

It is the policy of Morrison Homes to attempt to ensure that its computer facilities and systems are operated and used in conformance with all laws and regulations and all Company policies governing appropriate standards of conduct. This policy is intended to set forth standards for appropriate use of the Company's computer facilities and systems. Violation of this policy is a serious matter which may result in disciplinary action. Questions concerning this policy should be directed to the Company's Information Systems Department or the Vice President of Human Resources.

System Resources

- All of the Company's computer facilities and resources, including hardware, software, network systems and data, are the property of the Company and may be used by employees only in connection with their employment. Except as set forth in this policy or other guidelines distributed to employees, personal use of the Company's computer systems is expressly prohibited.
- In order to maintain the integrity of the Company's computer systems and in order to avoid support issues, all computer applications and software used in connection with the Company's computing systems must be purchased and installed by or under the direction and supervision of the IS Department. Employees may not install applications or software, or modify existing applications or software, without the approval of the IS Department. Without limiting the foregoing, computer games and free software may not be loaded or used on any Company PC.
- All computer applications and software used in connection with the Company's computing systems must be properly licensed for use by the Company and its employees. Employees may not install or use unlicensed applications or software on or in connection with the Company's computer systems. Employees must abide by all licensing agreements entered into by the Company. In order to ensure compliance with licensing laws, employees may not install Company-owned or licensed software on their own personal computer equipment without written approval by the IS Department.
- Employees may "sync" personal digital assistants (PDA's) to Company-owned computers, provided that the device is based upon Palm OS technology (the Palm operating system). The Company IS Department will not, however, support such use, except for handheld devices issued by the Company to construction personnel. (Questions regarding the use of PDA's in conjunction with the Company's computer system should be directed to the IS Department's Help Desk.)

Personal Use

The Company recognizes that limited personal use of the Company's computer facilities by employees is appropriate in certain circumstances and may in fact promote increased employee productivity (for example, use of e-mail in lieu of personal telephone calls, use of e-mail to contact schools or child-care providers, or use of certain Internet services). Employees must, however, exercise reasonable judgment in utilizing the Company's systems for personal purposes and should not abuse the privilege of being permitted to use such systems. While no strict rule can be enunciated, employees are expected to limit personal use to appropriate circumstances and

times. Use of Company computer facilities and resources should not interfere with an employee's job performance, and employees must abide by this policy and all other guidelines and procedures even when their use of the Company's computers is for personal purposes. Employees who receive unwanted or unsolicited e-mail that violates this policy or any other Company policy must take reasonable steps to cause the cessation of such e-mail. The Company reserves the right to revoke an employee's permission to use the Company's computer systems for personal use.

Security and Passwords

Computer security is the responsibility of every employee. Employees should keep proprietary and confidential information confidential and should exercise reasonable care to protect the integrity of the Company's computing systems.

- Network user names are unique to each employee and are for the exclusive use of the specific employee.
- Individual passwords should be unique and should be maintained as confidential. Passwords should not be divulged to any other person and should be changed regularly.
- Network passwords should be maintained as confidential. (If an employee needs access to another employee's files or data, the local Division Controller or the IS Department may grant the employee appropriate access to the other employee's directory.)
- When appropriate (for example, an employee's computer is accessible to non-employees or the employee is accessing highly confidential information), employees should log off from any password-protected system whenever they leave their PC unattended.
- All employees should log out of the network every night.
- All laptop computers should be locked away securely every night.
- Employees should not attempt to repair or otherwise modify their PC's.
- All important data files are to be stored only on the network server.

E-Mail

- The Company's e-mail system is intended for Company business. Except as set forth in this policy or other guidelines concerning computer use that are distributed to employees, personal use of the Company's e-mail system is expressly prohibited.
- Even though e-mail is generally perceived as an informal means of communication, its effect is the same as any other written document and it should be treated in the same manner as formal correspondence on Company letterhead.
- It is the policy of the Company not to discriminate against any employee on the basis of race, religion, national origin, ancestry, sex, age or physical disability. It is also the policy of the

Company to maintain a workplace that is free of discrimination and intimidation in any of these areas. Without limiting the foregoing, it is the specific policy of the Company to provide all employees with a work environment free from sexual harassment. Accordingly, any e-mail communications that are or may be considered offensive, obscene, discriminatory, racist, sexist or which otherwise infringe upon or violate this policy or any other Company policy or guideline are strictly prohibited.

- Chain e-mail messages, either internal or external, are strictly prohibited.
- The transmission of video attachments or other attachments that utilize significant memory for a non-business purpose is strictly prohibited.
- All computer users should exercise extreme care when opening e-mail from an unknown or unsolicited source. Attachments from an unknown source should never be opened.
- Global e-mails may be sent only with the permission of the IS Department.

Internet Usage

- Access to the Internet by Company employees using the Company's computer facilities is strictly controlled and based on business need. Authority for access will be controlled by local Division management with the concurrent approval of the IS Department.
- Employees are granted access to the Internet for the purpose of conducting Company business. Except as set forth in this policy or other guidelines concerning computer use that are distributed to employees, personal use of the Company's computer systems for Internet access is expressly prohibited.
- It is the policy of the Company not to discriminate against any employee on the basis of race, religion, national origin, ancestry, sex, age or physical disability. It is also the policy of the Company to maintain a workplace that is free of discrimination and intimidation in any of these areas. Without limiting the foregoing, it is the specific policy of the Company to provide all employees with a work environment free from sexual harassment. Accordingly, any use of the Internet that is or may be considered offensive, obscene, discriminatory, racist, sexist or which may otherwise infringe upon or violate this policy or any other Company policy or guideline is strictly prohibited.

Screen Savers and Wallpaper

The Company installs uniform wallpapers and screen savers on Company PC's. Employees may not remove, replace or modify these wallpapers and screen savers.

Virus Protection

The Company has installed virus detection software on all of its PC's and servers. If an employee suspects that his or her PC has been exposed to or infected with a computer virus, the employee should contact the IS Department Help Desk immediately. (Employees should not notify other employees by e-mail.)

Protection of the Company's computer systems from viruses is the responsibility of every employee. Employees should exercise reasonable care to avoid undue exposure of the Company's computing systems to attack from external viruses. All computer users should exercise extreme care when opening e-mail from an unknown or unsolicited source, and attachments from an unknown source should never be opened. Employees should avoid opening chain e-mail messages, "joke" e-mail and any other e-mail that may create additional exposure to viruses.

Ownership; Lack of Employee Privacy

The Company's e-mail system and the information transmitted on the system belong to the Company. All e-mail messages created or stored on the Company's computers or networks are the property of the Company and are not considered private. **The Company reserves the right to and does in fact scan and monitor e-mail. In addition, all pages accessed on the Internet are logged and these logs are periodically reviewed** to identify any misuse of the Company's computer systems by Company employees. Without limiting the foregoing, all attempts to access certain specifically prohibited sites are logged and are reported to local Division management for appropriate action.

Violations of Computer Use Policy

Employees who violate this Computer Use Policy are subject to appropriate disciplinary action, up to and including immediate discharge for cause.

Acknowledgment of Computer Use Policy

All employees are required to acknowledge in writing that they have read this policy and understand it and that they agree to comply with its provisions. All new employees will be required to sign a similar acknowledgment at the time of their employment. The Human Resources Department shall adopt and implement appropriate procedures to obtain such acknowledgments.