....	6
1.3. COMMUNICATION.....	7
1.3.1. TELEPHONE / MOBILE USAGE.....	7
1.3.2. Mobile phones and driving.....	7
1.3.3. E-mail content.....	7
1.3.4. Internet Use.....	8
1.3.5. Social Media websites at the workplace.....	8
1.4. MONITORING COMMUNICATION.....	8
1.4.1. Purpose of monitoring.....	9

## 1. Electronic communication & Social media usage policy

This policy sets out rules relating to the use of the Company's computer, and telephone facilities, including Company laptops and mobile telephones. It applies to all users of the Company's telecommunications systems, whatever their employment status, and whether used at or away from the workplace. Any breach of this policy will be taken seriously and may lead to disciplinary action, which could include summary dismissal under the Company's Disciplinary Procedure. If you are unclear about the effect or meaning of any part of this policy, you should seek clarification from your Manager or IT Department before you use the computer or telephone system. This policy may be changed from time to time at the discretion of the Company. This Policy is applicable to all J&E Hall Limited Business units, subsidiaries & personnel (ADC, C&P, DAPS)

### 1.1. Purpose of this policy

The purposes of this policy are:

- to ensure that computer, and telephone resources are used properly;
- to establish clear rules on the extent to which you may use e-mail, Internet, and telephone facilities (both in the office and remotely) for personal use; and
- To ensure staff are aware of our GDPR Policies and procedures
- to inform you that monitoring will take place and the reasons for it.

### 1.2. Overall Computer Use

#### 1.2.1. Password Security

Your Windows password is issued by the IT Department and should not be altered without their express permission.

- Do not tell anyone your password
- Do not use another person's password or workstation without prior authorisation from their BU Manager / IT Manager
- You must log out of your terminal when it is not in use, there is an automated lock screen timeout function that meets current security guidance.

#### 1.2.2. Computer Usage

The Company's computers, including laptops, are to be used solely by employees for business purposes, subject to the following exceptions:

- you may make reasonable/limited use of the Company's computer system for sending personal e-mails (outside of your normal working hours or during your lunch break) in accordance with the terms of this Policy;
- you may use the Internet for reasonable/limited personal use (outside your normal working hours or during your lunch break) in accordance with the terms of this Policy
- personal use should not interfere with the performance of your duties or take priority over your work responsibilities;

---

In utilising the above exception you should not carry out any actions that cause sustained high volume network traffic that substantially hinder the normal use of the network by other users or disable / overload the Company computer systems or network. Examples of this include Streaming of TV / Radio programs

### 1.2.3. Guest Access Wifi

The company may provide access to a Guest Wi-Fi network at its sites. The company monitor's traffic in the same way as over our Corporate Wi-Fi and all policies and processes that apply to Company devices apply to Personal / Third-Party devices connected to our Guest Wi-Fi network.

You may provide the Guest Wi-Fi password to visitors, but this should only be for the benefit of the Company.

Under no circumstances should any guest device be connected to the corporate network, whether it be mobile or laptop.

### 1.2.4 Laptop Security

- Devices that are easily portable such as Laptops or Tablets (Mobile Devices) should not be left unattended in the office or workplace overnight (including weekends and holidays) they are the responsibility of their allocated owner and should either be in their possession or if left on-site then in a locked drawer or cabinet out of sight.
- Do not leave your password notes in your laptop bag, on your laptop, or near the device.
- When staying away overnight on business mobile devices should be stored in a hotel room safe where available rather than left unattended in a hotel room, if not possible it should be kept out of sight from windows etc
- Devices should not be left unattended in a parked vehicle unless there is no other option. They should be locked in the boot or out of sight while commuting. They should not be left in a vehicle overnight.
- Mobile devices are provided for business use by authorised employees. Devices must not be loaned or be allowed to be used by others, this is to prevent any unauthorised software being installed and / or inappropriate web access.
- Tracking or mobile device management software installed on the device must not be removed.
- Stolen devices must be reported to the police within 24 hours, the incident report number is to then be given to the IT Department and HR Department.
- Devices provided with protective casing should remain in the cases at all times (mobiles, tablets)
- Do not store USB or backup USB data within the same bag as the laptop. As this creates the risk of you losing both data sources at once.
- Always encrypt a USB pen before transferring or saving confidential data onto it.
- When at any public location, on plane / train, in a coffee shop, use your privacy screen, when this is not possible, be vigilant when logging in in case someone is looking over your shoulder.

---

### 1.2.5 Virus & Malware protection Software

Your computer is provided with virus protection software. This is pre-configured to be regularly updated. You should not remove, tamper or modify this software without prior authorisation from the IT Department. We also have other security applications to protect our infrastructure,

You should be aware that viruses can be introduced via e-mail attachments, the Internet and external storage devices (such as CDs, DVDs and memory sticks, etc). It is your responsibility to take care when opening e-mail attachments, especially when they are not expected, or they are from unknown sources. The last form of our defence system is you, the user, our systems cant eliminate all threats. You should be alert to malicious e-mails being represented as legitimate using familiar names. If in any doubt you should contact the IT Department, who will advise whether it is safe to open the attachment.

### 1.2.6 Maintaining PCs

The Company systems are installed according to internal rules and standards. This standardisation enables IT to manage computers more efficiently as each PC has been setup using a common platform. Occasionally software updates will be deployed and will require authorisation to install, you must approve these updates to ensure your machine functions efficiently.

You should not repair, modify, tamper or upgrade a Company computer or laptop without prior authorisation of the IT Department.

You must not refuse any reasonable request by the IT Department to inspect your computer or laptop in order to audit the software licenses or verify your e-mail or internet activity.

### 1.2.7 Software Licensing and Copyright

There are strict regulations on intellectual property rights on software. To avoid severe penalties and to respect the creator of software, it is important that we use software according to its licensing conditions.

Any software required should be requested and approved by the IT department. We use 3rd party applications that verifies if software to be installed is safe and has appropriate license agreement.

Any free trial software is to be uninstalled or removed at the end of the period or an appropriate license is to be purchased. Evidence of such purchases should be recorded and kept for subsequent inspection and software audit.

You should not download any material, including games and screen savers, or make any changes to software without prior IT department approval.

## 1.3 Communication

### 1.3.1 Telephone / Mobile usage

You are permitted to make occasional/reasonable private telephone calls during your lunch hour or outside of working hours. The following types of personal calls are never permitted:

- calls to premium lines,
- calls to chat lines,
- directory enquiries.

Calling home to the UK when working overseas is permitted but calls must be kept to a reasonable minimum and costs will be monitored.

Mobile telephone contact lists are the property of the Company. Employees are not authorised to give the mobile phone numbers of any colleague to a third party without the express permission of the mobile phone user, except for legitimate business purposes (i.e. a sales lead etc)

Monthly usage is checked for excessive costs or usage, if it is seen to be above the corporate average it could be highlighted with your line manager who will check the logs and will raise it accordingly with you.

### 1.3.2 Mobile phones and driving

It is a criminal offence to use a hand-held phone or similar device when driving. As a result, you are forbidden from using a hand-held mobile in a moving vehicle whilst driving on a Company or private vehicle.

Please refer to the company "Vehicle Policy" for full details on mobile usage while using a company vehicle.

### 1.3.3 E-mail content

When sending e-mails, internally or externally, you must not send, forward, distribute or retain e-mail messages that contain language that is abusive, aggressive or offensive. You must not make any improper or discriminatory reference to a person's race, colour, religion or belief system, sex, age, national origin, sexual orientation, disabilities or physique when writing e-mails and must not forward or distribute any material which does so.

We have a send and receive attachment size limit of 30mb this is to reduce the email storage requirement and to also reduce network utilisation and slowness.

It is a requirement that the Company disclaimer must be included at the foot of every e-mail sent using the Company e-mail address, on both business and private messages. Under no circumstances should it be altered. Employees should not use personal e-mail addresses to send e-mail for business related correspondence.

E-mail is not a secure way of sending information. It is a requirement under the Data Protection Act that you take measures to ensure there is no unlawful processing or loss of personal data. Any document containing employee personal information, or commercially sensitive information should be encrypted by way of password protecting the documents.

The use of Shared Mailbox's, where practical, is encouraged for customer / supplier correspondence. This will ensure data is readily accessible in a GDPR compliant manner should you leave the company.

Please ensure you have read and are familiar with the "General Protections Regulations Policy" and "Procedures" located on Cascade. The policy is based on laws and regulations related to personal data protection in the EU and the UK, and prescribes the basic rules to be complied with by Employees of the Company when processing personal data

#### 1.3.4 Internet Use

You are reminded that the Internet is a public forum where it is inappropriate to reveal confidential Company information, customer data, trade secrets and any other material covered by existing Company secrecy policies or procedures.

The Company retains the copyright to any material posted to any forum, newsgroup or World-Wide Web page by any employee in the course of his or her duties.

Internet browsing is tolerated during break and lunchtimes

We have systems in place that monitors and content checks website access, you must not, under any circumstances, access inappropriate or offensive Web sites or distribute or obtain similar material through the Internet or e-mail when using Company equipment, even if you are doing so in your own time. Examples of inappropriate or offensive material include racist material, pornography, sexually explicit images, text and related material, the promotion of illegal activity or intolerance of others. Inappropriate web sites include those related to gambling and betting.

You must not download games or entertainment software or music files (including iTunes). You should not play games against opponents over the Internet.

#### 1.3.5 Social Media websites at the workplace

The Company has the final decision as to whether it considers particular material to be inappropriate under this Policy. If you are unsure whether particular material would be considered appropriate by the Company, you should seek clarification from the IT Department before accessing or distributing such material. Or, if in any doubt as to whether the Company would consider certain material inappropriate, do not access or distribute it.

If you receive material which contains, or you suspect contains, inappropriate material or you access such material on the Internet inadvertently, you must immediately report this to the IT Department who will tell you what to do. You must not under any circumstances forward, show to anyone else, or otherwise distribute the material.

#### 1.4 Monitoring communication

Auditing and excessive usage

The Company may log and audit use of communication systems, including Company telephones, mobile telephones, land lines provided by the Company, Computers, including e-mail, Internet and other computer use.



---

In particular, all calls from all extensions, and lines provided by the Company and from Company mobiles are logged and regularly audited. Auditing software has also been installed which will monitor e-mails being sent and received. The Company may deploy software and monitoring equipment to record any Internet sites visited.

Where it has good cause, the Company may monitor and record the contents of telephone calls, voice mail messages, computer files and Internet use and e-mails sent, received and stored. You should not regard either business or personal communications on the Company's facilities as private subject to GDPR

#### 1.4.1 Purpose of monitoring

The purposes of such logging, auditing, monitoring and recording are to:  
ensure the effective operation of the Company's telecommunications systems and to maintain system security;

- investigate and detect unauthorised use of the systems in breach of Company policies and Data Protection Regulations, such as excessive personal use or distribution of inappropriate material;
- monitor employees' standards of performance;
- check whether matters need to be dealt with in your absence;
- investigate allegations of misconduct, breach of contract, a criminal offence or fraud by the user or a third party;
- pursue any other legitimate reason relating to the operation of the business,
- comply with any requests from law enforcement and regulatory agencies for information about your e-mail or Internet activities.