HR Policy

LEYLAND TRUCKS
A PACCAR COMPANY

Subject:	Policy Number: 1.5	
USE OF COMPANY E-MAIL, INTERNET/INTRANET FACILITIES	Date: 17/10/2008	Page 1 of 5
	Policy Issue Number: 4	

1. **PURPOSE**

1.1. This Policy provides strict guidelines on the permitted use of Company internal/external electronic mail systems and Internet/Intranet usage.

2. **SCOPE**

2.1. This Policy applies to all employees of Leyland Trucks Ltd and PACCAR Parts UK.

3. **RELATED POLICIES**

3.1. PACCAR Standard Policy SP28 – Electronic Communication

3.2. Leyland HR Policy 1.4 – Personal Computers and Software

4. **DEFINITIONS**

4.1. 'Information' or 'communication' is defined as including text, images, video, sound, computer programs and data files.

4.2. 'E-mail' is defined as electronically transmitted information, communication, fax, or material, internal or external to the Company sent to any third party or other entity, organisation, physical location or e-mail address.

4.3. 'Internet' is defined as any system external to the Company network.

4.4. 'Intranet' is defined as any internal system available for use within the Company.

5. **GENERAL PRINCIPLES**

5.1. To ensure equipment is used only for proper business usage and to minimise the risk to the Company, such as unauthorised access to Company systems, corruption of programs or data the following guidelines apply:

5.1.1. Requests to the IT Department for Internet services beyond general browsing must be in writing and include a statement of business benefits and be approved by the respective Functional Head.

5.1.2. Internet access during working hours is restricted to Company business purposes only. Internet access is allowed during breaks and lunchtime but only within the confines of PACCAR policy SP28.

5.2. All Internet access must use Company provided Software and hardware and be through a secured Company Internet gateway approved by the IT Department.

5.3. Any Internet or Intranet activity, including e-mail, may be monitored and recorded by the Company without notification. Random audits of files and data on Company computers may be actioned at any time.

5.4. Any communication, transmitted or displayed electronically, must comply with UK and European legislation and the Company's policies and its content must not be harassing, obscene, defamatory, or offensive.

5.5. Information must not be transmitted or displayed electronically which could bring the Company into disrepute or which contravenes any laws of the receiving location, including Discrimination Legislation as defined in the Equality Act 2010. Employees must therefore only e-mail what would be seen as acceptable by third parties.

5.6. Employees must not transmit any information by e-mail over the Public Internet which is confidential or proprietary. If there is a compelling business case to do so files must be encrypted. In the case of proprietary information the appropriate legal owner's permission must be obtained. The relevant provisions of SP21 'Protection of Confidential Information and Trade Secrets' applies.

5.7. Requests by non-PACCAR employees to use Company e-mail or Internet/intranet facilities must be pre-authorised by the senior functional manager who should satisfy herself/himself that usage will not breach the provisions of this policy, (see section 8). A User Access Request Form should be completed.

5.8. Further information may be found in the Company's Guide to Using the Computer Infrastructure and apply the conditions of use and limitations specified within.

6. E-MAIL USAGE GUIDELINES

6.1. Access to and usage of Company e-mail resources is governed by these guidelines and the general principles stated in section five of this policy.

6.2. The Company's e-mail link to the Internet is protected to prevent anyone accessing Company computer systems from the Internet. E-mail through the Internet cannot be assumed to be a secure form of communication.

6.3. There is a risk that what is sent or received could be intercepted and seen by others. The actual likelihood of the communication being intercepted is relatively small but misdirection's are not uncommon. Accordingly when information is deemed to be of a potentially confidential or sensitive nature all parties should be made aware of the security implications of e-mail transmissions and the use of e-mail should be agreed with all parties concerned prior to use.

6.4. E-mail is often wrongly assumed to be a less formal medium; it is important to realise e-mails are legally held to be Company documents with the same status as written or letter-headed communications. Normal standards of professionalism through use of e-mail must therefore be maintained.

6.5. Passwords must not be sent by e-mail, especially passwords for documents that are also being sent by e-mail. If it is not possible to avoid emailing a password, a following email should be sent which should be restricted to the recipient, with no obvious reference to what the password is for in the email.

6.6. Passwords are confidential information. Do not print, display, or share your password.

6.7. Increasingly, E-mails are being received that are malicious in nature and generally termed Phishing emails. They may come from email addresses that appear to be legitimate and look very authentic, especially at first glance. Be on guard for any unexpected or unsolicited emails, asking you to take action often with a sense of urgency. These actions may include prompting you to open an attachment, click on a link, provide personal information, verify username and password or transfer funds.

6.8. In summary, employees must always be aware of the security and confidentiality issues surrounding e-mail. Check the Intranet for the latest guidelines; the Company's reputation depends on all employees taking such issues seriously.

7. INTERNET USAGE GUIDE

7.1. Access to and usage of the Internet is governed by these guidelines and the general principles stated in section five of this policy.

7.2. The Internet is an electronic worldwide and largely unregulated public domain arena containing information resources, commercial activities and advertising of every conceivable type. This reflects the full range of human activities which

inevitably will attract a small minority who will use this medium for illegal, subversive and/or immoral activities.

7.3. The Company has good malware protection, but viruses can be created that cannot be detected. If there is a need to download any file from the Internet it **must** be virus checked prior to use. The local LAN administrator can assist employees with this task. Any unsolicited documents or attachments received from unknown sources must be deleted, unopened,

7.4. Accordingly, employees authorised to access and browse the Internet for genuine business reasons must, with the above in mind, take care at all times that they:-

7.4.1. Only view web sites or other information sources that would be considered appropriate for their business needs do not enter into any commercial transactions on behalf of the Company, or commit the Company to any liabilities without permission from a senior manager

7.4.2. Do not register their own or the Company's details without the express permission of a grade '15 and 16' Manager

7.4.3. Any accidental viewing of inappropriate web sites should be recorded and reported to the appropriate Line Manager as soon as practicable (all sites visited are recorded by the Company).

7.4.4. Observe normal business courtesies and maintain a high professional image of the Company when interacting on any web site or while connected to any area of the Internet.

8. INTRANET USAGE

8.1. The Company operates an internal Company computer network and throughout the PACCAR organisation worldwide. Electronic communication facilities are available internally and accordingly all general principles in section five and E-mail Usage.

8.2. Guidelines in section six of this policy apply equally to intranet electronic transmissions of information or communication.

8.3. The Company's computer networks are provided for the efficient running and management of business software applications, inter-company communication and sharing access to various Company data.

8.4. Any disruption or damage to these systems or the operating system software or loss of Company data could have very serious consequences for the Company's operations. Therefore employees are required at all times to:-

8.4.1. take care in using and actioning transactions using the network.

8.4.2. only attempt to access unrestricted 'public' designated areas of the network or those areas required to carry out their specific work responsibilities.

8.4.3. respect the privacy of other employees' files and folders by not attempting to gain access, reading, copying, pasting, editing or moving others files or folders.

8.4.4. only use internal e-mail facilities and other electronic messaging systems for business use. Private and personal communications across the internal network are not permitted.

9. MANAGEMENT RESPONSIBILITY

9.1. It is part of all Managers' responsibility to ensure all staff in their departments are aware of the provisions of this policy and take any practical steps to ensure compliance. Furthermore any instances or suspicion of improper use of Company e-mail or Internet facilities by customers, suppliers, contractors or visitors should be brought to the attention of senior management as soon as possible.

10. POLICY ENFORCEMENT

10.1. Violation of this policy may result in disciplinary action. This may include dismissal in cases of very serious and/or persistent breaches of this policy.

FURTHER INFORMATION

Further information can be obtained from the Human Resources Dept.

This document is non-contractual unless otherwise stated.