# eOPF Frequently Asked Questions

**What is the Official Personnel Folder (OPF)?**

The Official Personnel Folder (Standard Form 66) is a file containing records that cover an individual’s employment history. The long-term records included in the file are chosen to protect the legal and financial rights of the Government and the employee. The Official Personnel Folder is part of the Government-wide system of records, OPM/GOVT-1.

**What is the Electronic Official Personnel Folder (eOPF)?**

The eOPF is an electronic version of the original OPF and a system for accessing the electronic folder online. The eOPF allows each employee to have an electronic personnel folder instead of a paper file. Some of the features of the system include:

1. Provides immediate access to OPF forms and information for a geographically dispersed workforce
2. Supports a multi-level secure environment, with security rules for vital information
3. Eliminates loss of employee’s official personnel files in filing and routing
4. Sends e-mail notification to employees when documents are added to their eOPFs
5. Reduces costs associated with storage, maintenance, and retrieval of records
6. When an employee transfers to another federal agency, provides for electronic transfer of pertinent human resources data
7. Integrates and complements agency human resource information systems capabilities
8. Complies with Office of Personnel Management (OPM) and federally mandated HR employee record management regulations

**Who owns the OPF and eOPF, the employee or the agency?**

Neither. According to [The Guide to Personnel Recordkeeping](http://www.opm.gov/feddata/recguide2006.pdf), "The Office of Personnel Management (OPM) owns the personnel folder and its contents." The Guide contains OPM's rules for creating, maintaining, using, and disposing of the Official Personnel Folder.

**What will happen to my paper OPF upon implementation of the eOPF application?**

OPM has directed that the OPFs be shipped to the National Personnel Records Center (NPRC) for retention and disposition in accordance with the General Record Schedule (GRS).

**Do other agencies use electronic Official Personnel Folders?**

As of April 2010, approximately 70 agencies are in the process of, or have completed, their eOPF implementation. Over 1.1 million records have been converted to eOPF. Numerous agencies have made eOPF available to their employees. The list of agencies using eOPF continues to grow.

**Who will have access to the eOPFs?**

HR staff that process personnel actions and payroll documents and those who provide advisory services or benefits support will have access to eOPFs for employees that they service. Employees will have read-only access to their own information. Each employee is responsible for the consequences of providing others access to their eOPF. In addition, each time a folder is accessed by someone other than the employee, a record is made of who accessed it and why. Employee's supervisors, other DOT officials and OPM investigators may be granted temporary access to view eOPFs provided they have a need-to-know for such information.

**Will employees be notified if a manager or HR specialist looks at their eOPF?**

No. E-mail notification occurs only when an SF-50, ‘Notification of Personnel Action’, is added to the eOPF. However, a complete audit trail is recorded each time a document is accessed by any user. The audit trail is a permanent piece of information archived into the system never to be deleted. Please contact your HR office if you have a need to review the audit trail of your eOPF.

**How can I get email notifications when new documents are added to my eOPF?**

If you would like the system to notify you each time a document, such as an SF-50, ‘Notification of Personnel Action’, is added to your eOPF account, your eOPF account profile must contain a valid email address. Many agencies provide an email address for users during system configuration. If an email address was added for you during system initiation, it will be displayed on the “Welcome to the eOPF System” under “User Info:” If there is no valid email address under “User Info:” you will need to add an address; otherwise you will not receive notifications regarding eOPF updates. Use the “My Profile” button on the left-side menu to add your address.

It is recommended that your government provided email address be used, but it is not mandatory. It is your responsibility to change the email address if you no longer use it. If you do not have an email account, contact your local HR specialist to learn of the alternate arrangements in place at your organization.

**Should I sign up for a free email account (e.g., yahoo or gmail) to use in eOPF if I do not have a government provided email address?**

This is NOT recommended. If the email account was considered dormant by the email provider, the email address associated with your eOPF in the application may be reassigned to another user. This could result in email notifications for the system, including password reset letters, going to an unauthorized individual who might then be able to access your personal information.

**How secure is my personal information in the eOPF system?**

OPM has taken several steps to ensure that your information is protected. First, the eOPF can only be accessed through an Internet browser using Secure Socket Layer (SSL) with 128-bit encryption. This ensures that all of the information the eOPF system sends to you over the Internet is encrypted or ‘scrambled’ and thus cannot be readily intercepted and read. Second, access to your eOPF account is controlled by your user name and password. Do not give your password to anyone else. Third, the eOPF has been programmed to limit movement between screens, meaning that you can only get to the screens to see your data by properly entering the system with a valid user ID and password. Fourth, system timeouts are employed to inactivate the system after periods of inactivity.

Additionally, to ensure the confidentiality of data viewed within the eOPF application, you will only be able to access the system from a secured DOT network. Even with these protections, every employee should protect their own data privacy and ensure others are not able to access their information.

### What measures will be taken to ensure that eOPF data will not be lost?

OPM will be managing the eOPF system for all participating federal government agencies.  Nightly incremental system backups will be conducted, which include all new documents and any related information added on a given day.  Full system-wide backups will occur weekly. Both backups are placed on backup tapes in an encrypted format and are stored off-site from the hosting facility.  These steps will ensure that the system and data can be restored in the event of a disaster.

### How will I receive training on the system?

The eOPF, like other web-based systems, is very intuitive. For an overview of the application functionality refer to the [Employee Quick Reference Guide](http://dothr.ost.dot.gov/hrprograms/automation/eOPF/eOPF%20QRG%20v1.0_2008-01-31.pdf) ([text version of the Quick Reference Guide](http://dothr.ost.dot.gov/hrprograms/automation/eOPF/eOPF%20QRG_Text%20Only_%20v1%200_2008-02-04.doc) here) or the user manual via the Help link embedded in eOPF. “eOPF End-User training” is also available on the eLMS and TMS Training Systems.

If additional assistance is required, please contact the eOPF Help Desk at 866-275-8518 or [eopf\_hd@telesishq.com](mailto:eopf_hd@telesishq.com).

### What is a ‘Folder’?

Documents are filed in the Official Personnel Folder to record important events in an individual's Federal employment history. In the standard eOPF release, documents are either temporary or permanent documents. In the paper world OPFs consisted of a single folder. Documents were often referenced as “left side” (Temporary) or “right side” (Permanent.) These folder sides are replicated in the electronic world by their formal names and are referenced as individual folders or folder sides (these terms are often used interchangeably.)

1. LEFT Side = Temporary Documents. Temporary documents are documents that are not kept for the life of the personnel folder. These documents were filed on the LEFT side of the folder.
2. RIGHT Side = Permanent Documents. Permanent documents are kept for the life of the folder. These documents were filed in chronological order on the RIGHT side of the personnel folder.

Within eOPF, agencies can create additional ‘virtual’ sides to store other HR documents, such as training or performance. If your Operating Administration has created additional folder sides beyond the standard issue, end users will see them as options on the search screen. HR staff will have the option to assign documents to the additional folder sides in the same manner as the standard folder sides. Access to other forms will be based on current OPM recordkeeping practices.

### Is it mandatory to complete the Emergency Contact Information in eOPF?

Employees will be able to enter information regarding whom to contact in an emergency on the Employee Contact Information page. Entering this data is voluntary, but may be required by your operating administration, and it will be up to the employee to keep it accurate. The home address information comes directly from the payroll system and cannot be changed within the eOPF application.

### What if I forget my password for accessing my eOPF?

There is a ‘Forgot Your Password’ link on the eOPF login screen if you forget or lose your password. You will be asked a few questions to verify your identity and, once successfully verified, you will be able to establish a new password in the application immediately.

Note: Please use the ‘Forgot Your Password’ link if you have attempted to enter your password three times unsuccessfully. Otherwise, if you do not enter it correctly on your fourth attempt you will be locked out of the system and will need to contact the eOPF Help Desk to have your password reset manually.

### Is there a Help feature for eOPF?

eOPF has an online help function that you can reach by clicking on the word 'Help' at the top of most pages within the web site. The instructions in the help feature can be printed. If you are having system problems or content with your eOPF, please contact the eOPF Help Desk. The eOPF Help Desk can be contacted using the following methods:

Email: [eopf\_hd@telesishq.com](mailto:eopf_hd@telesishq.com)

Phone: 866-275-8518

You will need to provide the following information:

1. Name
2. Organization (DOT)
3. Contact information (phone and email)
4. The URL impacted (this can be obtained by copying the address from your web browser)
5. Severity of problem (high, medium or low)
6. Description of problem
7. Any specific instructions (if necessary)

### Why are there documents in my eOPF dated 01/01/1901?

During the backfile conversion/scanning process, some documents that contained illegible identifying information and/or dates, were indexed with a default effective date of 01/01/1901. If you have questions about any of these documents in your eOPF, please contact your [servicing HR office](http://dothr.ost.dot.gov/hrprograms/automation/eOPF/eopf-poc.htm).

### What is backfile conversion?

All of the paper documents in the existing OPF were scanned, digitized, and indexed into eOPF.

### I noticed that a document in my eOPF is incorrect, what do I do?

Contact the eOPF Help Desk. The help desk is equipped to “diagnose” the problem and direct it to the correct resource to solve the issue. In this case, the help desk would route your issue to the appropriate HR representative at your agency. Please do not contact your HR staff, as that may not be the correct contact to solve the issue.

### I have reviewed my folder and it appears that the latest document is missing. What should I do?

It’s probable that the missing document is still at your HR Office and has not yet been added to your eOPF file. Some forms, like the Notification of Personnel Action (SF-50) come from another system and are transmitted directly into the eOPF. However, certain processes still produce paper which have to be manually scanned in-house and added to your eOPF. There may be a short delay between when a process is completed and when the paper document is scanned and available in the eOPF application.

### Why are the current SF-50s in eOPF not signed?

The Federal Personnel and Payroll System (FPPS) that is used by DOT for processing personnel actions and generating SF-50s retains a record of the approval of personnel actions. The approved SF-50s are passed from FPPS to eOPF, so there is no requirement to display a signature on the SF-50s.

### Who processes removal of documents?

HR staff are the only users that may add or delete documents from the eOPF. If you have a concern about a document (e.g., a letter of reprimand), call the eOPF help desk. The Help Desk will route your request to the appropriate HR specialist at your agency.

### Will employees be notified when items are removed from their eOPF? i.e. letters of reprimand?

The removal of documents, such as the expiration of a Letter of Reprimand, will not generate a notification.

### If I leave the Department of Transportation will I still have access to eOPF?

If you leave the Department you will not be able to access the system. If you move to another Federal agency that is an eOPF client, you will be issued a new user ID and password to access your data.

### What happens to my records if I transfer to another agency?

If you transfer to an agency that is using eOPF, your records will be transferred electronically. If you transfer to an agency that is not using eOPF, your records from eOPF will be forwarded to the new agency, where they will create a hard copy OPF.

### Who is covered by eOPF?

All DOT Federal civilian employees are covered.

### How often will I be required to change my password?

You will be required to change your password every 90 days.

### Can any of the information be downloaded to an employee’s local PC?

Yes, any document can be downloaded individually or in its entirety to their local PC. Be advised when using this function it is your responsibility to protect your own data.