**VEEVE Social Media and Computer Usage Policy**

1: Computer Security

Set out below is Veeve’s Computer Security Policy relating to computer equipment and information. You are responsible for ensuring that these rules are adhered to. Any breach of these rules may result in disciplinary action being taken against you including, in serious cases, dismissal without notice or pay in lieu of notice.

You agree we may take all actions necessary to ensure our Computer Security Policy is adhered to.

All PCs and related computer hardware, including printers, are considered corporate assets and are the property of the Company (not individuals, departments or projects).

Leavers' network accounts will be disabled and the contents of personal drives and email accounts made available to the Line Manager and/or any employee deemed by the Line Manager to require access for an agreed period, before being archived from the network.

Hardware must only be installed or uninstalled into any PC by IT. No user will open a PC to attempt to repair it. This act may contravene applicable Health and Safety regulations and could invalidate any warranty on the hardware.

Security

As all information regarding our business interests is strictly confidential, all computerised information should be securely managed within the Company.

You should treat electronic information with the same care that you would any written documentation. In particular:

1. Appropriate security levels should be set on all documents within the computer system. If a document is highly confidential, or contains price-sensitive material, then access should be limited to the specific individuals who have good reasons to use the document.
2. Great care should be taken in transmitting documents electronically.
3. Portable computers containing confidential information should never be left unsecured or unattended when off-site or elsewhere.
4. Information about the Company, including details of our financial affairs and future operational plans, is highly confidential. Much of this information is available to authorised employees via the computer system and should not be made available to anyone outside the Company.

Unauthorised Access

There are a number of security measures built into the computer system to prevent unauthorised access to our systems and data. They are designed to provide a high degree of security against external attack or intrusion (for example, malicious hacking or computer viruses). However, these formal security measures will only be effective with your full co-operation and support.

Specifically, it is important that all employees respect the following at all times:

1. Never disclose your password to anyone else. If you think that your password has been compromised, you should take appropriate measures to change your password immediately and, if appropriate, inform your Line Manager.
2. Log off and switch off your computer workstation at the end of each day. Remember that a workstation logged onto the computer provides a means of access to all your files.
3. Lock your computer when you leave it unattended.
4. Passwords should be complex and contain letters and numbers and should not be a normal word or name. Passwords should be at least seven characters long.
5. Software of any kind must not be loaded onto a workstation or run without authorisation from IT as this may disrupt our existing systems and could also contravene the software licence.
6. No attempt should be made to by-pass the existing security measures.

Software

We use software from a number of different suppliers and make every effort to comply with the obligations of our licensing agreements. You are obliged to respect the following:

1. Software must **never** be copied from or to any of the Company's computers, including portable computers. This includes transfer to, discs/CDs/DVDs, or onto hardware devices (such as PDAs, portable memory, memory sticks, and other USB-type devices) or via email.
2. Software licensed to the Company must never be used outside the Company without specific written authorisation.
3. You must not download additional software from the internet or install it from discs/CDs/DVDs without authorisation from your Line Manager or IT department, including downloading or installing screensavers, desktop wallpaper, games, pirate copies, etc.

2: Email and Internet

Email Policy

Our email facility is intended to provide effective business communication within Veeve, and externally with clients and customers. While there are many advantages to be gained from the correct use of internal and external mail, there are also certain dangers.

When sending internal or external emails, please ensure that you comply with the following:

1. If you receive an email that has been incorrectly delivered to your email address, you should notify the sender of the message by re-directing the message to that person. If the email contains confidential information, you must not disclose or use that information.
2. Emails should be checked thoroughly before sending (including checking that they have been properly addressed), using the same care you would give to a formal letter on the Company's letterhead.
3. You must not impersonate any other person when using email.
4. You must not amend messages received and then store, print or forward as if they were received in the altered state.
5. Be aware that legally binding contracts can be formed by email.
6. You are allowed to use the email facility for personal reasons as long as it does not interfere with your work-related responsibilities.
7. General personal messages to a large number of addressees must not be sent.
8. Do not use internal or external emails for any material that could potentially be defamatory (for example, containing untrue, malicious or otherwise inappropriate statements about our customers, competitors or other employees).
9. Do not respond to "Junk Mail" or warnings to new email viruses.
10. Do not send 'fun' or 'flame' emails; what may seem harmless fun to some can be offensive to others and may be regarded as harassment. If you receive an email which you consider offensive, you should raise the issue with your Line Manager. The Equality Act 2010 prohibits discrimination and harassment because of age, disability, gender reassignment, marriage and civil partnership, pregnancy and maternity, race (including colour, nationality and ethnic or national origins), religion or belief, sex or sexual orientation.
11. Do not respond to, or forward on, chain letter-type emails.
12. Do not disclose information that is protected by embargo or could in any way be considered confidential to the business and/or the employees.
13. Do not make any statements via email which intentionally or unintentionally create a binding contract or make negligent statements.
14. Do not initiate or forward emails that contain obscene, pornographic and/or offensive material.
15. If you are sending out attachments by email, please ensure that you have obtained the consent of the author of the attachment if they are not an employee; otherwise you may infringe the author's copyright.
16. Bear in mind that, in some cases, recipients can view previous changes to attachments.
17. Never import unknown messages, files or attachments onto your system without authorisation.
18. Do not send large graphic files unless they are related to the Company's business.
19. You must ensure you log off your computer workstation if leaving it for any length of time. You must change your personal password regularly and never disclose it to others.
20. Please remember that we have the authority and ability to intercept, read and print out all internal and external (incoming and outgoing) emails, including those marked 'personal'. Communications of a sensitive or confidential nature should not be sent by email because they are not guaranteed to be private.
21. You agree that we may take all actions necessary to ensure our Email Policy is adhered to. We reserve the right to open any email file.
22. All emails that are sent to external recipients will carry disclaimers and other information that is required by law to be attached to Company correspondence. Delivery of external emails depends on third parties and is via the internet. At times, internet communication networks fail and may result in emails going astray, being delayed or lost. Sending an email does not guarantee its delivery, and delivery does not guarantee that it will be read. If your message is urgent and/or important, make sure that the recipient is aware that you have sent the message by phoning him/her, or asking for a reply, or making use of the message tracking options available in Microsoft Outlook.

The purposes for which we may intercept, read and print out emails include, but are not limited to:

1. Promoting productivity and efficiency.
2. Ensuring there is no unauthorised use of the Company’s time.
3. Ensuring that all employees are treated with respect and dignity at work, by discovering and eliminating any material that is capable of amounting to unlawful discrimination or harassment.
4. Ensuring the security of the system and its effective operation.
5. Ensuring there is no breach of commercial confidentiality.

Personal emails which are clearly marked as such will only be read in exceptional circumstances where a problem relating to an employee’s excessive, inappropriate or when unauthorised use is suspected.

The Procedures, as set about above, are of critical importance. Non-compliance or breach of this Email Policy will be viewed as misconduct and may result in disciplinary action being taken against you including, in serious cases, dismissal without notice or pay in lieu of notice.

Internet Usage Policy

Internet access, including internet email, is provided to employees for the purpose of conducting business-related activity for the benefit of the Company and its clients. Since our IT resources are costly and require significant work to maintain, it is important that you adhere to the Internet Usage Policy, thus ensuring these resources are available to everyone for legitimate, business-related purposes.

Please remember that we have the authority and ability to access, read and print out details of all internet sites and emails sent/received accessed by persons using our computer systems.

Personal use of the internet should be minimal, and in any event should not be used in a manner that:

1. Interferes with your work-related responsibilities.
2. Is offensive to others.
3. Burdens or degrades any of the Company's systems or network resources.
4. Threatens the security of the systems.
5. Allows unauthorised access to the systems.

The Company reserves the right to restrict or deny access to any websites. This might include networking or video sharing websites such as Facebook, MySpace, Bebo, Twitter and YouTube. This does not apply to business use of the sites.

Logging on to sexually explicit, gambling or any other inappropriate websites is prohibited. Should you visit inappropriate websites unwittingly through unintended response of search engines, unclear hypertext links, misleading banner advertising or mis-keying, you must exit immediately and inform your Line Manager of the incident.

When logging on to and using any web site for any purposes, including social networking, video-sharing websites and blogs (even from your own equipment), you must not:

1. Conduct yourself in a way that is detrimental to Veeve or brings it into disrepute. Bear in mind that you may be identified as working for the Company even if you do not overtly state that.
2. Allow interaction on these websites or blogs to damage working relationships between employees and clients of Veeve.
3. Include personal information about our employees, suppliers, customers or clients without their express consent (you may still be subject to disciplinary action even if employees, suppliers, customers or clients are not expressly named in the websites or blogs as long as we reasonably believe they are identifiable).
4. Make any derogatory, offensive or defamatory comments about the Company, our employees, suppliers, customers or clients (you may still be subject to disciplinary action even if the Company, our employees, suppliers, customers or clients are not expressly named in the websites or blogs as long as we reasonably believe they are identifiable).
5. Disclose any confidential information belonging to us or our suppliers, customers or clients, or any information which could be used by a competitor.

Breach of this internet Usage Policy will be viewed as misconduct and may result in disciplinary action being taken against you including, in serious cases, dismissal without notice or pay in lieu of notice.

The law with regard to email and internet access and use is still evolving. This policy takes into account the current legal situation but you should be aware that it will continue to change, often at great pace. For this reason, you will be notified of any changes and you must ensure you update yourself regularly with the current version of this policy.

Virus Protection Procedures

In order to prevent the introduction of virus contamination into the software system, the following must be observed:

1. Unauthorised software (including public domain software, magazine cover discs, CDs or internet/WorldWideWeb downloads, etc.) must not be used.
2. All software must be virus-checked, using standard testing procedures, before being used.

Breach of these Virus Protection Procedures may result in disciplinary action that may lead to dismissal.

Usage

These Policies are designed to prevent problems with email and internet usage, and, you are therefore expected to be familiar and comply with the contents of the overall Social Media Policy. If you are unsure about whether anything you propose to do might breach this Policy, you should speak to your Line Manager.

Breach of this Policy will be viewed as misconduct and may result in disciplinary action being taken against you. This could include your access to our email facilities and the internet being suspended or withdrawn, or, in serious cases, dismissal without notice or pay in lieu of notice.

IT Purchasing

All IT related purchasing must be carried out by IT. This includes (but is not limited to) requests for PCs, Macs, laptops, printers, other peripherals, memory and other components, software and other IT related Services. We will discuss your requirements with you, give selection and purchasing advice and seek authorisation. Once the authority to purchase has been received, we will order the items, configure them for you and, during their economic life, support them.