Office 365 Basics for Secure Work From Home

NPC Safe Computing Webinar Series
March 27th, 2020

Larry Keating, President

Darren Mar, National Accounts Manager

Copyright © NPC DataGuard 2020. A division of Compugen Inc.

AGENDA

- The Importance of Secure Computing from Home at this Time
- Specific Cyber Threats
- The Essentials for Secure Computing in Your WFH Environment
- Connect to Your Data with SharePoint
- Connect People with Teams
- Q&A

NPG

PRESENTERS:

Larry Keating, President

30 years' experience with information technology, remote communications and data security

Darren Mar, National Accounts Manager

10 years in SMB technology products and services, with emphasis on financial services small office security

The Importance of Secure Computing from Home at this Time

WORKING FROM HOME – TOP LEVEL

- Those not prepared are rushing solutions together and making security and operational compromises
- Law enforcement, intelligence agencies and security vendors are alerting that cyber threat activity has increased significantly since the pandemic was declared
- Cyber criminals are opportunistic, and without remorse:
  - US Department of Health and Human Services attacked last week

FOR CYBER CRIMINALS, IT'S A PERFECT STORM

An anxious population in an uncertain moment in time

A fog of misinformation

High demand for certain goods

Massive, rapid change in business operational flows, and how we work as individuals

SPECIFIC THREATS

- Crisis-related threats from unsolicited calls and emails are active:
  - Sanitization services, calls with apparent test results seeking health/credit card information, Red Cross donations
  - Sale of fake cures, personal protective products
  - Increase in BEC (Business Email Compromise) scams
  - “hot stock” and “pump and dump” scams for crisis related companies
  - Government department crisis-themed information

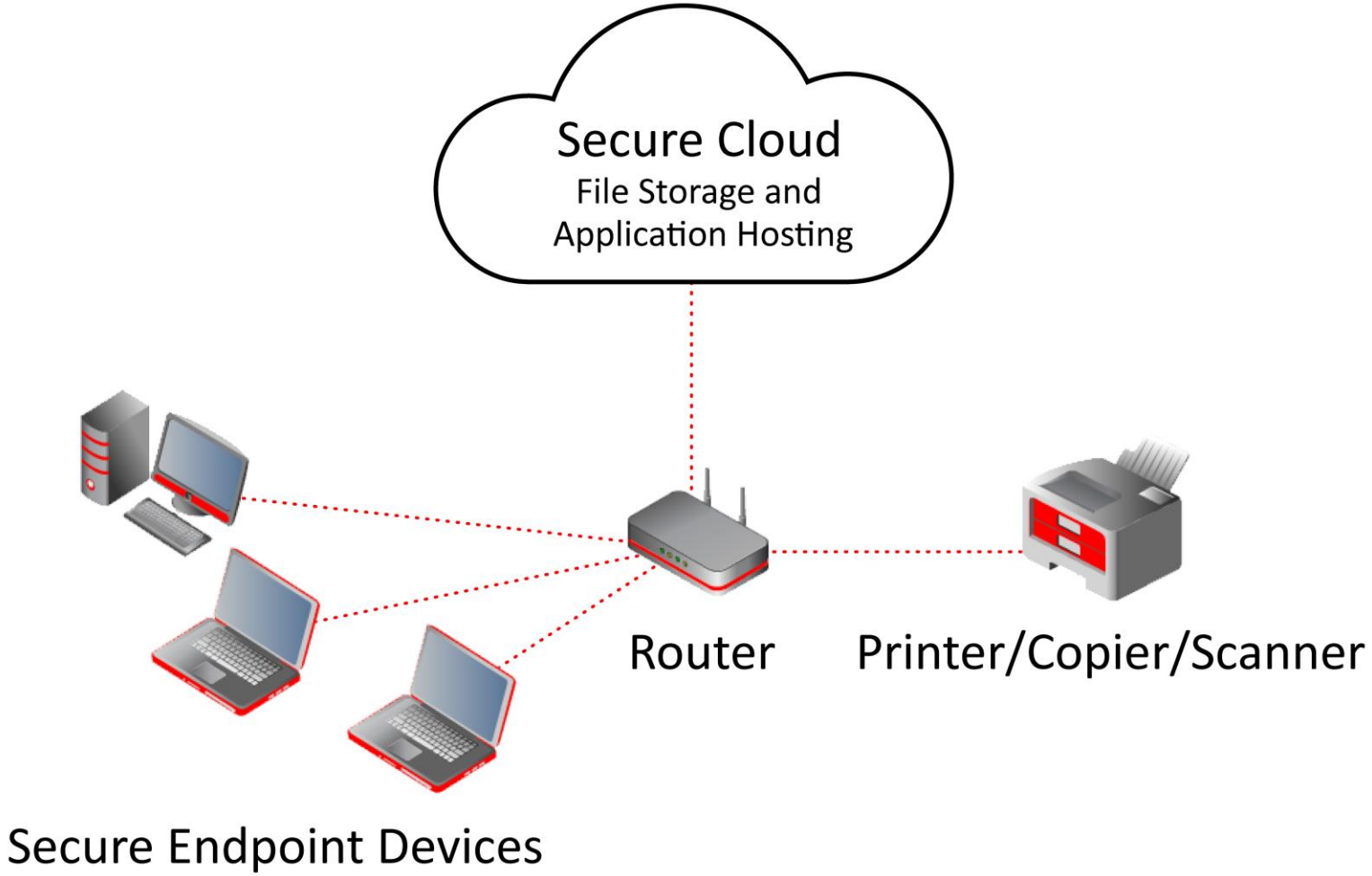
CORONAVIRUS COVID-19 EXPLOITATION

- Malware infected links containing ransomware, trojans
- Credential phishing
- Product scams

Source: Sophos Security Bulletin February 5, 2020

The Essentials for Secure Computing in Your WFH Environment

OFFICE OF THE FUTURE



© NPC DataGuard 2008-2020

WFH PROTECTION

- ❑ Ensure every computer is secure (slides following)
- ❑ Enable multi-factor authentication wherever possible; Office 365, Salesforce, your service providers sites, VPN's, etc.
- ❑ Ensure all your connections are https
- ❑ Use a VPN when available to connect with your office server
- ❑ Ensure you have had a professional look at your Remote Desktop setup

WFH PROTECTION

- ❑ Ensure that home Wi-Fi:
  - ❑ Has a strong, long password that has been changed from the default
  - ❑ WPA2 level security is enabled
  - ❑ The home router is patched and up-to-date
  - ❑ The router's firewall, if present, is enabled
  - ❑ Has an obscure SSID, or disable SSID broadcast

WFH PROTECTION – PERFORMANCE ISSUES

- ❑ Ensure adequate bandwidth and a reliable connection
  - ❑ Test your connection – e.g. www.speedtest.net
    - ❑ At least 25 Mbps down, 10 Mbps up
  - ❑ Limited or unreliable bandwidth can look like poor computer performance, especially for SharePoint and Teams video
  - ❑ Consider an Ethernet-over-Power or Wi-Fi Booster
- ❑ Ensure an adequate computer with a current operating system
  - ❑ For SharePoint
    - ❑ Minimum 8GB of RAM memory, SSD drive
    - ❑ Recommend 16GB of RAM memory, fast SSD drive

WFH PROTECTION

- ❑ Train your team in safe computing
- ❑ Set up a weekly meeting to talk about operational WFH issues and security
- ❑ Remind to double-down on company data handling policies
- ❑ Provide staff a dedicated WFH device, not to be used for recreation
- ❑ Do a password audit
- ❑ Ensure you are backing everything up

WFH PROTECTION

- Don’t forget about physical workspace security
  - A separate, low-traffic area is a top WFH recommendation anyway
- Advise staff to sanitize their equipment and workspace daily https://store.hp.com/us/en/tech-takes/how-to-clean-laptop-screen
- Staff may be more distressed than they are showing. When you are stressed you make mistakes. Do extra video conferencing, calls, chats, etc.

PROTECT YOUR ENDPOINT DEVICES

- ❑ Ensure you have up-to-date and fully patched:
  - ❑ Computer BIOS, operating system, office suite
  - ❑ System apps like Java and Adobe
  - ❑ Web browser
  - ❑ Anti-malware suite
- ❑ Enable personal firewall on endpoint computers
- ❑ Only do your work on a secured device
- ❑ Use a secure file sharing solution to eliminate sending files through email
- ❑ Change default passwords on all IoT devices

TRAIN YOUR STAFF

- ❑ Don’t click what you don’t know:
  - ❑ Links or attachments in unexpected emails
  - ❑ Websites you are uncertain of
- ❑ Observe error and warning messages from your computer
- ❑ Observe email addresses
- ❑ Establish email source and address verification process

PROTECT YOUR SYSTEMS

- ❑ Use strong, unique passwords, change occasionally on computers and systems
- ❑ Apply principles of least privilege for user access, lock admin accounts
- ❑ Employ adequate spam email filtering and content scanning, provided by your ISP, email service, or optionally on your firewall
- ❑ Know who and what is connecting to your network; guests, employee devices, etc.
- ❑ Conduct a risk assessment, preferably using a security professional
- ❑ Ensure you have adequate cyber insurance, and your new method of operation is covered

NPC

PLAN 1 – INCIDENT RESPONSE PLAN

The plan I would do first if I had no other plan or policy in place:

- ❑ What are your particular risks, what type of incident would have the most impact
- ❑ Have an Incident Response Team organized and at the ready
- ❑ Ensure a lawyer, your insurance agency, and your compliance professional are part of the team, and are immediately contacted in the plan
- ❑ Map out how you will communicate within the team
- ❑ Know your regulator or professional association reporting requirements and timelines
- ❑ If you do business internationally or extra-provincially, know your responsibilities in those territories
- ❑ Map out how you will mitigate damage, quell the attack
- ❑ Ensure you are using professional technical services immediately to minimize damage, preserve evidence
- ❑ Perform a post-mortem, and extensive post-event technical testing
- ❑ Test and revisit the plan at least annually

OFFICE 365

A suite of mobile, desktop and cloud-based productivity tools on a unified communication and collaboration platform

Teams
Chat, Meetings, Apps, Calls

OneDrive
My Files Sync

SharePoint
Intranet, Shared Docs

NPC

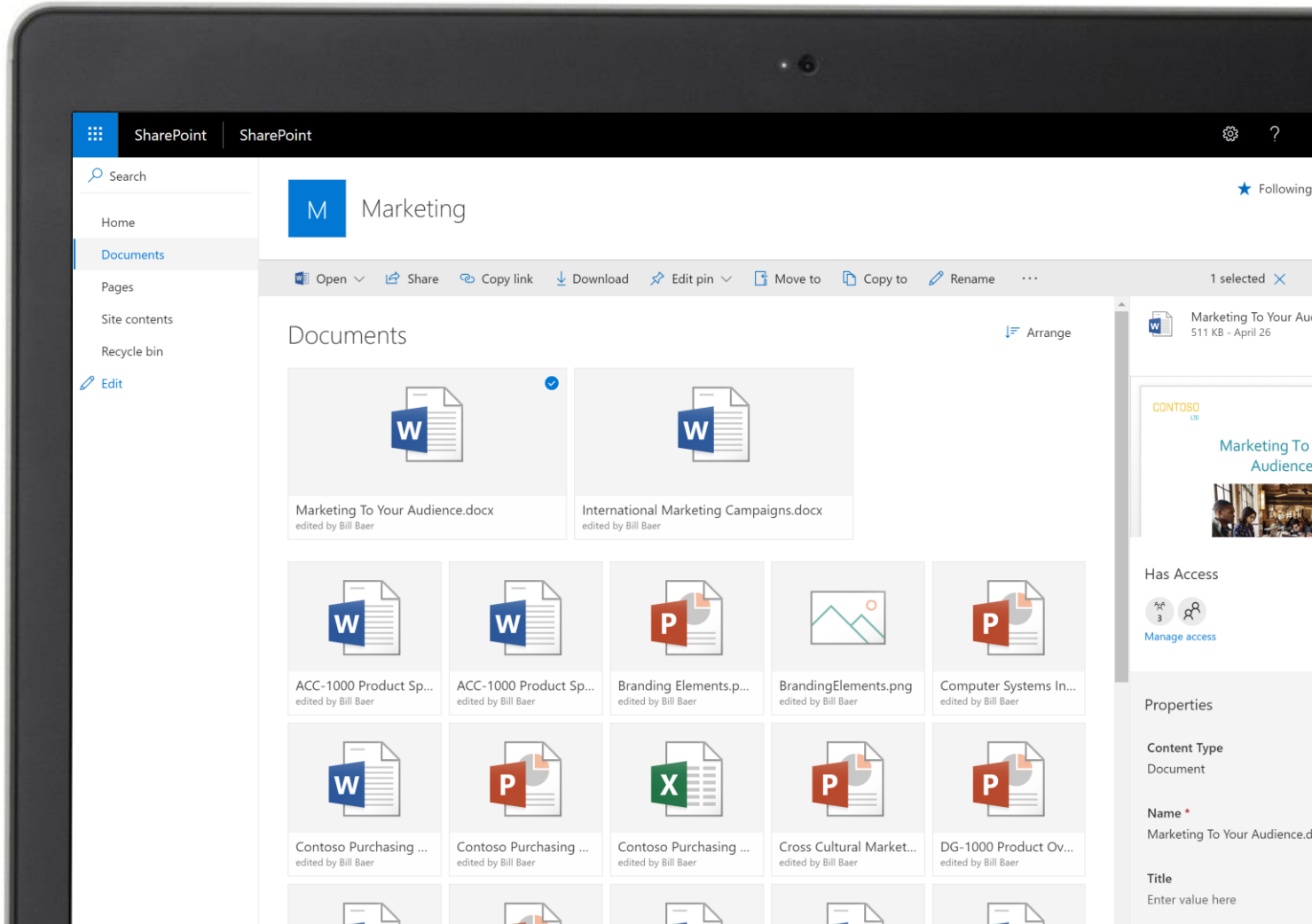
OFFICE 365 LICENSE LEVELS

	Core Collaboration and Communication Services					
	OneDrive	OneDrive Business	Skype	SharePoint	Teams	Exchange
For Home						
Office 365 Home	✓		✓			
Office 365 Personal	✓		✓			
Office 365 Office Home & Student						
For Business						
Office 365 Business	✓					
Office 365 Business Premium		✓		✓	✓	✓
Office 365 Business Essentials		✓		✓	✓	✓
For Enterprise						
ProPlus, E1, E3, E5	Variations on the above with greater capacities, analytics, and advanced, deployment, compliance and data and user management tools					

All licenses include Word, Excel, PowerPoint either desktop, web and/or mobile version

NPC

Connect to Your Data with SharePoint



ONEDRIVE v ONEDRIVE FOR BUSINESS

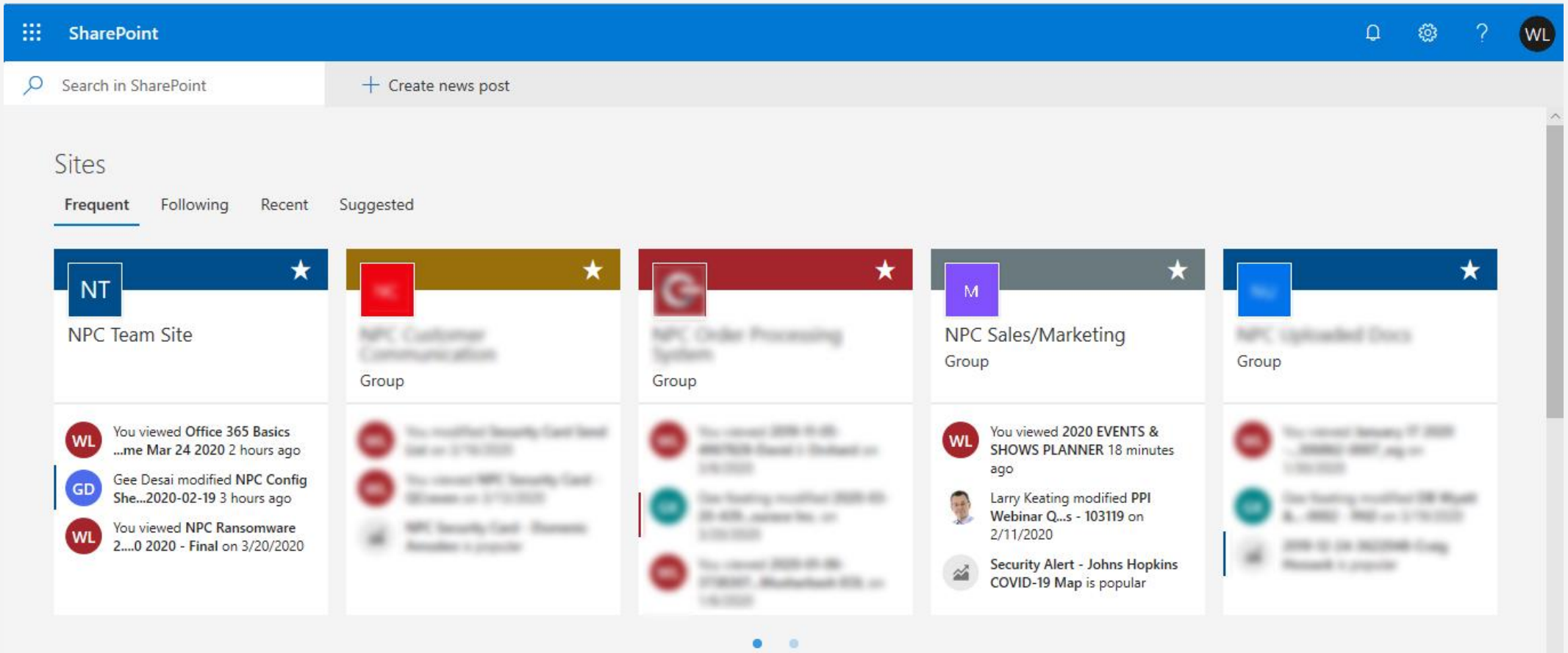
- Both just say OneDrive on the interface
- OneDrive or “OneDrive Personal” is
  - Free storage space in the cloud for personal use
  - Designed for one person
  - Can be used to share files, more or less 1:1
  - Lacks some collaboration, versioning, sharing capabilities
- OneDrive for Business is synchronized to SharePoint, a central file storage and collaboration site for a team
  - Individual file storage space that is integrated with the businesses’ corporate control of information, compliance, archiving, etc.
  - A collaboration, synchronization, sharing control, automated file saving tool, and more…

NPC

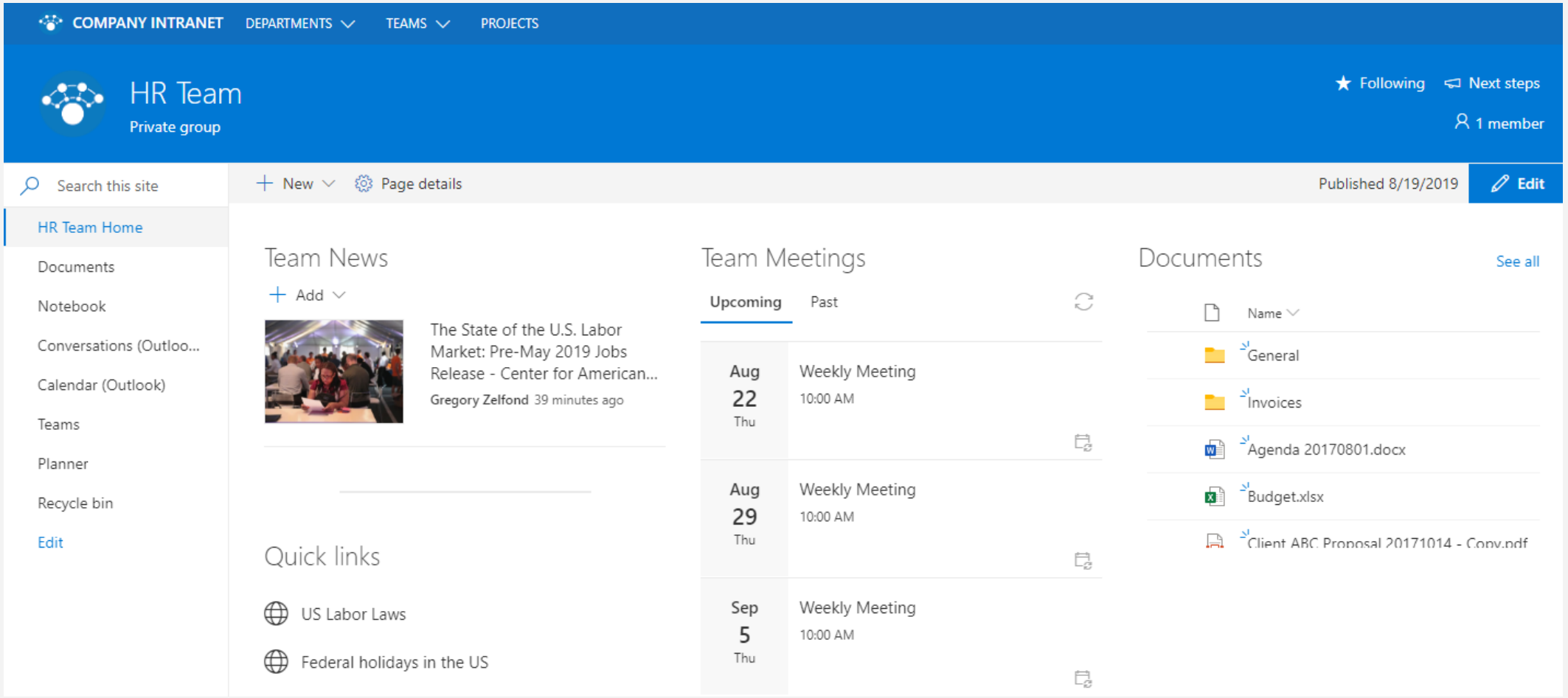
SHAREPOINT – FILE STORAGE, SHARING AND COLLABORATION

- Replaces your file server, USB drives, or email file sharing
- Mobile access everywhere
- Powerful collaboration and integrated tools and apps
  - Project Planner, Power Automate, etc.
- Generate links for secure file sharing, or grant controlled access
- “Data sovereign” in certified secure facilities meeting compliance requirements
- At first, it may be more complicated “knowing where you are” when in SharePoint

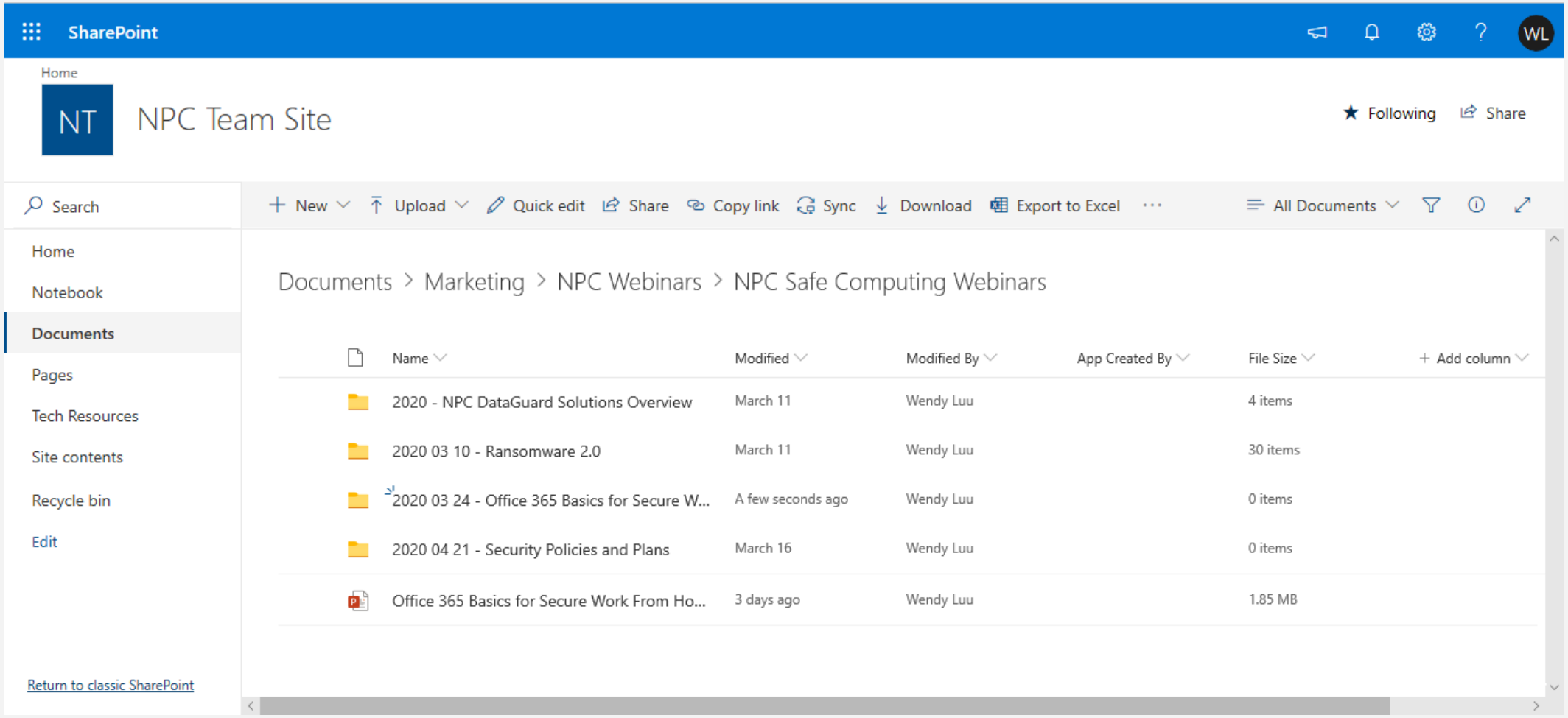
USING SHAREPOINT - SITES



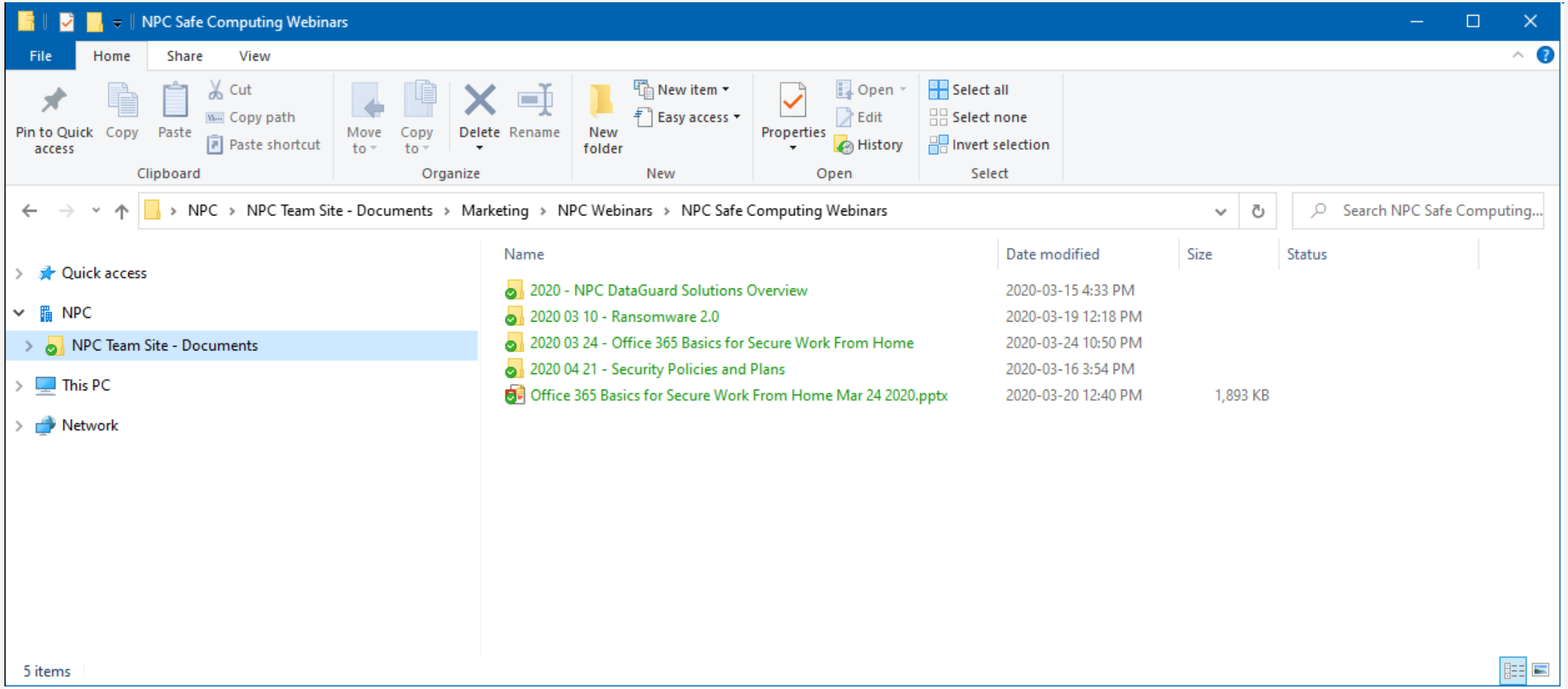
USING SHAREPOINT – TEAM SITE EXAMPLE



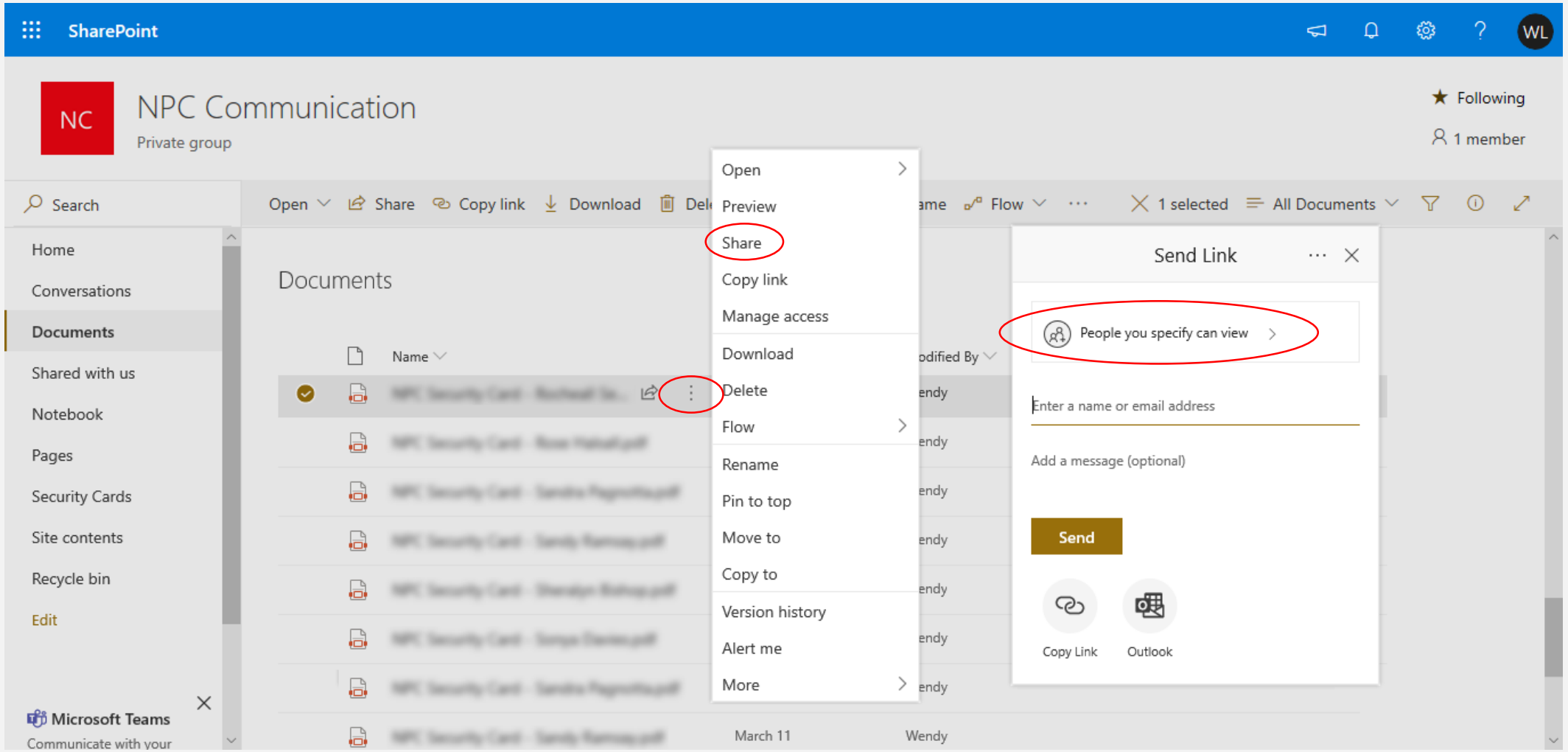
USING SHAREPOINT - DOCUMENTS



USING SHAREPOINT - SEAMLESSLY



USING SHAREPOINT – SECURE SHARE



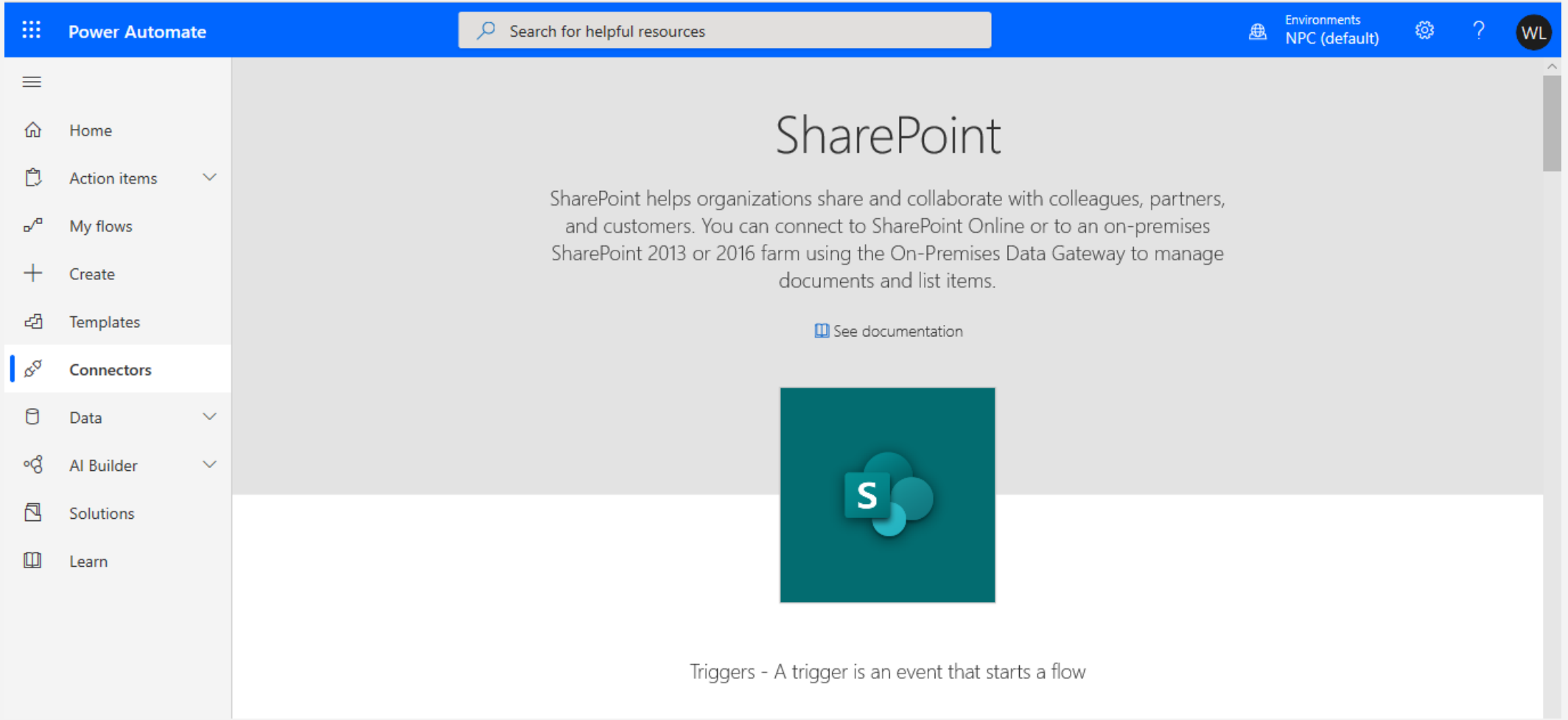
USING SHAREPOINT – SETUP POINTERS

- Know specific levels of access by user, what configuration settings you require
- Ensure the source data is malware and corruption free
- SharePoint is not a backup
- Very long files names (name and path exceeds 400 characters) will not migrate
- Certain illegal file extensions such as .lock .con .prn, or special characters like *:<>?/, etc. will not migrate
- PST files in the folders will replicate on each synchronization
- Files greater that 15GB will not sync

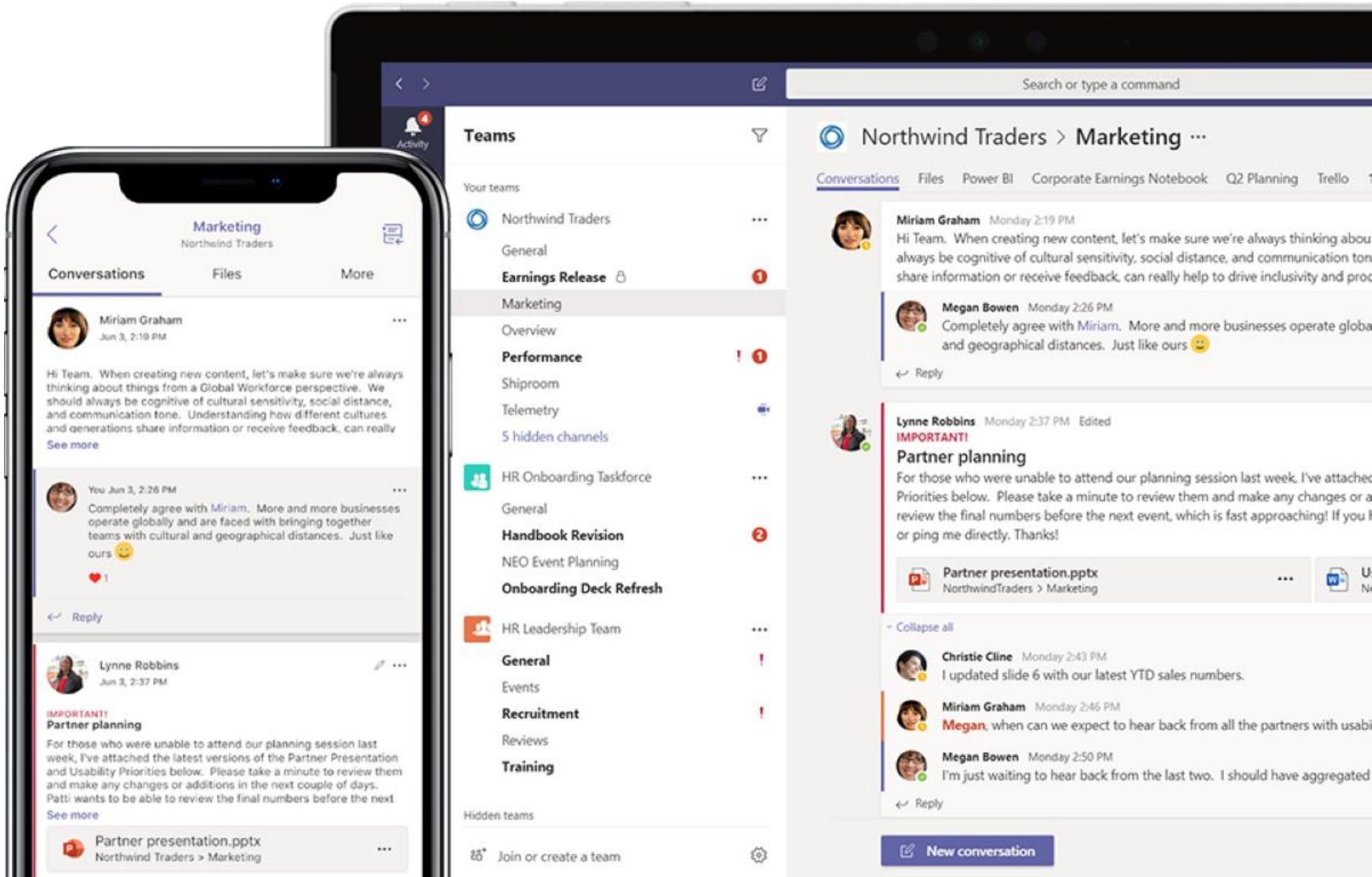
USING SHAREPOINT – SETUP POINTERS

- Do not “copy and paste” your data from a server or drive into SharePoint directly:
  1. Link to the site via SharePoint
  2. Use File Explorer to move the data into the local site
  3. Let it sync up to the site
  4. Sync no more than 100,000 files in one sweep

USING SHAREPOINT – ~~FLOW~~ POWER AUTOMATE



Connect People with Teams



SKYPE v SKYPE FOR BUSINESS v TEAMS

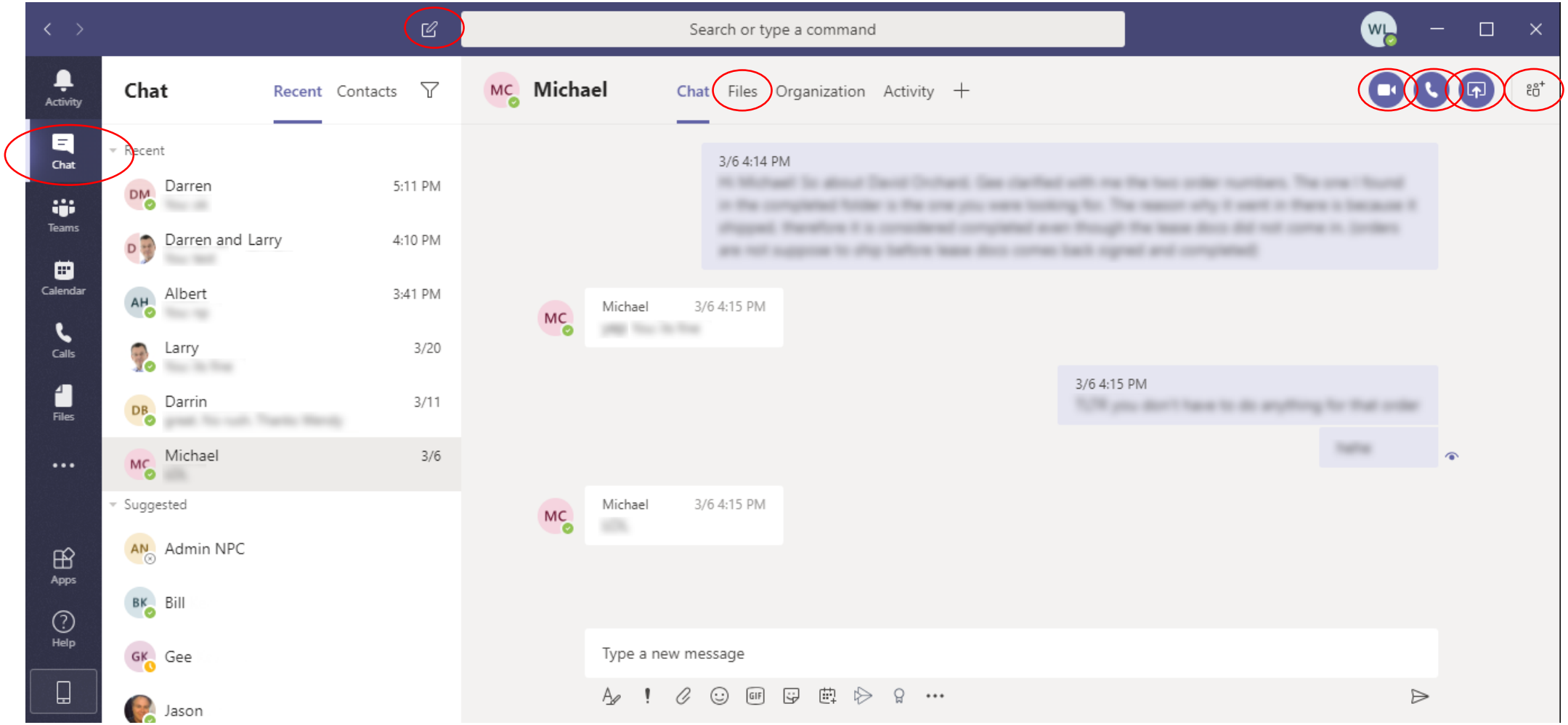
- Skype
  - Basic voice, chat and video conferencing

- Skype For Business
  - Larger meetings (25 v 250)
  - Integration with Office Apps
  - Security controls and permissions
  - Conference call set up and lobby, etc.
  - Skype for Business Online, not Server, to be discontinued in 2021 - auto upgrades already occurring

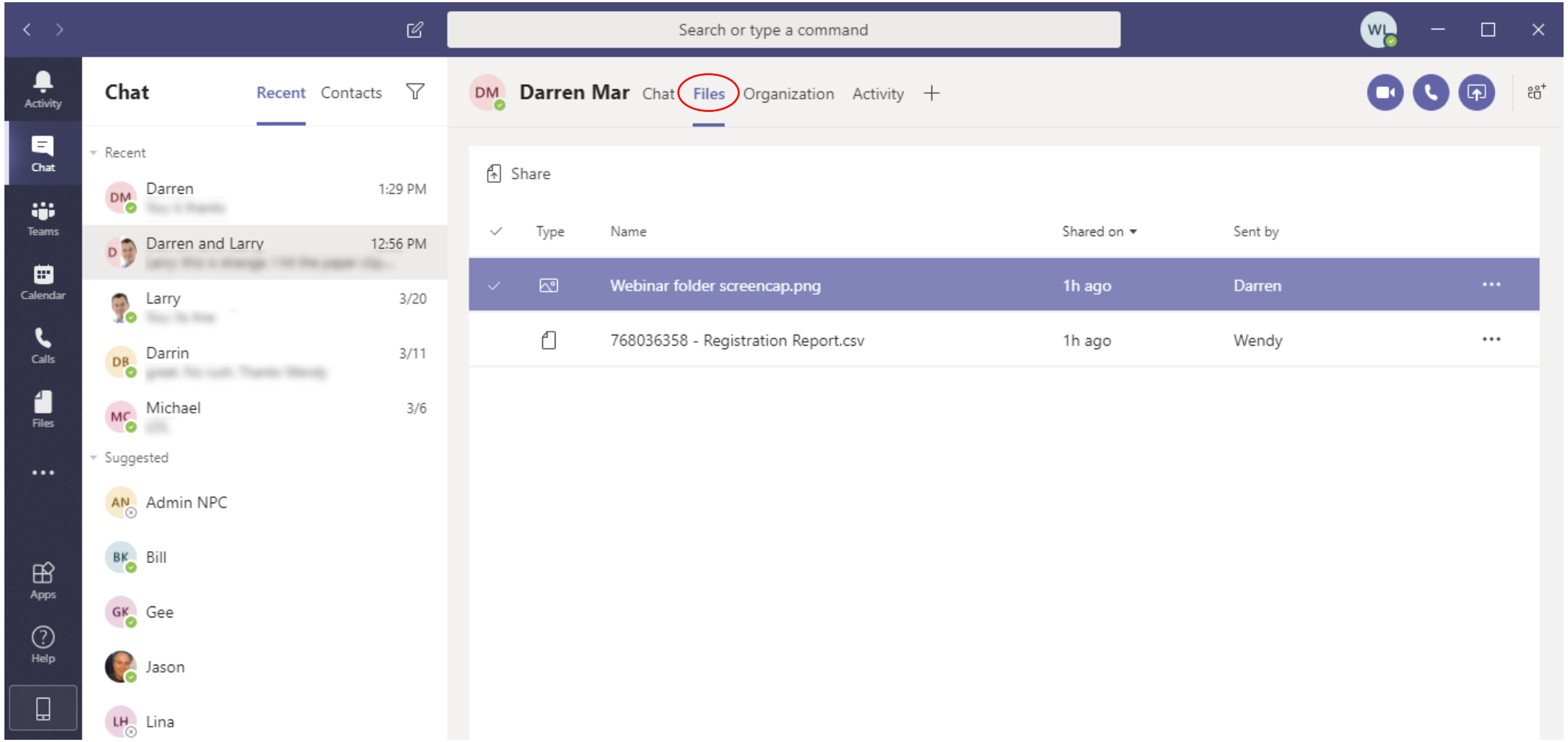
TEAMS

- Everything brought together, unified communications
  - Chat, video, calls, conference calls, screen sharing, set appointments, mark events, share files, create groups, call recording, guest access

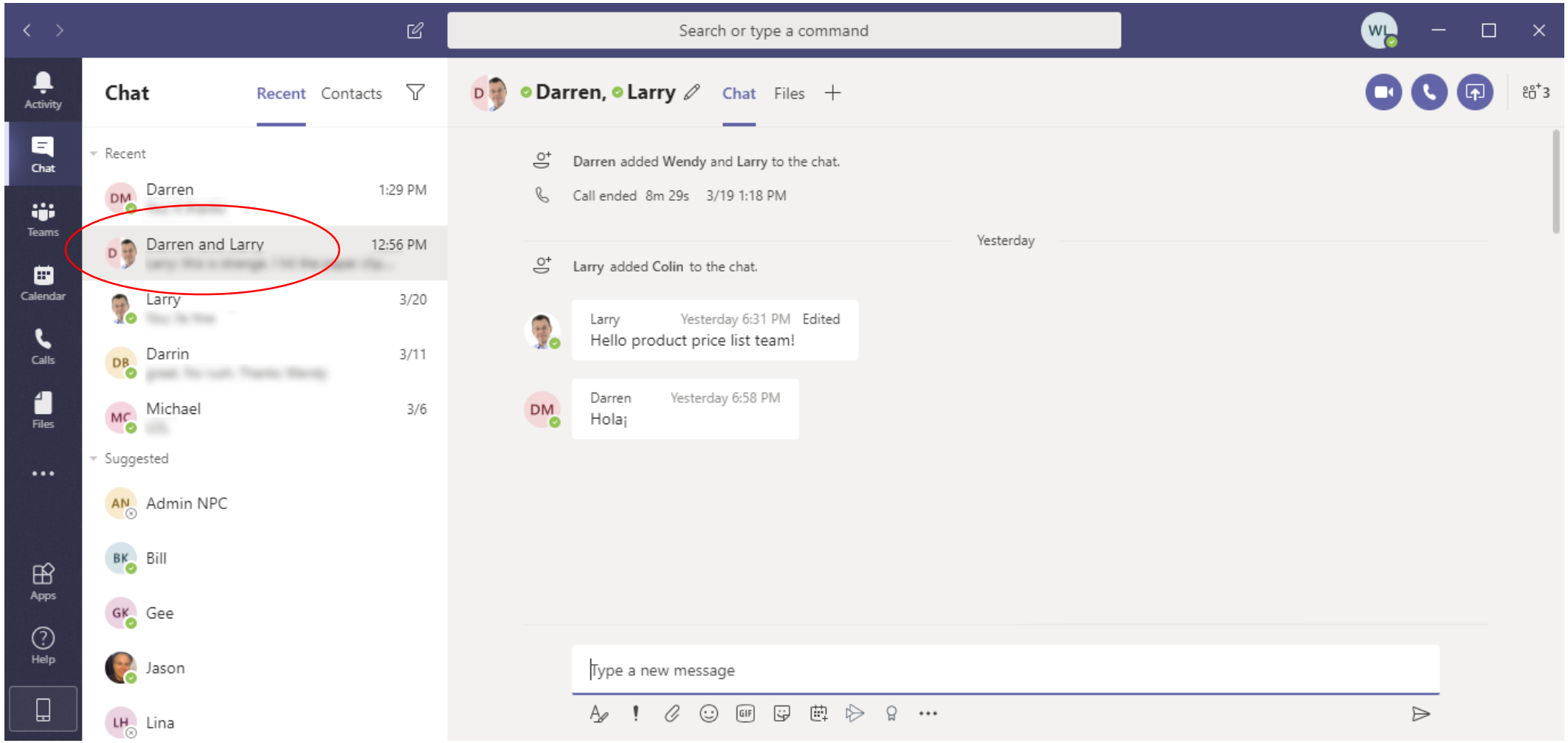
USING TEAMS–CHAT



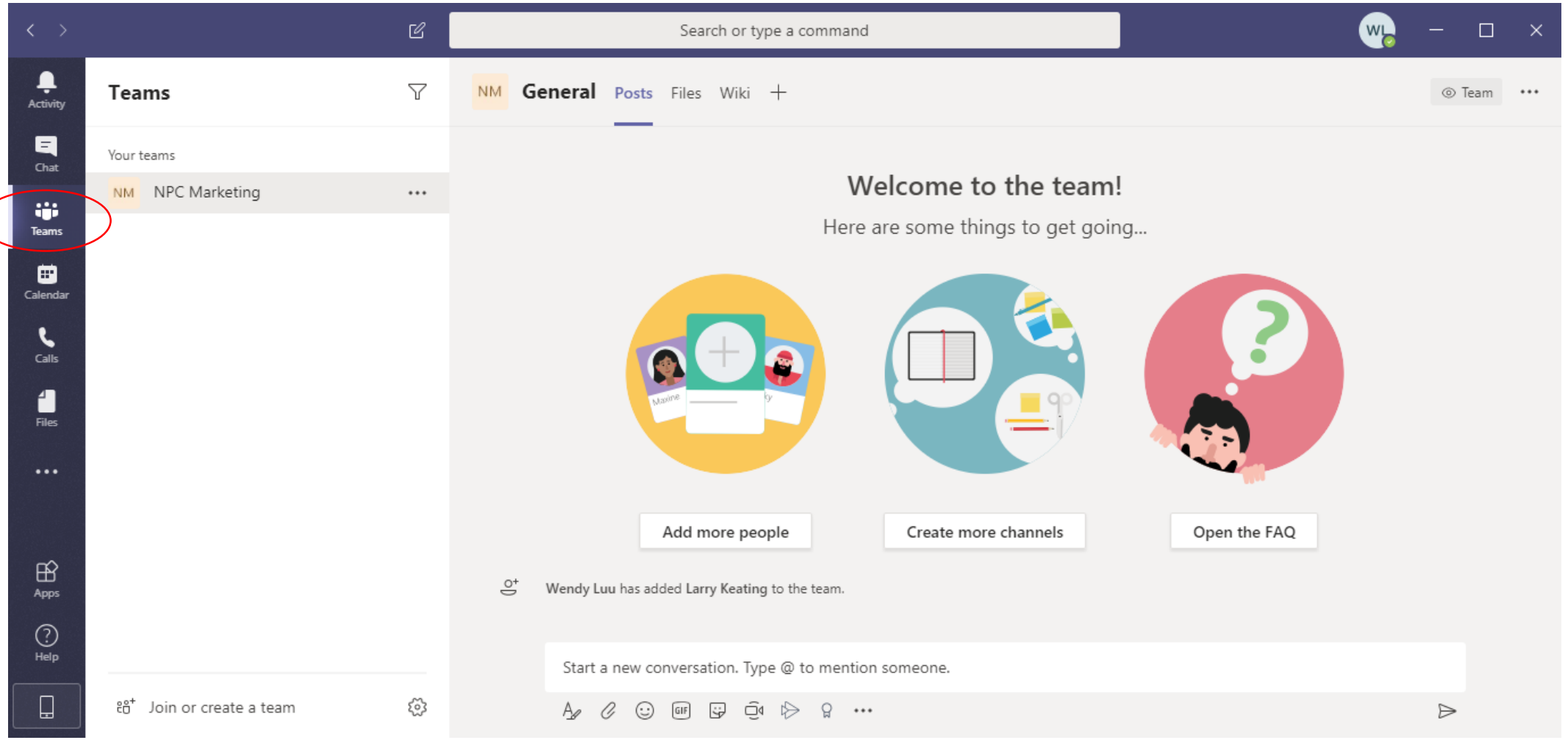
USING TEAMS–CHAT–INTEGRATED FILE ACCESS



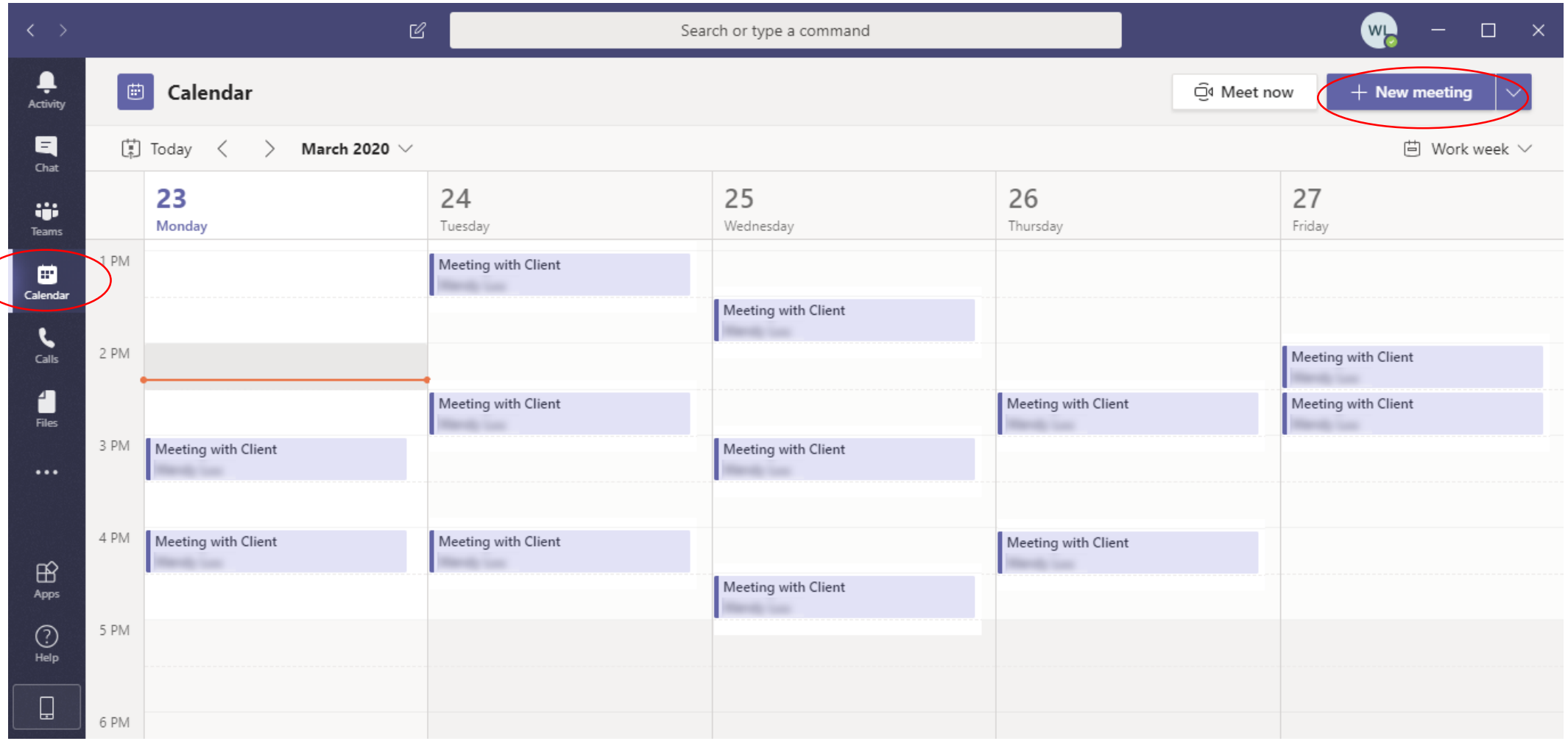
USING TEAMS–GROUP CHAT



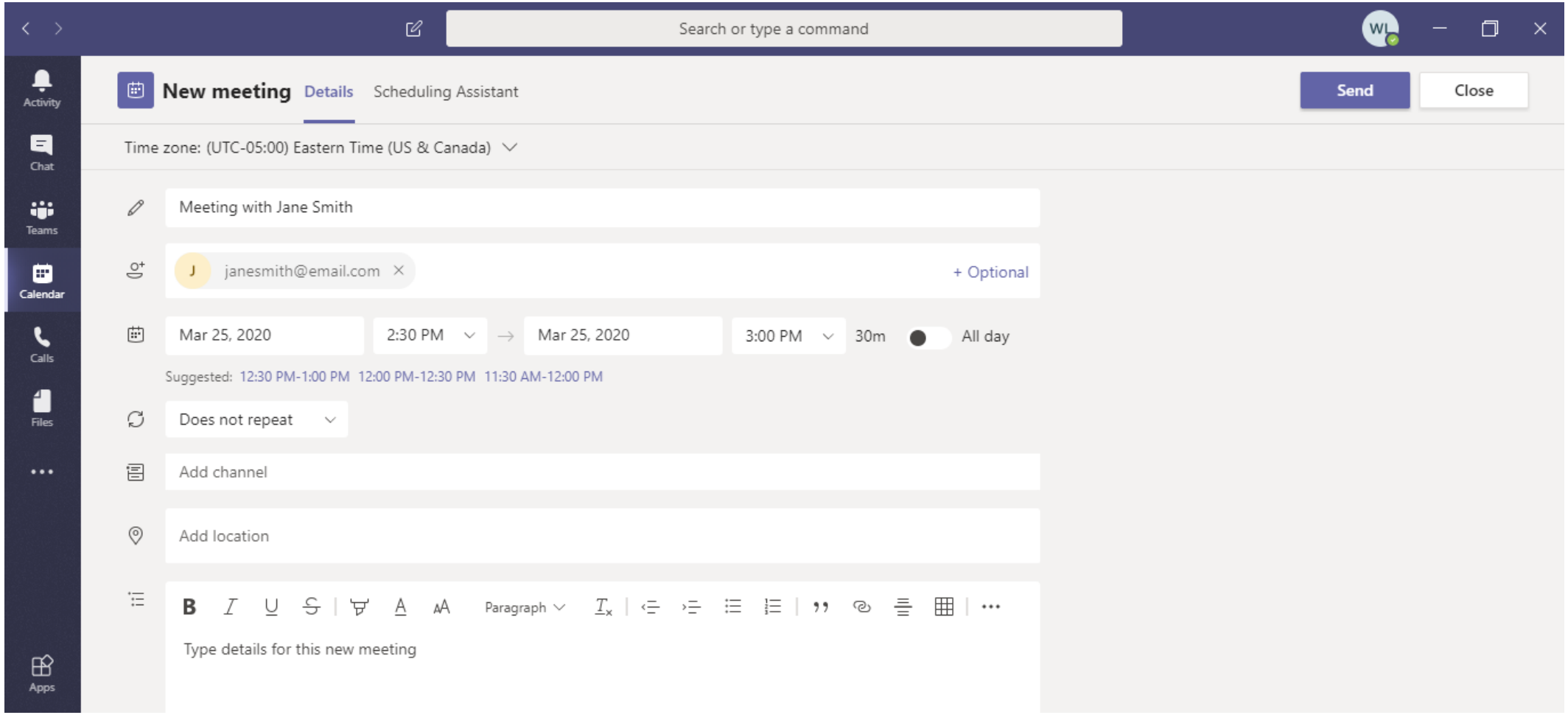
USING TEAMS–CREATE YOUR TEAM



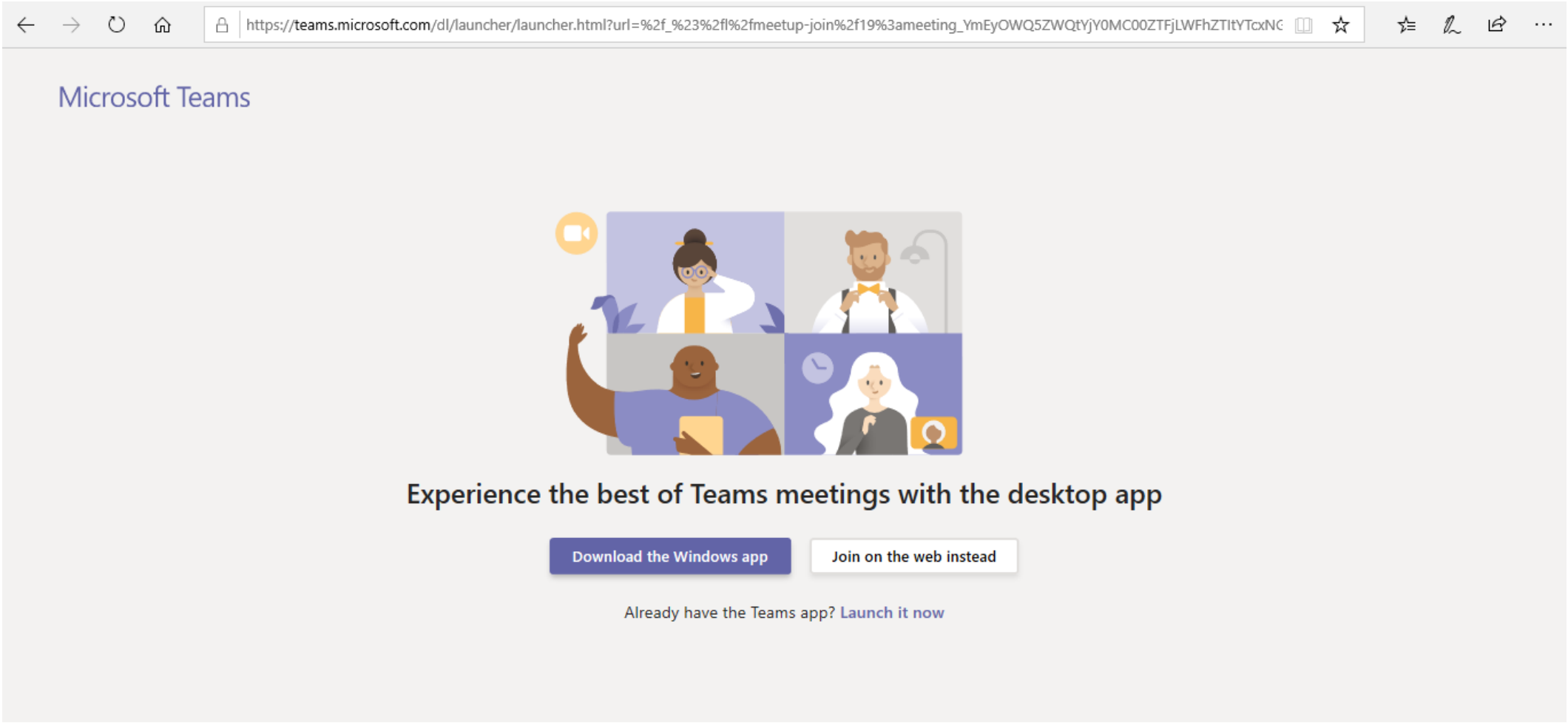
USING TEAMS–CALENDAR



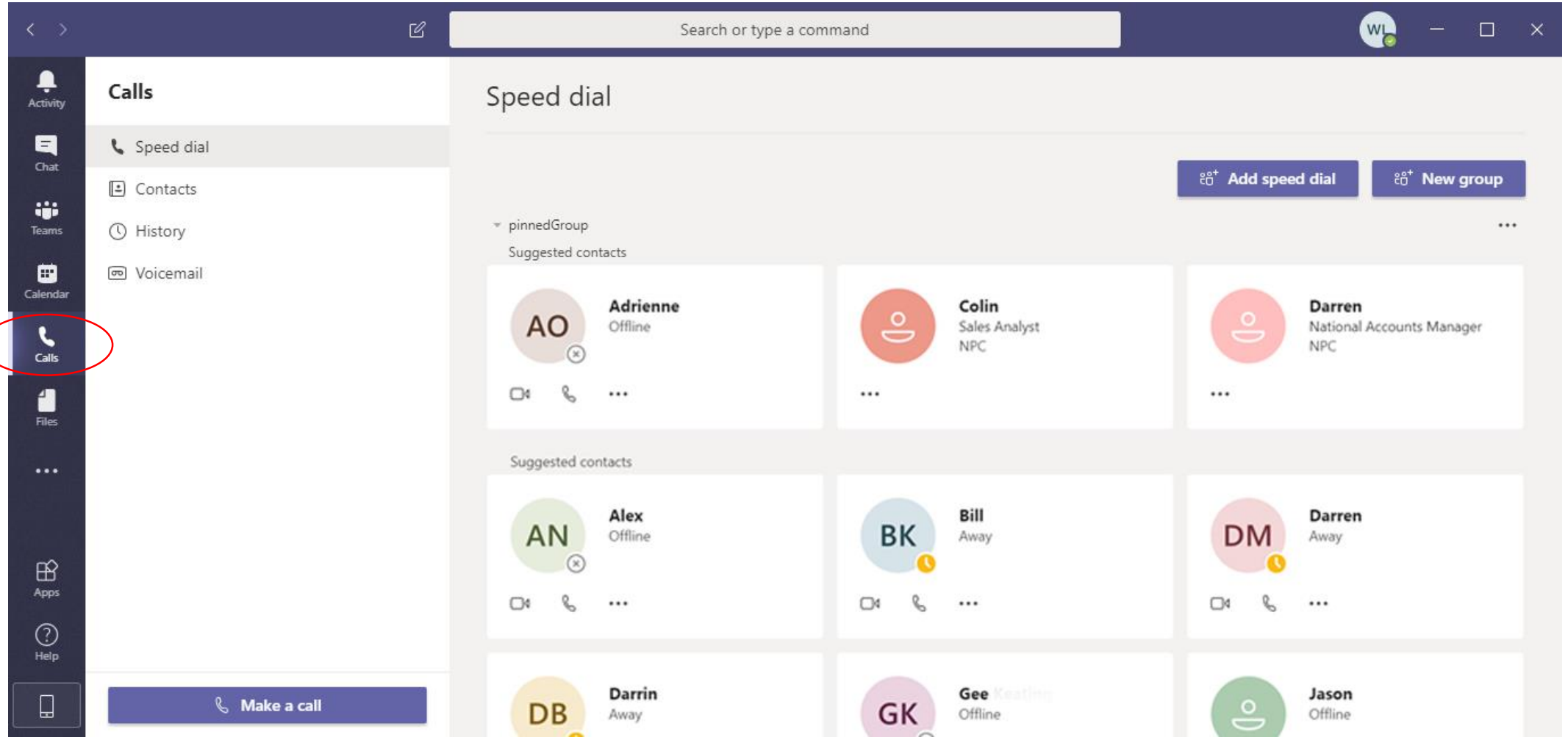
USING TEAMS – CREATE NEW MEETING



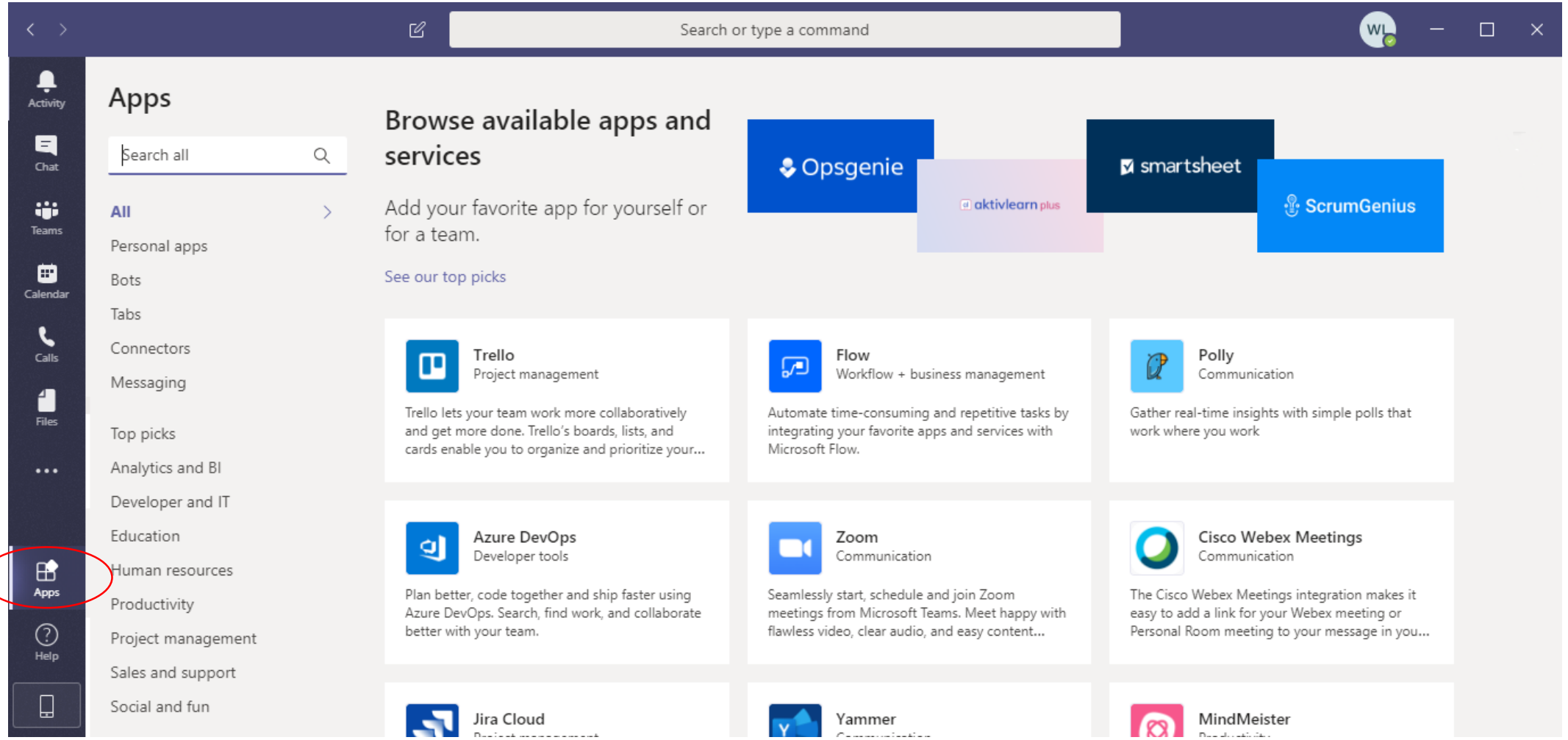
USING TEAMS – MEETINGS



TEAMS – CALLS


Search or type a command
Activity
Chat
Teams
Calendar
Calls
Files
Apps
Help
Calls
Speed dial
Contacts
History
Voicemail
Make a call
Speed dial
Add speed dial
New group
pinnedGroup
Suggested contacts
AO
Adrienne
Offline
Colin
Sales Analyst
NPC
Darren
National Accounts Manager
NPC
Suggested contacts
AN
Alex
Offline
BK
Bill
Away
DM
Darren
Away
DB
Darrin
Away
GK
Gee
Offline
Jason
Offline

USING TEAMS–APPS INTEGRATION



UPCOMING NPC WEBINARS

- April 2th – 30 minutes **NPC Solutions Overview**
- April 21th – 60 minutes **Security Policies and Plans Overview for the SMB Professional**
- June 9th – 60 minutes **BEC (Business Email Compromise) Attacks and How to Prevent Them**
- July 14th – 60 minutes **Building an Incident Response Plan for the SMB**

NPC SECURITY ALERTS

Sign up

www.npcdataguard.com/alerts

Q & A

Thank You
Please be safe, stay healthy

Larry Keating
lkeating@npcdataguard.com
905 305 6501

Darren Mar
dmar@npcdataguard.com
905 305 6513

NPC™

Smarter Computing