



| Policy Document | |
|---|--|
| Title: IN R/CCC EO Cell Phone and Internet / Computer Use Policy | To: Maximus Employees and Contractors |
| Department: Human Resources | Effective Date: July 8, 2022 |
| Revision Time Period: Annually | Version Number: 1 |
| Revision History | |
| Version | Approved Date and Reason |
| 1.0 | July 8, 2022 – Initial Release |

Cell Phone Guidelines

The use of cell phones is prohibited during the work schedule or in work areas by both Maximus and non-Maximus employees (contractors). Ringers must be turned off and phones should not be visible in the work area during scheduled work hours. The use of all functions of cell phones including phone, texting, camera, and internet are prohibited in work areas and during scheduled working hours. Limiting the use of wireless phones at work will help productivity and help fulfill the Maximus quality principle of “maintaining excellent customer relations” by eliminating potential distractions. Limiting cell phone use is also intended to meet Maximus and client security requirements regarding protection of client and project information.

In addition to your personal cell phone, the following items are not allowed in the work area:

- Personal Laptop
- Kindle/Nook/iPad/Handheld Games
- Other devices deemed by management to interfere with job responsibilities

Note: All employees (up to and including Supervisor/Management level) must not utilize any of the USB ports on work on computers or in work areas. For example, do not plug in fans, phones, etc., even if only charging.

Employees will need to use a smart phone for multi-factor authentication (MFA) connection for secure VPN access throughout the day when gaining specific applications and software. We understand that you will need to access your phone when this takes place. In order to comply with this policy phone access limited only to multi-factor authentication (MFA) connection is allowed during scheduled working hours. DFR reserves the right to approve certain operations to work at home. Please adhere to all elements of this policy while working from home.

Unless specifically authorized by Maximus Management, the use of cell phones as cameras is prohibited in compliance with corporate privacy and security policies. The camera feature on cell phones potentially allows images of customer Protected Health Information (PHI) and Personally Identifiable Information (PII) to be released.

Cell phone use for personal reasons can be used during scheduled breaks and lunch periods. This pertains to all employees working remotely or in the office. While working in the office employees are expected to step away from production floor to utilize their cell phone in either the break room or outside of the office. Employees are required to be respectful of others in common areas, refrain from using profanity/inappropriate conversation and speak at a reasonable volume. Cell phones should not be readily accessible (and should be put away) while in the work area.

Project Management may have cell phones accessible or in use in the office, as this may be the primary communication tool for the client or other project partners.

In an extreme emergency, exceptions to this policy will be granted on a provisional basis only. Exceptions must be approved by Project Management. Supervisors or leads cannot approve temporary cellphone exceptions.



Internet/Computer Use Guidelines

All Maximus and non-Maximus employees should exercise care, perform required maintenance, and follow all operating instructions, safety standards, and guidelines when using Maximus and State property. Maximus and State property, including computers and other electronic equipment, is not intended for personal use outside of the employee's job duties.

Please notify your direct supervisor or Project Management if any equipment appears to be damaged, defective, or in need of repair. Prompt reporting of damages, defects, and the need for repairs could prevent deterioration of equipment.

Maximus provides telephones, internet access, and electronic mail to assist employees in performing their jobs. All messages generated on or handled by Maximus electronic communications systems, including back-up copies, are the property of Maximus. Electronic communications systems should be used primarily for business purposes.

Improper use of internet and other computer resources is a violation of company policy. Employees are expected to use the internet responsibly and productively. Downloads or streaming of applications to include data, video, or music will not be allowed. You are not permitted to "save" data, music, or video materials to the computer hard-drive.

Use of any computer station in the building implies consent to monitoring. Employees should have no expectation of privacy in the use of any of the electronic systems owned by Maximus or the State. Users must promptly report all information security alerts, warnings, suspected vulnerabilities, and similar threats immediately to Project Management or Human Resources. Project Management will then forward to Maximus IT and / or Security when necessary.

Failure to comply with this policy will result in disciplinary actions up to, and including, termination following your employer's progressive discipline policies.