FORT SAM HOUSTON CIVILIAN PERSONNEL ADVISORY CENTER

THE ADVISOR NEWSLETTER

April 2022 Volume 15 Issue 2

INSIDE THIS ISSUE:

CPAC Leadership Corner

HR Managers Rethink Their Role During the Corona Virus

By Tonie Case

The Coronavirus pandemic has disrupted all organizations, whether the federal government or private industry. It caused Human Resources (HR) professionals and managers to think differently about their role as they continue to adjust to social distancing practices and a new work environment that they ever have imagined.

To prevent the spread of the virus, many organizations switched to a remote work model at a rate and scale they've never experienced. Routine face-to-face collaboration has been replaced with email and MS Teams video conferencing; as a result, HR professionals have to do complex work under sometimes difficult circumstances.

During this pandemic, until very recent, it was over a year that many of us set a foot back in our offices. A time of upended routines and irregular schedules; of working besides relatives, not colleagues; of learning from experience what words like "virtual" and "MS Teams" and "remote" really mean.

But now, with the pandemic ebbing in the United States, it may soon be time for many of us to return. Some employees-those who enjoyed remote work or found it more practical-may be able to work from home. In contrast, those returning may find offices that are being transformed to serve the emerging needs of both organizations and their employees. Of course, HR managers still realize that efficiency is essential, especially in advising our customers and getting work done for them as quickly as possible. Still, there's an understanding that now an individual has to be thought of in a broader perspective so that there can be growth opportunities. That means more flexibility, more responsibilities, basically more trust all around.

So as a military or civilian manager, whether you are an HR manager or not, what can you do as things continue to change? Here are a couple of things to consider if you want to rebuild those energy levels:

--Check-in with your team members regularly.

--Offer resources such as Chaplin services, Employee Assistance programs.

--Meet employees where they are, depending on your mission. Please make sure that you keep the appropriate safety measures and options in place for them.

--Be flexible. If two years of surprises have taught us anything, we should expect more surprises in the future. That may include new ways of doing business, working, etc.

Paid Paternal Leave

Submitted by Christina Davis

Paid Paternal Leave

Did you know that the Federal Employee Paid Leave Act provides eligible employees with 12 administrative workweeks of Paid Paternal Leave (PPL) in connection with the birth, adoption, or placement of a child? Employees may elect to substitute PPL for unpaid Family Medical Leave Act (FMLA) leave and/or any portion of their available sick and/or annual leave. There is no requirement to use any or all accrued annual and/or sick leave prior to using PPL.

Am I eligible for PPL?

The initial eligibility requirement for PPL is that the employee meets the general FMLA eligibility requirements, including the following:

- Has completed at least 12 months of federal service of a type that is covered under the FMLA Title II provisions.
- Has a part-time or full-time work schedule (i.e., employees with an intermittent work schedule are ineligible).
- Has an appointment of more than one year in duration (i.e., employees with temporary appointments not to exceed one year are ineligible).

The agency may require the employee to provide appropriate documentation it deems necessary to establish that the use of PPL is directly connected to the birth or placement of a child.

When can I request PPL?

PPL is triggered by the birth or placement of a child and therefore may not be used prior to the birth or for placement-related purposes.

The agency will require the employee to provide appropriate documentation necessary to establish that the use of PPL is directly connected to a birth or placement.

Before the commencement of paid parental leave, the employee must agree in writing to work for the applicable employing agency for not less than a period of 12 weeks beginning on the date such leave concludes.

If the employee fails to return for the required 12 weeks of work after PPL concludes, the agency may decide to recover, from the employee, the total amount of any government contributions paid by the agency on her/his behalf to maintain health insurance coverage under the Federal Employees Health Benefits Program during the period(s) when PPL was used. An employee who separates from the agency before completing the required 12 weeks of work is considered to have failed to return to duty.

What happens if I don't use all 12 administrative weeks of PPL?

Entitlement to use PPL will expire at the end of the 12-month period beginning on the date of the birth or placement of the child. If an employee has any unused balance of PPL remaining at the end of the 12-month period following the birth or placement, the entitlement to the unused leave expires at that time. Any unused leave will not be rolled over to use in the future and will not be paid out to the employee.

Supervisors must check their applicable collective bargaining agreement for family leave provisions that may be relevant to each employee's specific situation. For additional information you may contact your Management Employee Relations Specialist.

Hail and Farewell

Delina Melendez

Nakiya Nicasio

Alonzo Soto

Jabriah Stevens

Dora Garcia-Meza

Felicia Hughes (Retired)

Angela Trevino (Retired)

Where is your hometown?
Camden, New Jersey.

Which Branch do you work for?
Branch D.

How long have you been with the CPAC?
One year.

What is your favorite part about working at the CPAC?
Everyone is very helpful.

What is something most people would not know about you?
I love music.

What is it that you do that sets you apart in providing excellent customer service? I don't think it sets me apart, but I just try to communicate and help the customer with what they need the best way I know how.

HATCH ACT 5 U.S.C. 7321

Submitted by Sara Orozco

The Hatch Act, an attempt to regulate corruption and possible intimidation of federal employees in the civil service by their elected supervisors, was enacted by Congress in 1939. The act banned the use of federal funds for electoral purposes and forbade federal officials from coercing political support with the promise of public jobs or funds. Carl Hatch, Senator from New Mexico, introduced the act.

The Hatch Act restricts federal employee participation in certain partisan political activities. The political activity restrictions apply during the entire time of an employee's federal service. Certain rules prohibit both on-duty and off-duty conduct.

Partisan political activities are those activities directed at the success or failure of a political party, candidate for partisan political office, or partisan political group. While most Federal employees are permitted to take an active part in partisan political management and partisan political campaigns, the Hatch Act does prohibit certain participation by all Federal employees, as described below.

An employee who violates the **Hatch Act** is subject to a range of disciplinary actions, including removal from federal service, reduction in grade, debarment from federal service for a period not to exceed 5 years, suspension, letter of reprimand, or a civil **penalty** not to exceed $1000.

Permitted and prohibited activities for Federal employees

*Federal employees **may**:*

- register and vote as they choose;
- assist in voter registration drives;
- express opinions about candidates and issues;
- contribute money to political organizations or attend political fund raising functions;
- attend political rallies and meetings;
- join political clubs or parties;
- sign nominating petitions;
- campaign for or against referendum questions, constitutional amendments, municipal ordinances;

*Federal employees **may not**:*

- use their official authority or influence for the purpose of interfering with or affecting the result of an election;
- knowingly, personally soliciting, accepting or receiving a political contribution from any person;
- run for the nomination or as a candidate for election to a partisan political office;
- participate in political activity while on-duty or in any room or building occupied in the discharge of official duties by an individual employed by DoD;
- engage in political activity while wearing a uniform or official insignia identifying the office or position of the DoD employee;
- engage in political activity while using any vehicle owned or leased by the Government of the United States or any agency or instrumentality thereof;
- knowingly soliciting or discourage the participation in any political activity of any person who has an application for any compensation, grant, contract, ruling, license, permit, or certificate pending before the employee's office;
- knowingly soliciting or discourage the participation in any political activity of any person who is the subject of or a participant in an ongoing audit, investigation, or enforcement action being carried out by the employee's office.

WHAT IS NOT POLITICAL ACTIVITY

- Discussing legislation, ballot initiatives and nonpartisan elections (e.g. gun control measures, executive orders, and school board elections)
- Discussing issues (e.g., abortion, immigration)
- Attending an issue march or rally (e.g. March for Life, Women's March, etc.)

Titling Positons

Submitted by Angel Ponce

The law (5 U.S.C. 5105) requires OPM to establish the official titles of positions in published classification standards. Accordingly, position classification standards generally prescribe the titles to be used for positions in the covered series. Only the prescribed title may be used on official documents relating to a position; e.g., position descriptions and personnel actions.

The requirement to use official titles, however, does not preclude agencies from using any unofficial title they choose for positions. Unofficial titles (such as those relating to specific agency organizations or programs) may be appropriate and helpful for internal agency use or for recruiting purposes, but are not always descriptive of the overall occupation for Government wide purposes.

Agencies may designate the official title of positions in occupational series for which OPM has not prescribed titles; i.e., those not specifically covered by classification standards. The title selected by the agency should not be one that has been prescribed by OPM as an official title for positions in another series. Agencies should consider the following guidance when constructing official titles of positions.

- Nonsupervisory Titles: The purpose of a position title is to communicate an immediate understanding and identification of the job. Titles should be short, meaningful, and generally descriptive of the work performed. They should also be consistent with the occupational series titles established by OPM. Once established titles should be used consistently throughout the agency.

- Supervisory Titles: The duties, responsibilities, and qualifications involved in supervisory work should be recognized in the titles of positions. Therefore, when supervisory qualifications and skills are needed to perform the work, as defined in the appropriate guide or standard, the official title should be supplemented with the word Supervisory as a prefix or Supervisor as a suffix.

- Parenthetical Titles: For some occupational series OPM has prescribed certain parenthetical titles to be used as appropriate for positions in those series. Only these designations may be used. For positions in series for which OPM has not established parenthetical titles, agencies may supplement official titles with parenthetical designations determined by the agency. A parenthetical designation should be used only when it is decided that it would add materially to the understanding and identification of the position. Examples of parenthetical titles would be Typing, Policy and Planning, and Office Automation (OA).

- Student Trainee Titles: All positions classified to a student trainee series should be titled Student Trainee followed by a parenthetical title consistent with the occupational field involved; for example: Student Trainee (Human Resources Management), Student Trainee (Psychology), or Student Trainee (Civil Engineering).

More information on titling positions can be found in the Introduction to the Position Classification Standards TS-134 July 1995, TS-107 August 1991 Revised: August 2009, at the following link: https://www.opm.gov/policy-data-oversight/classification-qualifications/classifying-general-schedule-positions/positionclassificationintro.pdf

Quality Step Increase (QSI)

Submitted by Monica Manchester

I received an inquiry from a supervisor last week who asked, "One of my employees asked about a Quality Step Increase (QSI). What exactly is a QSI?" In good HR fashion, I responded that I could provide a simple answer, but that I wanted to provide him a more clear and concise answer and that I would conduct a little research and get back to him. Here is what I found.

As defined by the Office of Personnel Management (OPM), a Quality Step Increase or QSI is "an additional within-grade increase (WGI) used to recognize and reward General Schedule (GS) employees at any grade level who display outstanding performance. A QSI has the effect of moving an employee through the GS pay range faster than by periodic step increases alone."

Of course, there must be more to it and there is. In order to be eligible for a QSI the employee has to meet several requirements: They must be below a step 10 in their current grade level. They have had to receive the highest rating of record available under their performance management program. They must demonstrate an outstanding quality of performance for a sustained period. The employee cannot receive a QSI if they received one within the last 52 consecutive weeks.

One very important fact to keep in mind is that a GS employee must be in a Permanent Position to receive a QSI. The employee must be eligible for a WGI in order to be eligible for a QSI. A temporary employee is not eligible for a QSI.

The QSI should be effective as close to the date of the most recent outstanding performance rating and usually at the beginning of the next pay period.

A QSI does not affect the timing of an employee's next regular within-grade increase, unless the QSI places the employee in step 4 or step 7 of his or her grade. In these cases, the employee must complete the full waiting period for the new step, 104 weeks for steps 4-6 or 156 weeks for steps 7-9. However, the time an employee has already waited is not lost; it continues to count towards the waiting period for the next step increase. The QSI provides the employee the benefit of receiving an additional step increase at an earlier date than he or she originally would have without losing any time creditable towards his or her next WGI.

The below links provide examples on the timing as a guide for supervisors.

https://www.opm.gov/policy-data-oversight/pay-leave/pay-administration/fact-sheets/quality-step-increase/

https://www.opm.gov/policy-data-oversight/performance-management/faqs/

https://www.opm.gov/policy-data-oversight/performance-management/performance-management-cycle/rewarding/know-the-costs/

https://www.opm.gov/policy-data-oversight/performance-management/performance-management-cycle/rewarding/quality-step-increases/

HR Enters Quality Step Increase (QSI) Performance Based Award

Advance Your Career Through Army eLearning

Submitted by David Grider

Army e-Learning as a program component of the Army Training Information System (ATIS), also known as "The Future of Army Training", offers free individual training for Soldiers and Department of the Army (DA) civilians.

With Army e-Learning:

- Soldiers and civilians can train when it fits their professional needs and personal schedules
- Access to web-based courses in Information Technology, Business Leadership and Personal Development at no cost to the individual or organization
- Available 24x7 anywhere there is internet via desktop or mobile app
- IT certification prep courses/tests in CompTIA, Security+, Network+, MCSE, CISSP, C++, Oracle and many more
- Access to on-line e-books and virtual practice labs
- AEC college credit course training modules
- Custom Learning Paths unique to organizational training needs
- Continuous Learning Points for DA Civilians

To access Army e-Learning and to take advantage of the free training visit, Army e-Learning at https://usarmy.skillport.com. If you are a new user and do not already have a Username and Password, select the "Click here to register" link. You will need your CAC to register. Once you've successfully registered and established a Username and Password, you will be able to access Army e-Learning from any computer.

Note: As of 13 January 2022, in order for Skillsoft to provide the best and most secure learning experience, Internet Explorer will no longer be supported. This means that if you use Internet Explorer, you will encounter a degraded experience and some features may be unavailable and/or have limited functionality. Please use Microsoft Edge, Google Chrome or Mozilla Firefox to continue your training.

Wi-Fi Safety Tips

Submitted by Diana Kent

Free Wi-Fi is available in shopping malls, airports, restaurants, coffee shops, libraries, public transport, hotel rooms - you name it. These networks are used by millions of people on a daily basis. According to a recent survey by the Identity Theft Resource Center (ITRC), three out of four respondents said they use free public Wi-Fi.

However, what most people don't realize is that free public Wi-Fi isn't secure. Even if it requires a password to login, that doesn't necessarily mean your online activities are safe. You might love public Wi-Fi, but so do hackers! So, if you use public Wi-Fi without adequate protection, you're essentially risking your online identity and money.

5 Tips to Keep Your Data Safe on Public Wi-Fi

If you can't avoid public Wi-Fi networks, you should at least ensure you're well-protected when using them. Fortunately, there are some useful tips that you can follow to yourself safe on public Wi-Fi networks:

1. Verify the Network; Configure and Turn off Sharing

Remember that hackers are very clever, so it's better to surf and play smart. Read the network name very carefully and ask an employee of the business if the link is legitimate. You can also ask the offering IP address. As mentioned above, hackers often set up fake networks, so verify the name to avoid being victim.

Another important thing to consider, when connected to the public internet, do you really need to have sharing preferences turned on? Obviously, not! So right after you verify the network, turn off the file sharing option. File sharing is usually pretty easy to turn off from the system preferences or control panel, depending on your operating system.

2. Use a VPN

A VPN (Virtual Private Network) is the most secure option to surf on public networks. It is one of the most useful tools to help people keep their information secure when logged on to public networks.

VPNs encrypt your data traffic and act as a protected tunnel between the client (browser) and server. All the data passing through the tunnel won't be visible to hackers and they won't be able to access your information and the activities you do online.

Another potential benefit to VPNs, is they mask your IP with their own IP address from different location. You could physically be in the Australia, but your VPN would show that you're in a different location.

Not all VPN services are created equal. There are some free VPNs that are less secure than the paid ones. Paid VPNs do cost some money, but they gives additional security to your needs.

3. Use HTTPS

If you don't have access to a VPN, making sure you are only visiting encrypted sites can also help protect your data from some of the threats outlined above.

Look for HTTPS at the beginning of a website's address. This means the connection between the browser and the web server is encrypted, so any data that is submitted to the website will be safe from eavesdropping or tampering. Most browsers also include a padlock symbol at the beginning of the address to indicate the site uses encryption.

Continued on Page 9

Continued from Page 8

CIVILIAN PERSONNEL ADVISORY CENTER

Building 144
2438 Stanley Road
Fort Sam Houston, TX. 78234

Phone: (210) 221-1425
Fax: (210) 221-1015

https://www.samhouston.army.mil/cpac/index.aspx

https://www.facebook.com/Ft-Sam-Houston-Civilian-Personnel-Advisory-Center-217123538373277/

https://twitter.com/FSHCPAC

usarmy.jbsa.hqda-cpac.mbx.inquiry@mail.mil

4. Keep the Firewall Enabled

Turning on the firewall can prevent hackers' unauthorized external access to your system. A firewall won't provide complete protection, but it's a setting that should always be enabled.

A firewall also acts as a barrier that protects your device from data-based malware threats. It actively monitors the data packets that come from networks and checks whether they're safe or not. If it sees any malicious data packet, it gets blocked by the firewall. By blocking certain kinds of data, the firewall protects your computer or network and safeguards your data from attacks.

Usually we turn off the Windows firewall because of the annoying pop ups and notifications and then just completely forget about it. If you want to restart it, then head over to the Control Panel, go to "System and Security" and select "Windows Firewall". If you are a Mac user, you can go to "System Preferences", then "Security & Privacy", then "Firewall" tab and enable Firewall on Mac.

5. Use Antivirus

Antivirus can help protect you while using public Wi-Fi by detecting malware that might get into your system while using the shared network. Always make sure to use latest versions of antivirus program that is installed on your device. An alert will be shown if any known viruses are loaded onto your device or if there's any suspicious activity, malicious attack, or malware gets into your system via network.

Other Important Tips to Stay Safe on Public Wi-Fi Networks

Other than mentioned above tips, here are some more recommended tips of keeping your system secure on public Wi-Fi:

- Always turn off automatic connection.
- Always use 2 factor authentication - this way, even if a hacker obtains your username and password, they still won't be able to access your accounts.
- Always check forget network after using public Wi-Fi.
- Don't run financial transactions over public networks.

And most importantly! Instead of using these insecure networks, it is better to use your smartphone as a hotspot.

FSH CPAC OPERATING HOURS

Office HOURS

Due to the COVID-19 pandemic, our staff is working virtually. Our doors are currently closed to walk-in customers until further notice. However, you may contact your servicing specialist directly via email or ARMY 365 MS Teams. For additional information, questions, or inquiries please call (210) 221-1425.

We appreciate your patience and support during this time.