HPD Teleworking Technology Usage and Data Privacy Guidelines

Updated March 18, 2020

As an integral element of the City's efforts to mitigate the effects of and the continued spread of the coronavirus (COVID-19), HPD is implementing a temporary telework policy to enact and encourage social distancing strategies in the workplace.

The documents in the attached packet provide guidance on HPD's telework policies and practices. ***These policies and practices are designed to ensure that teleworking employees conduct their work at the level of efficiency required to sustain HPD's business operations, and a level of effectiveness to continue fully promoting HPD's mission.*** They also ensure that HPD's teleworking employees are using technology responsibility, in a manner that:

- safeguards private data about the individuals that HPD serves and eliminates the possibility of sharing individuals' personally identifiable information (PII).
- reduces network traffic and unnecessary tech system usage that can prevent other staff from completing their work efficiently and effectively.
- adheres to Citywide guidelines and requirements for protecting agency information, while avoiding the possible misuse of City-managed tech systems.

The following documents appear in this packet; together, provide an overview of the current policies and practices for conducting telework:

A) **Preparing to Telework**: This document outlines the technology you may need at home in order to take advantage of teleworking through HPD's systems, and how to ensure that it meets City requirements.
B) **Teleworking and Data Privacy**: This document describes PII and indicates the steps you must take to avoid using, downloading, or transmitting PII in ways that are not permitted. (Signature required.)
C) **Teleworking Environments**: This document orients you to the various resources available outside the office for completing HPD work and provides basic instructions for how to access them.
D) **Downloading and Installing Office 365 Applications**: This document provides instructions to download and install Office 365 products on devices.

Please read these documents carefully, and contact TechRA@hpd.nyc.gov if you have any questions about them. After you have reviewed them, you will be asked to sign the Data Privacy Acknowledgement Agreement indicating your understanding of the instructions and information they contain and affirming your compliance with the requirements and restrictions that they outline.

Please also note the following:

1) HPD is providing this permission to telework on a *restricted basis*. Your telework permission may be revoked:
   - If the nature of your work changes.
   - If you violate any of the policies for telework.
   - If HPD's telework policies change, are suspended, or are discontinued.

   Please review the basic Telework Policy which appears as the first section of this packet.

2) The information contained in the attached documents may change as policies and practices are refined and updated, and as new resources become available that improve and better support teleworking. Please stay alert for updated guidance, which will be issued on an as-needed basis.

We thank you for your flexibility and dedication.

Department of Housing Preservation & Development (HPD)
Telework Policy During the COVID-19 Outbreak

Date: March 16, 2020

I. Purpose

As an integral element of the City's efforts to mitigate the effects of and the continued spread of the coronavirus (COVID-19), HPD is implementing a temporary telework policy to enact and encourage social distancing strategies in the workplace. The temporary policy will allow certain HPD employees to work from home, while ensuring the continuity of agency business operations. This policy does not supersede City rules, regulations, or policies applicable in the workplace, but rather is designed to facilitate the performance of City business in alternate work locations.

The Agency will make a weekly assessment of the need for telework and inform appropriate personnel about the continued use of this mitigation strategy.

II. Eligibility for Telework

Under appropriate circumstances, HPD may make special arrangements to allow employees to work remotely for a portion or all their work hours.

1. The nature of the employee's job must conducive to telework.
2. An employee must be able to effectively communicate with clients, stakeholders and team members from home or other alternative work site in order to be eligible.
3. Where an employee's responsibilities require daily case management through a workflow system, remote access to that system should be available for telework to be appropriate for that employee. If such responsibilities do not require access to the system every day, telework may be appropriate for that employee on days when such access is not required.
4. Work history may be considered in making telework eligibility determinations.
5. A position that requires frequent interactions with members of the public on a daily basis may not be eligible for telework unless such interactions can be handled through a team of employees such that each day there is sufficient staff available in the office to provide appropriate services to members of the public.
6. Non-represented and represented employees who provide essential services in a business continuity context, which can be performed in a remote capacity, are most ideal for telework opportunities.
7. Employees whose tasks have measurable deliverables including, but not limited to, responsibilities such as writing, research, or editing reports, and other tasks that require minimal supervision, should be considered appropriate for telework consideration.
8. The staffing level of the department is such that it will permit the employee to telework.

9. If an employee is subject to self-isolation or quarantine, and the position is one in which telework is otherwise eligible and feasible, an employee may be permitted to work from home on a voluntary basis if the employee is healthy enough to work and the other criteria under this policy are met.

III. Guidelines for Telework

The following guidelines will apply to all employees who telework:

1. Telework days may be five days a week or a hybrid schedule of telework and in-office work (e.g., telework three days a week and at the workplace two days a week).

2. Regular workload will be maintained through work schedules that will be agreed upon in advance. If an employee has a staggered work schedule approved by the agency, the employee's regular work schedule may be adjusted to conform to the staggered schedule on the days when the employee teleworks. Any deviation from an established schedule at the request of an employee must be approved by that employee's supervisor.

3. Annual leave, sick leave, and all time-off policies will apply to telework employees the same as employees working onsite. All absences from regular work hours must be reported to and approved by the employee's supervisor.

4. Withholding taxes will be deducted from payroll based on HPD's physical location in New York City, not based on the location of the employee's home address.

5. As determined necessary and appropriate by the supervisor, employees will be expected to attend meetings, trainings, or other work-related obligations, whether such meetings, trainings, or other obligations are located at the workplace or at another location.

6. All telework arrangements are granted at the discretion of HPD, on a temporary basis, and may be discontinued at any time and for any reason or for no reason by HPD or the employee.

7. Telework employees may be required to check in with their direct supervisors at the beginning of their daily work schedule to determine work deliverables during that day, e.g., work assignments, deadlines, projects, emails, and work product.

8. Telework employees must follow all HPD policies, including but not limited to, those regarding Confidentiality, Information Systems and Materials Usage, regardless of offsite remote access.

IV. Location and Equipment

1. The designated alternate work location must be an appropriate work environment. This location should be one in which the employee's telework duties can be performed in a safe and ergonomically

appropriate manner. The teleworker must agree to perform all work at the primary alternate location. If business or exigent circumstances arise requiring the employee to work at location other than the primary designated location, the employee shall immediately notify his or her supervisor.

2. Agencies shall provide equipment (computer, phone, internet access), where possible. Personal equipment (e.g. an employee's own laptop, smartphone, scanner, etc.) may be used, provided that strict adherence to information security protocols is followed. Any questions about information security protocols should be referred to HPDtech or DoITT, and NYC Cyber.

3. Any HPD equipment that is loaned to an employee will remain the property of HPD and is the employee's responsibility while it is used by them offsite. The employee must return any loaned equipment in the same condition in which they received it from HPD (minus normal wear and tear). Employees must reimburse HPD for lost or damaged HPD equipment.

4. The agency will provide access to CityTime, if technically feasible, or develop another method for timekeeping.

V. Compliance with City Policy

1. All terms and conditions of City employment will continue to apply.

2. Workplace rules prohibiting private activities during work hours must be followed notwithstanding the fact that employees are working from home.

3. Overtime must be approved in advance.

4. Leave time must be requested and processed in the same manner as in the workplace.

5. Employees who telework must participate in conference calls and team meetings as necessary.

Employees who telework must follow all information security protocols when using City and/or electronic equipment and accessing systems. Employees must maintain any approved safeguards to protect agency records from unauthorized disclosure or damage and comply with the privacy requirements set forth by the City of New York.

PREPARING TO WORK FROM HOME

Teleworking allows employees to perform work duties using communication tools, such as phone, modem, video- or teleconferencing, e-mail, and/or instant messaging from a secure remote location. With Microsoft Office 365 and/or credentials to remotely access HPD's networks, employees can perform the following activities:

- Make and receive phone calls
- Send emails and schedule meetings from their HPD outlook accounts
- Hold team meetings and conversations to work collaboratively
- Access files and edit documents in Word, Excel, and PowerPoint
- Conduct presentations and trainings for colleagues
- Use HPD applications
- Connect to their actual desktop to access files in the C Drive and on Access

Please see the following section to ensure that you have the information and technology system set up required to conduct your work remotely.

HPD Account Login Information

Your network password expires 90 days after a new password has been set. It is possible that your password will expire will you are teleworking. It will be difficult to change your network password if you do not have remote access, so please plan ahead.

For those without remote access credentials:

- Change your password on your desktop at the HPD office before teleworking, by click [control] & [Alt] & [delete] simultaneously. Add the expiration date to your calendar as a reoccurring notification.
- Go into one of HPD's offices and log into a desktop and proceed to change your password using the prompts.

For those with remote access credentials:

- Log into remote access. Connect to your virtual desktop and follow the prompts to change your password.

If these methods do not work, then contact the Citywide Service Desk, call 212-692-4357 (212-NYC-HELP) or e-mail NYCHelp@doitt.nyc.gov to request to have your password reset. You may need another HPD staffer or supervisor to send an email to DOITT on your behalf. Please make sure to have contact information for at least one person.

Saving and Scanning Files Prior to Leaving Work

If you do not have Remote Access, you will need to begin saving critical files in OneDrive. While onsite, review your files and folders to determine what you will need while teleworking. You may want to have access to paper files while you're away, please make sure to also review those files and scan and save these files as directed by your supervisor if they are for the collective use of your division. Documents uploaded to OneDrive

cannot include Personally Identifiable Information (PII). Remove all PII data from the files you will need for your personal use then upload to OneDrive.

Please refer to the "Guidelines for Safeguarding Personally Identifiable Information while Teleworking" for information about how to make the determination of what can be uploaded to OneDrive.

Accessing HPD Office Locations

As of now, HPD Office locations will be open during the COVID-related teleworking period. You may return to the office if you need files or if your supervisor requests your return. Please check hpdnyc.org for continual updates on the current emergency plan to see if office locations are closed.

Telework Equipment Requirements

In order to telework, it is requirement that you have all technical capacities to perform your work responsibilities (i.e. password-protected computer, phone, and secure network access). HPD staff must adhere to the following policies and best practices.

Best Practices for Equipment Maintenance

All staff must agree to the following technology guidelines to ensure the security of HPD data:

Web Connection Options

- Use a secure, password-protected internet connection. **Do not** use open network/public Wi-Fi. You can connect to the internet through:
    - A modem connected to your home Wi-Fi network.
    - A wireless phone that has a data plan as the primary device or a hotspot. The hotspot creates a personal, secure internet connection for a second device (e.g. computer). Search the web for instructions on how to set up a hotspot for your device. Be sure to restrict access with a password.

Best Practices for Password Creation and Maintenance

- Passwords must never be shared, displayed on screen, or written down
- Passwords must be changed immediately if there is any indication that it has been compromised
- System passwords and pins must have a minimum length of eight (8) characters
- Passwords must be constructed using at least one alphabetic character and at least one character which is either numeric or a special character

- Passwords must not be constructed from user IDs, proper names or other names, words, numbers or dates readily associated with the individual user (e.g., telephone extension, Social Security number, or zip code).
- Passwords must be changed every ninety (90) days.
- Users cannot re-use any of the past four (4) passwords.
- Passwords used on non-City of New York systems and devices should be different from your HPD login and password. This reduces the risk to City systems if a personal (non-City) account password is compromised.

Additional Best Practices for Desktop Users

- Use a strong password-protected computer (i.e. either a personal computer or your home computer that has a password protected profile that no one else uses). Search the web for instructions on how to create user profiles for your desktop computer.

- We also encourage that you check your system to ensure that it is using up-to-date anti-virus and malware software.

GUIDELINES FOR SAFEGUARDING PERSONALLY IDENTIFIABLE INFORMATION (PII) WHILE TELEWORKING

When working remotely, you may need to take extra steps to manage **sensitive agency data**. This document outlines your responsibilities, and the guidelines you are expected to follow, when handling Personally Identifiable Information (PII).

What is PII?

PII are data elements that may reveal, or lead to the unintentional release of, an individual's identity. **It is illegal to make public the identities of or information that can, in concert with other publicly available information, identify those who use HPD's services**; for this reason, protecting PII is critical. Whether teleworking or working in-office, **PII should never be shared outside of the agency**.
Below is a list of common categories of PII.

Types of Identifying Information	
• Name • Social security number (full or last 4 digits)* • Biometrics such as fingerprints or photographs	**Government Program Information** • Any scheduled appointments with any employee, contractor, or subcontractor • Any scheduled court appearances • Eligibility for or receipt of public assistance or City services • Income tax information • Motor vehicle information
Contact Information • Current and/or previous home addresses • Email address • Phone number	
Work-Related Information • Employer information • Employment address	
Demographic Information • Country of origin • Date of birth* • Gender identity • Languages spoken • Marital or partnership status • Nationality • Race • Religion • Sexual orientation	**Technology-Related Information** • Device identifier including media access control MAC address or Internet mobile equipment identity (IMEI)* • GPS-based location obtained or derived from a device that can be used to track or locate an individual* • Internet protocol (IP) address* • Social media account information
Status Information • Citizenship or immigration status • Employment status • Status as victim of domestic violence or sexual assault • Status as crime victim or witness	**Law Enforcement Information** • Arrest record or criminal conviction • Date and/or time of release from custody of ACS, DOC, or NYPD • Information obtained from any surveillance system operated by, for the benefit of, or at the direction of the NYPD

* Types of identifying information designated by the Chief Privacy Officer.

Accessing and Using PII During Telework

As part of your day-to-day work you may handle PII. However, in a telework environment (where certain in-office-based firewalls and safeguards may not be in place), it becomes incumbent on the user of telework tools to ensure that PII is not being inadvertently exposed or transmitted.

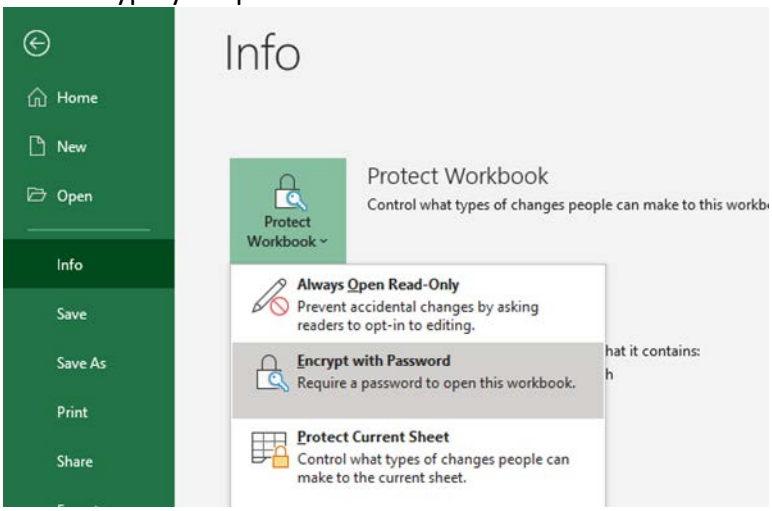
For this reason, when teleworking with files that contain PII, the following are preferred and acceptable options:

1) **Preferred Option: Access those files via Virtual Desktop, as these methods of access retain HPD's in-office firewalls and safeguards**.

2) Acceptable Option: If you are unable to use Virtual Desktop, remove all PII from the documents that is not essential to the specific work being done.

3) Acceptable, but Discouraged Option: If you are unable to use Virtual Desktop, either 1) remove all PII before sharing those documents on OneDrive or 2) password-protect the document and send it as an attachment in an email. Please notify the sender that they should not save the attachment to OneDrive if they are an internal user. To password protect a file:

    - Go to File
    - Click Info
    - Select "Protect Document"
    - Select "Encrypt with Password" from the dropdown
    - Type your password



if none of these three options will work for your circumstance, please contact the Remote Privacy Liaison at **dataprivacy@hpd.nyc.gov** for additional guidance and solutions. Please do NOT handle files with PII until establishing a plan with the Liaison.

Protecting PII while Using Microsoft Office 365

Microsoft Office 365 provides an efficient and user-friendly telework environment. But because Office 365 applications are cloud-based, they do not inherently protect PII (as is the case with in-office and Remote Desktop / VPN). For this reason, please take the following precautions when receiving or reviewing files with PII in Office 365.

- **MS OneDrive**: Do not save any document with PII to OneDrive.
- **Do Not Set Up AutoSave in Microsoft Office Products:** Because AutoSave saves copies of files to OneDrive, always keep "AutoSave" set to "Off."

- **MS Teams:** Do not reference or share any PII in MS Teams (whether teleworking or in the office).
- **MS Forms**: Do not collect any PII data from staff, CBO partners, or other agencies using the MS Forms tool.

PII Protection in All Environments

Whether teleworking or working in the office, the following guidance is always applicable.

- **Email:** Never email files that include PII (whether teleworking or in the office). If PII cannot be removed from a document, create a password protected file (per the instructions above) and instruct the recipient not to share the file.
- **Downloads to Personal Computers**: If you download a file on your personal computer with any PII, you must delete the file after you complete your task. You must also delete the file from your download folder.
- **Password Protection**: Never share login and password information to share reports or data that include PII.

If you have any questions about Protecting PII, please contact the Remote Privacy Liaison at dataprivacy@hpd.nyc.gov.

DATA PRIVACY ACKNOWLEDGEMENT AGREEMENT

You must abide by the City's Cyber Security Policies and Standards for PII. This will act as a safeguard from unintentionally or maliciously comprising data collected by the agency. Please review the HPD Data Privacy Acknowledgement Agreement in its entirety. Sign and return it to the Chief Privacy Officer (dataprivacyagreement@hpd.nyc.gov) within five business days of your official telework start date to maintain teleworking privileges.

If you are currently teleworking and do not have access to a printer and scanner, here are a few suggested ways to return your affirmation of this policy to the Chief Privacy Officer:

- **Markup:** Sign this document using the markup feature available on touch screen devices. You can use the marker function to sign your name with your finger. Save the document with the mark up and email it to the Chief Privacy Officer.
- **Electronic Signature:** Sign the document using an electronic signature and email it to the Data Privacy Officer.
- **Email Affirmation:** Send an email with the subject "*Data Privacy Acknowledgement Agreement*" to the Chief Privacy Officer. In the body of the email include the following affirmation: "*I acknowledge that I have received and reviewed 'Guidelines for Safeguarding Personally Identifiable Information (PII) while Teleworking' and that any failure to comply with these policies will result in disciplinary action,*" along with the information outlined below.
    - Full Name
    - Employee ID
    - Date

Data Privacy Acknowledgement Agreement

I _____ [Full Name / Employee ID] understand that, while teleworking, I may have access to electronic or spoken Personally Identifiable Information (PII), as described in the document titled *""Guidelines for Safeguarding Personally Identifiable Information (PII) while Teleworking."*

Accordingly, as a condition of, and in consideration of my access to this information, I promise that:

1. I will use PII only as needed by me to perform my legitimate duties as defined by my work responsibilities at HPD.
    a. I will not access PII files for which I have no work-related need.
    b. I will not divulge, copy, release, alter, revise, or destroy PII except as properly authorized within the scope of my work with HPD.
    c. I understand that it is my responsibility to assure that files with PII data in my possession are maintained in the most secure environment possible (e.g., a secure physical environment for printed files and/or a secure technology environment for electronic files).
2. I will safeguard and will not disclose to any other person my access code (username and password). I will be responsible for misuse or wrongful disclosure of this information and/or for failure appropriately to safeguard it. Specifically:
    a. I will log off computer systems after use.
    b. I will not permit others to access PII using my access code (in, or outside of, my presence).
    c. I will report any suspicion or knowledge that my access code or any PII has been misused or disclosed without HPD authorization.
3. I will not download or transfer electronic or paper files containing PII to any non-HPD employee, nor will I download or transfer electronic or paper files containing PII to any computer, data storage device, portable device, telephone, or other device capable of storing digitized data, unless
        i. Doing so is necessary for the completion of a task,
        ii. There does not exist a more secure option for handling the PII in order to complete the task.
        iii. The PII is immediately deleted when the task is complete.
4. I will print documents containing PII only in a physically secure environment, will not allow other persons' access to printed PII, and will destroy all printed PII when my legitimate need for that information ends, and in a way that protects the confidentiality of the information.
5. I will not email PII unless the document is password protected, the recipient is an internal HPD employee, and the password is provided only to the recipient.
6. I will transfer PII only to internal HPD staff, and only when it is absolutely necessary as part of my work; I will ensure that only the necessary information is sent.

By signing below, I acknowledge that I have received and reviewed "Guidelines for Safeguarding Personally Identifiable Information (PII) while Teleworking" and that any failure to comply with these policies will result in disciplinary action.

Print Name: _____ Signature: _____

Date: _____

TELEWORKING ENVIRONMENTS

There are two teleworking environments:

1. **Office 365:** Available for all HPD employees
    a. Staff should perform typical duties, like sending emails, hold team meetings in Teams, accessing files through OneDrive, and editing documents in Word, Excel, or PowerPoint.
    b. Please note, any files, documents, or conversations developed or conducted through any Office 365 application is stored permanently.
2. **HPD Remote Access:** Available for HPD employees that need continual access to HPD applications (e.g. HPDInfo) while teleworking.

Burden on the City's Data Infrastructure

Office 365 does not place a heavy burden on infrastructure resources. We suggest that employees use applications within Office 365 for the bulk of their work to reduce traffic on the City's data infrastructure. Most of an employee's duties can be performed on an application available through Office 365.

HPD Remote Access places a large burden on infrastructure resources. It may "brown out" or become unavailable from time to time. We recommend only using remote access when you really need it (e.g. accessing HPD systems) to conserve bandwidth for other City staffers and customers visiting City websites and databases. Conservation tips include:

- Do not use any streaming services while you're remoting into your desktop.
- Exit remote access after accessing HPD system and perform the rest of your work on Office 365.

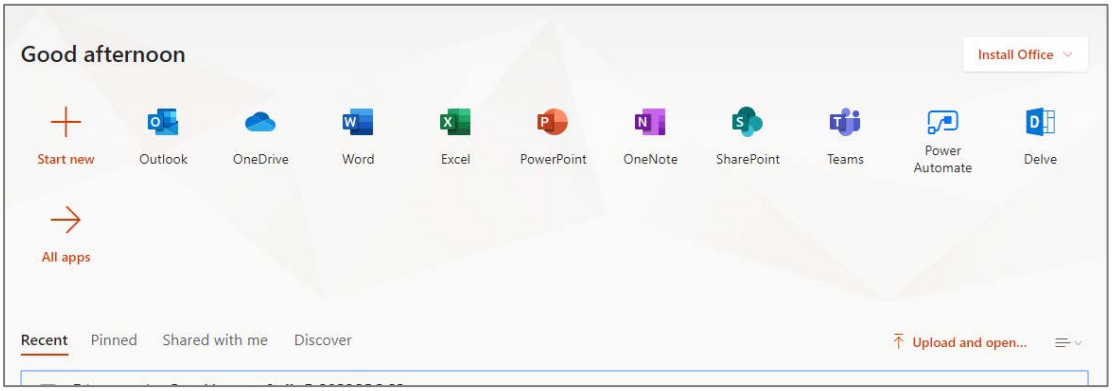
Given the constraints of the City's technology infrastructure, HPD has the right to remove remote access credentials from staffers at any point.

Office365 Access

To access Microsoft Office 365, follow the steps below:

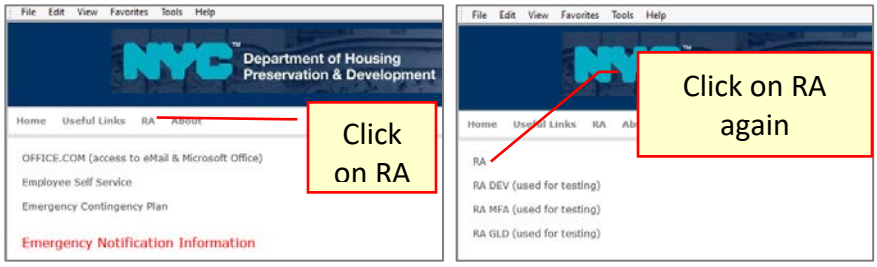
1. Enter the following website into your internet browser: https://www.office.com
2. Enter your full HPD email account (ex: SmithJ@hpd.nyc.gov)
3. Enter your network password – the same one you use when logging in daily at your HPD desktop PC.

You will be taken to your personal Office 365 Documents space. Web versions of Office 365 applications are arrayed in a banner at the top of the page. These applications can be **downloaded on up to 5 devices**. See Downloading and Installing Office for more information.

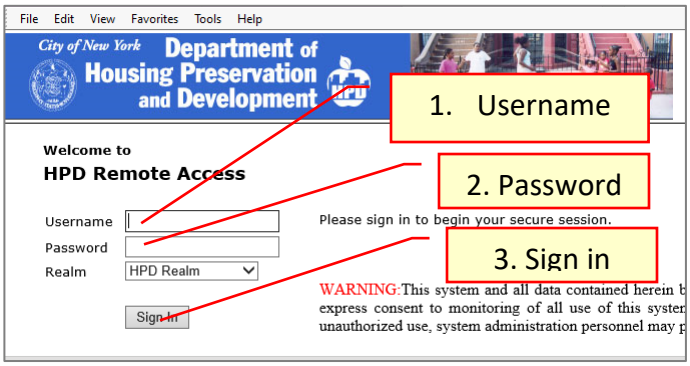


HPD Remote Access

In addition to Office 365, if you have **HPD Remote Access,** you can access the share drive or reach HPD's systems through a virtual desktop.
Full HPD Remote Access instructions are available at http://hpdnyc.org. Look for the link entitled **Remote Access Guidelines** under the **RA** tab. Following is a brief summary:



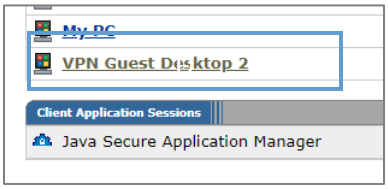
1. Go to: http://hpdnyc.org. (a) Click on the **Remote Access Guidelines** link for complete instructions (b) In the banner, click on "RA" (b) A menu of remote access options appear. Click on the first item: **RA**
2. You are taken to the Remote Access page.



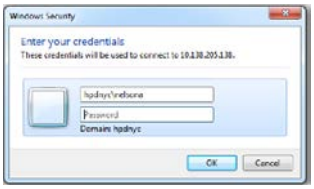
3. Enter your network Username without any "hpdnyc\" or other domain prefix
4. Enter your network password – use the one for your HPD desktop.
5. Make sure the Realm is "HPDRealm"
6. Click on **Sign In**.
7. On the next screen choose **HPD User Role**:

After choosing HPD User Role, you will be taken to the **HPD Remote Access Web** Interface. On this landing page you can access CityTime through the intranet link. You can also download files from the R or S drive. These files may contain personally identifiable information. Please refer to the "Guidelines for Safeguarding Personally Identifiable Information while Teleworking" to ensure that you are abiding by the data privacy guidelines.

8. To access the virtual desktop scroll to the bottom of remote access landing page. Click the link "**VPN Guest Desktop 2**."



9. First time users will be asked to download the Pulse Remote Access application. Follow the installation process.
10. You will be asked to sign in.



11. Type your network name **with a "hpdnyc\" prefix. Virtual Desktop requires this prefix!** For example hpdnyc\lastnameX.
12. Type the password you normally use to log into your desktop.
13. You will see a temporary popup telling you that you are connecting to 10.138.205.138.
14. You may see other Juniper or Pulse messages advising you that additional components are being downloaded.
15. If there is network congestion, you may see the message "Connection disconnected" and the popup disappears. Try logging in again a few minutes to a half hour later. In the meantime, consider if what you need to do can be done in the *Office365 Access* environment.
16. In most cases, the temporary popup appears and is replaced with a Microsoft Remote Access session. You will see the session start screen. Click on **OK** to Proceed.
17. Your Virtual Desktop appears. While it may be similar in appearance, it is not your HPD desktop machine. However:
    a. Office software and internal applications like the HPDInfo client tool is available as desktop icons.
    b. The HPD Intranet home page can be accessed through your browser. Reach internal web-based applications through the **application** banner at the top of the home page.
18. Your virtual desktop will have drives mapped to:
    a. Your S:\\ personal network drive on the HPD internal file server
    b. R:\\ network drive to access folders shared among HPD divisions
    c. C:\ Documents folder from your desktop machine will be mapped as well, but no other folders on your C:\\ will be available.

DOWNLOADING AND INSTALLING MICROSOFT OFFICE 365

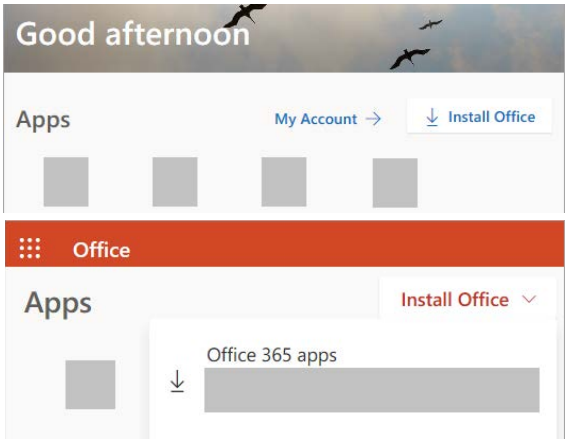
Installing on a PC or Mac

Before installing, check that your PC or Mac meets the system requirements.

If this is the **first time** you're installing Office, you may have some setup steps to do first. Below is guidance on how to sign in and install Office on your PC or Mac.

Sign in to Download Office

1. Go to www.office.com and if you're not already signed in, select **Sign in**.
2. Sign in with the account your HPD account credentials.
   a. From the Office home page select **Install Office**.
   b. Select **Install** (or depending on your version, **Install Office>**).
   c. From the Office 365 home page select **Install Office apps** (If you set a different start page, go to aka.ms/office-install.)
   d. Select **Office 365 apps** to begin the installation. You can install Office on up to 5 devices.
3. This completes the download of Office to your device. To complete the installation, follow the prompts in the "Install Office" section below.



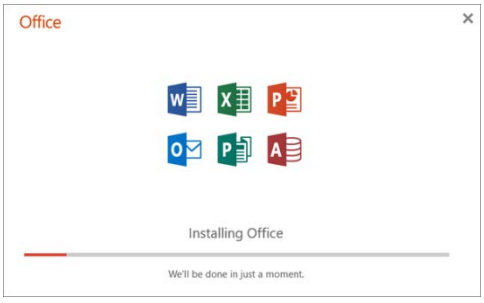
Tip: Don't see an install option after signing in? There could be an issue with your account. Select Need help? from above and review the solutions under **Account questions**.

Install Office

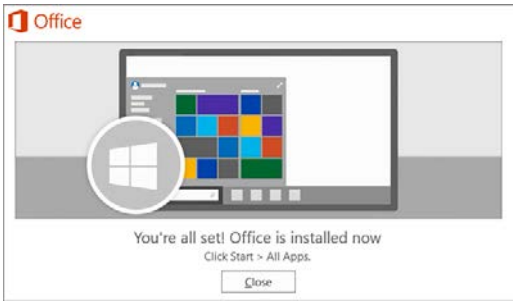
1. Depending on your browser, select **Run** (in Edge or Internet Explorer), **Setup** (in Chrome), or **Save File** (in Firefox).

   If you see the User Account Control prompt that says, **Do you want to allow this app to make changes to your device?** select **Yes**.

   The install will begin.



2. Your install is complete when you see the phrase, **"You're all set! Office is installed now"** and an animation plays to show you where to find Office applications on your computer.
3. Select **Close**.



Installation or sign in issues? If you're having an installation issue such as Office taking long to install, try Need help? for a list of common issues.

Activate Office

1. To open an Office app, select the **Start** button (lower-left corner of your screen) and type the name of an Office app, like **Word**.

   If you have Windows 8.1 or 8.0, type the name of an Office app on the **Start** screen. Can't find your Office apps?

2. To open the Office app, select its icon in the search results.
3. When the Office app opens, accept the license agreement. Office is activated and ready to use.

How to Install on A Mobile Device

In order to perform your work functions, you should download both Outlook and Microsoft Office, as well as Teams onto your mobile devices.

- Install and set up Office and Outlook on an Android
- Install and set up Office and Outlook on iOS devices
- Learn how to download Teams to your devices here: Make sure to scroll to the bottom and click on the appropriate device. For PCs click on Windows 64 bit

If you have issues with any of these instructions, you can find additional information here.