Student Name: Worlanyo Akpatsa Term: Winter 2025
Student ID: 101590287

Case Project: Implementing and Managing Microsoft 365 Environment for a Mid-Sized Organization

Objective: To provide hands-on experience in implementing, configuring, and managing a Microsoft 365 environment for a fictional mid-sized organization named "TechSolutions Inc."

Scenario: TechSolutions Inc. is a mid-sized IT services company with 300 employees. The company is transitioning to Microsoft 365 to improve collaboration, security, and productivity. As part of the IT team, you are responsible for setting up and managing the Microsoft 365 environment. This case project will cover various aspects of Microsoft 365, including user and group management, security and compliance, and service configuration.

Tasks:

Task 1: Setting Up and Configuring User Accounts

1. **Bulk Import Users**:
    - Use the Microsoft 365 admin center to bulk import 10 users from a CSV file.
    - Assign appropriate licenses (Microsoft 365 E3 or E5) to the imported users.
2. **Configure User Profiles**:
    - Ensure each user has a profile picture, contact information, and job title set.
    - Configure user settings to include organization-specific information.
3. **Create Office 365 Groups**:
    - Create three Office 365 groups for different departments: IT, HR, and Marketing.
    - Add users to their respective groups.
4. **Configure User Permissions**:
    - Assign specific permissions to the HR group to access sensitive HR documents in SharePoint.
    - Ensure the Marketing group has permission to create and manage Microsoft Teams.

Task 2: Implementing Security Measures

1. **Set Up and Configure Microsoft Defender for Office 365**:
    - Access the MS Defender and navigate to Secure Score.
    - Ensure that Safe Links and Safe Attachments have been enabled for all users.

- Navigate to Policies and rules, then configure at least one policy to protect against phishing, malware, or spam.

2. **Set Up Data Encryption**:
   - Configure Microsoft 365 Message Encryption.
   - Ensure that emails from inside the organization are automatically encrypted. (Hints: Navigate to Exchange admin center, and then Rules)

Task 3: Configuring and Managing Collaboration Tools

1. **Set Up SharePoint Online**:
   - Create an online SharePoint site for each department (IT, HR, Marketing).
   - Configure document libraries and permissions for each site.
   - Enable versioning and content approval for the HR document library.
2. **Implement OneDrive for Business**:
   - Configure OneDrive settings to restrict external sharing.
   - Enable file retention policies to ensure data is retained for at least five years.
   - Set up a policy to automatically move old files to the Recycle Bin after a year.
3. **Set Up Viva Engage for Enterprise Social Networking**:
   - Configure Viva to allow only internal communications.
   - Set up groups for company-wide announcements and department-specific discussions.
   - Ensure compliance with the company's social media policy.

Task 4: Monitoring and Reporting

1. **Configure Audit Logs**:
   - Enable and configure audit logging in the Microsoft 365 compliance center.
   - Create a custom audit log search to track user activities related to at least one activity in SharePoint such as updating the site content.
2. **Set Up Alerts**:
   - Configure alert policies to notify administrators of suspicious activities, such as multiple failed login attempts or mass deletion of files.

    - Set up notifications for data loss prevention (DLP) policy breaches. (You can navigate to Insider risk management)

3. **Generate Usage Reports**:
    - Use the Microsoft 365 admin center to generate reports on user activity, email usage, and SharePoint site usage.
    - Schedule monthly reports to be sent to IT administrators and department heads.(Optional, you can use Power Automate)
4. **Implement and Monitor Service Health**:
    - Set up service health alerts to notify administrators of any issues with Microsoft 365 services.
    - Monitor the Service Health dashboard regularly to ensure all services are running smoothly.

Deliverables:

- A detailed report documenting each step taken during the project, including screenshots and explanations.
- A summary of configurations and policies implemented, along with their rationale.
- A presentation to the class demonstrating the setup and explaining the choices made during the project.

Assessment Criteria:

- Completeness and accuracy of the tasks performed.
- Understanding and application of Microsoft 365 features and best practices.
- Quality of documentation and presentation.
- Ability to troubleshoot and resolve issues encountered during the project.

~~~~~~
Paste your screenshots here
~~~~~~

~~~~~~

Student Name: Worlanyo Akpatsa Term: Winter 2025
Student ID: 101590287

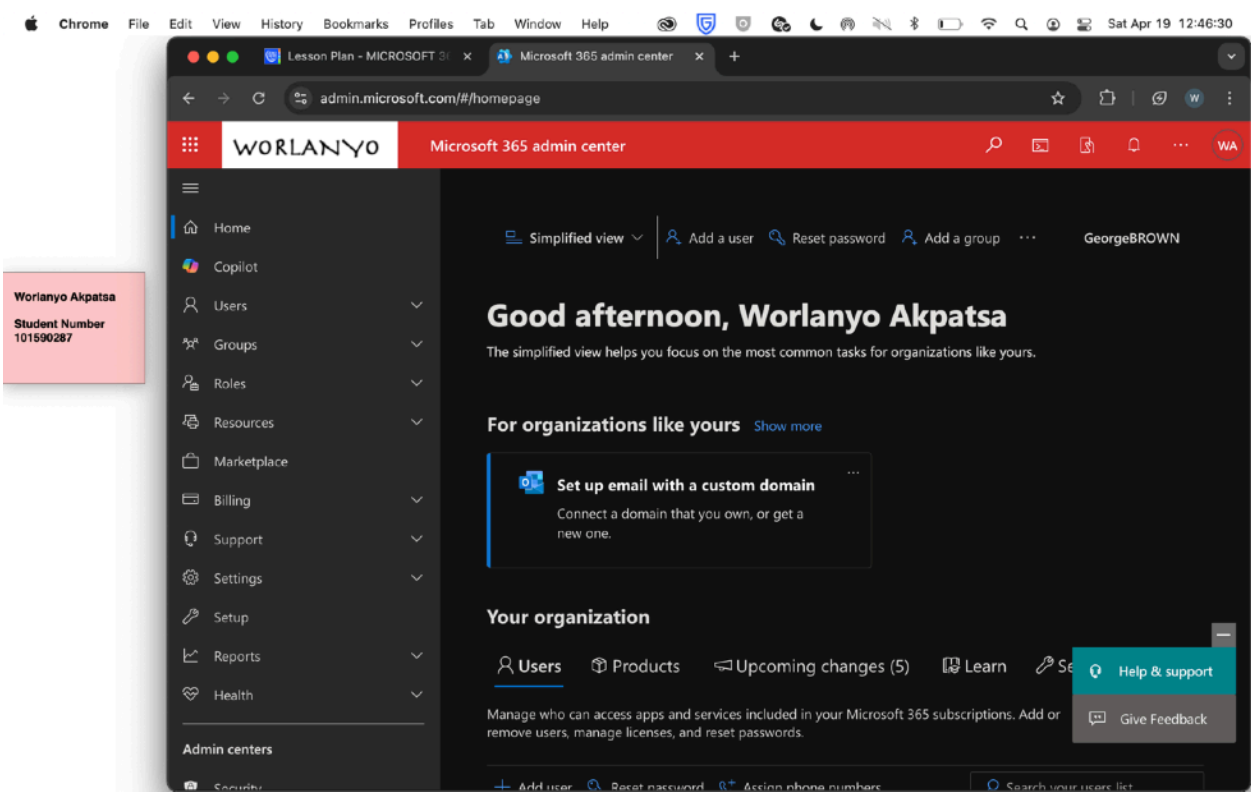
~~~~~~

TASK 1: SETTING UP AND CONFIGURING USER ACCOUNTS

1: Bulk Import Users

1.1: Use the Microsoft 365 Admin Center to bulk import 10 users from a CSV file.

A: Navigate to 365 Admin Center Homepage

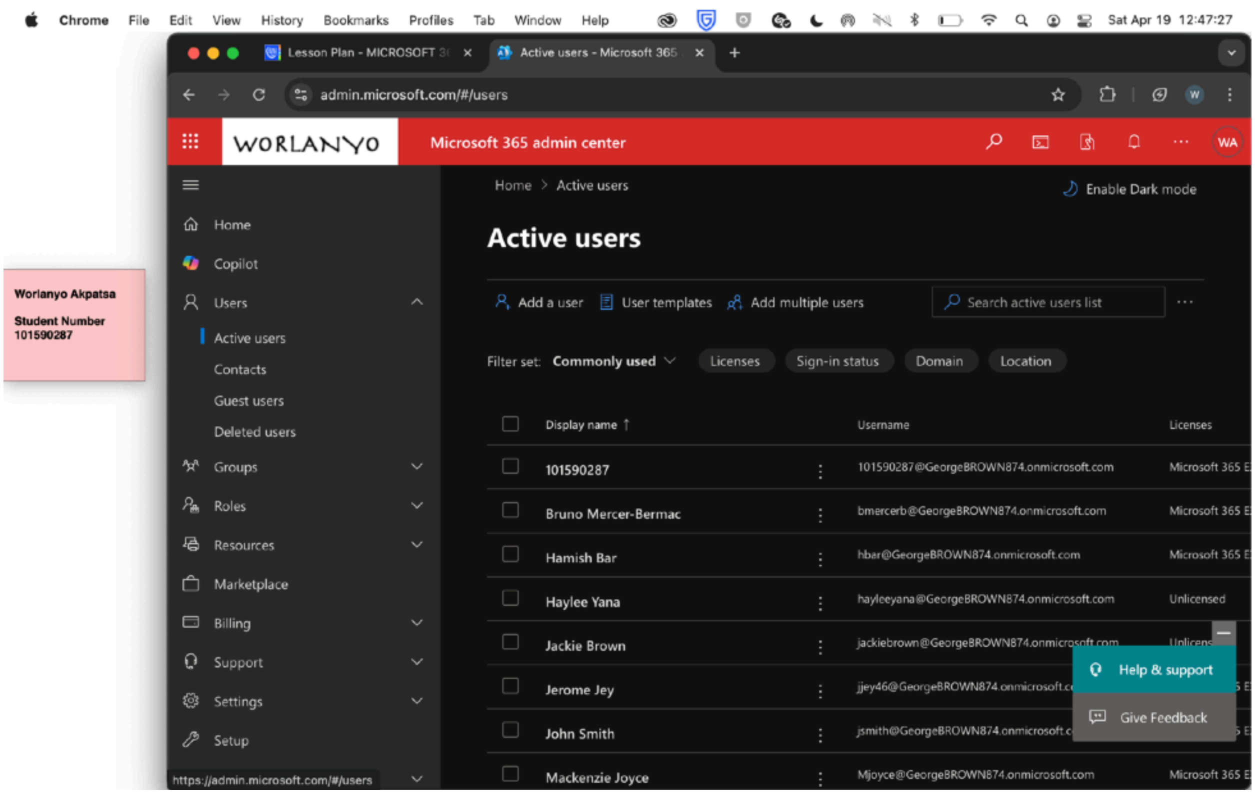


~~~~~~

Student Name: Worlanyo Akpatsa | Term: Winter 2025
Student ID: 101590287

~~~~~~

B: In the left pane, select users->active users

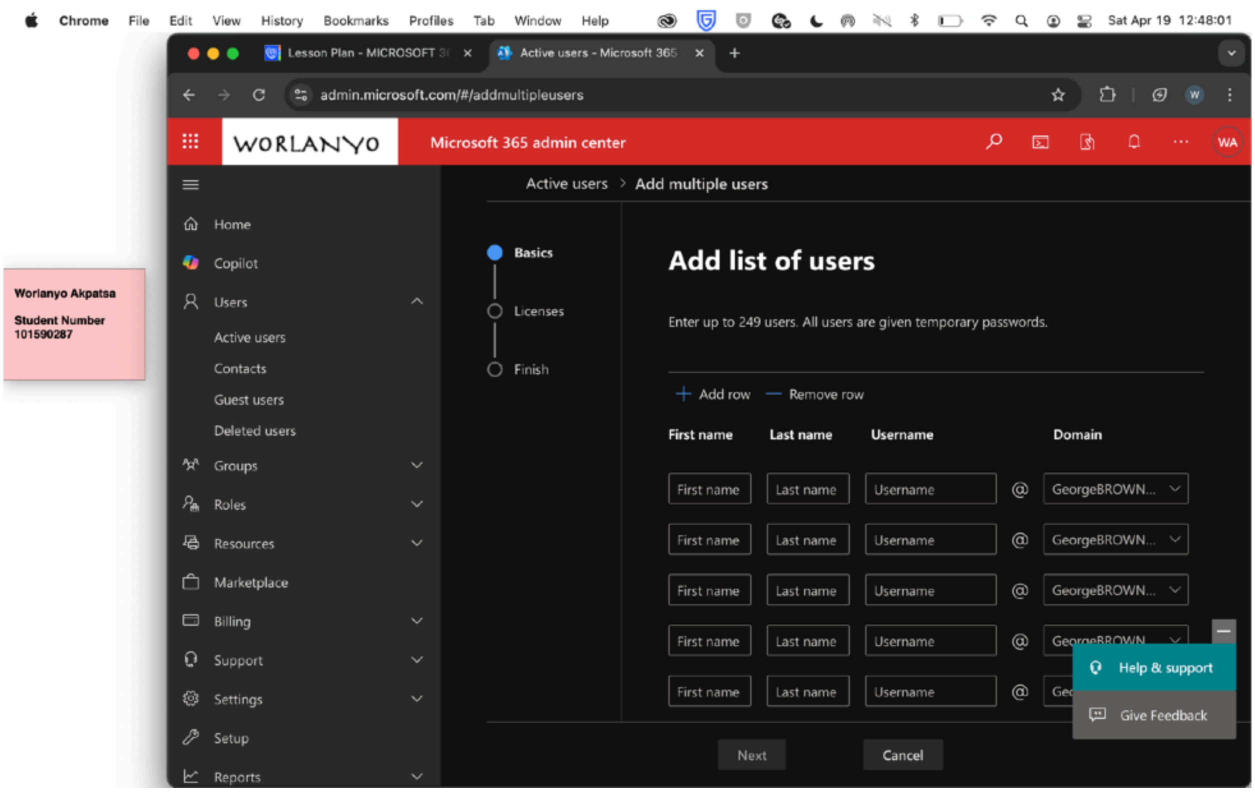


~~~~~~

Student Name: Worlanyo Akpatsa | Term: Winter 2025
Student ID: 101590287

~~~~~~

C: Select "Add multiple users"

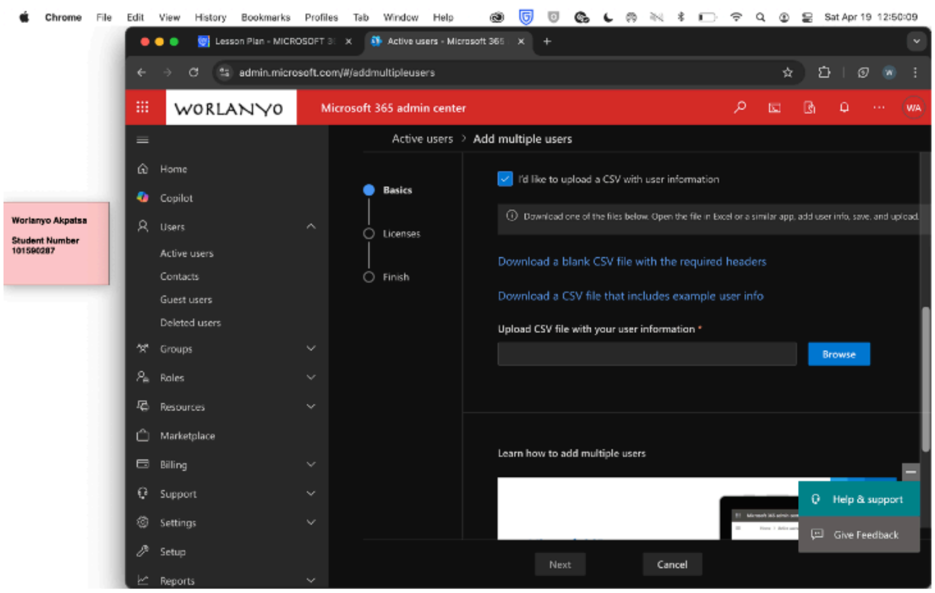


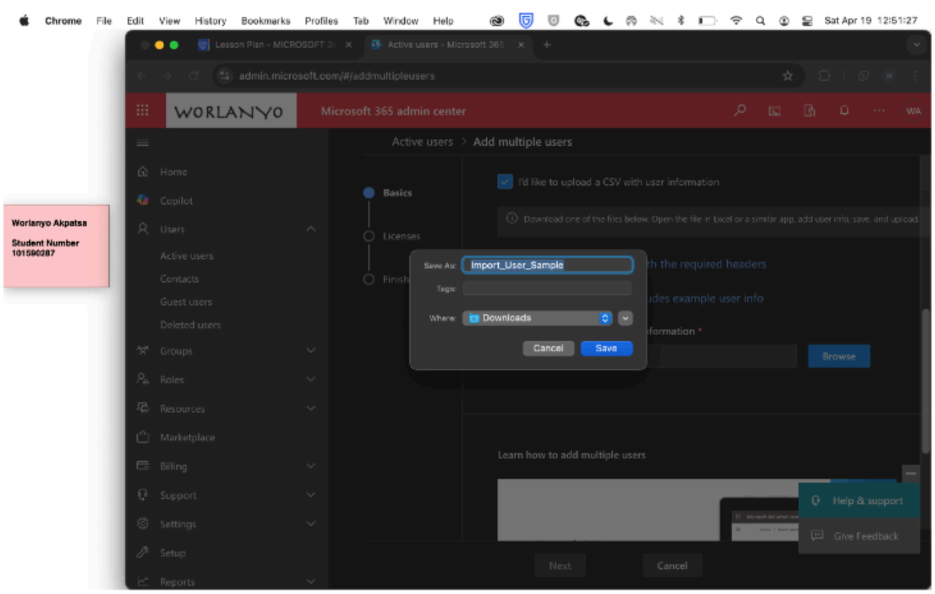
~~~~~~

Student Name: Worlanyo Akpatsa Term: Winter 2025
Student ID: 101590287

~~~~~~

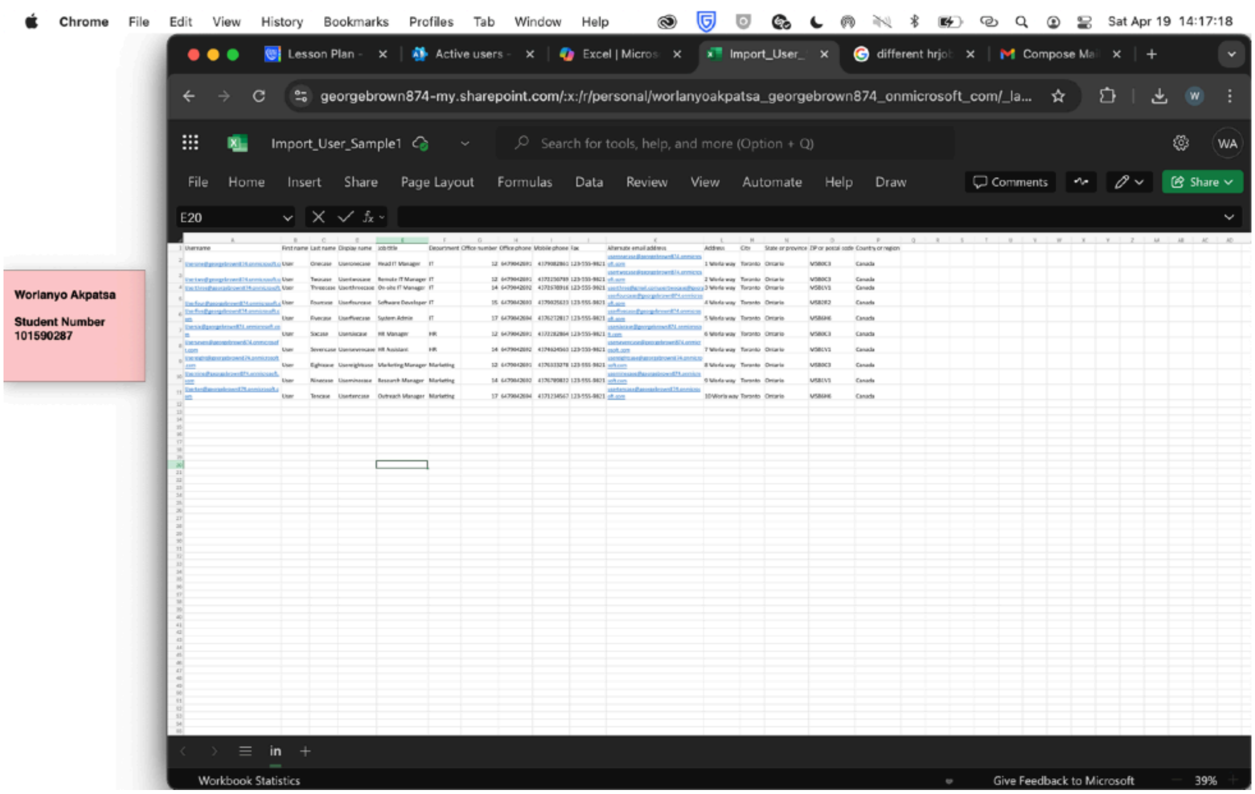
D: Scroll down on the "Add multiple users", select "I'd like to upload a CSV with user information" and download one of the CSV files.



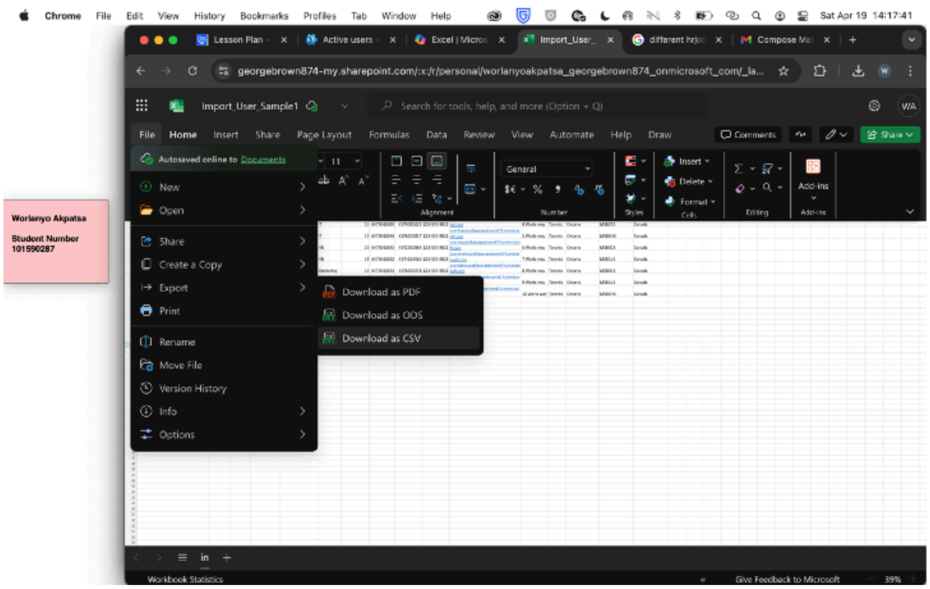


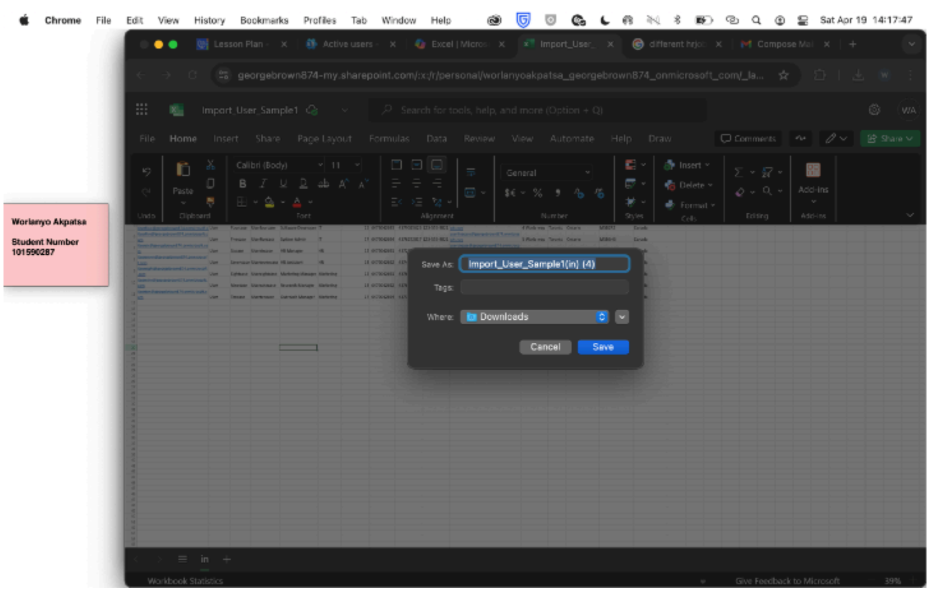
Student Name: Worlanyo Akpatsa
Student ID: 101590287
Term: Winter 2025

E: Editing CSV file (Using Excel)

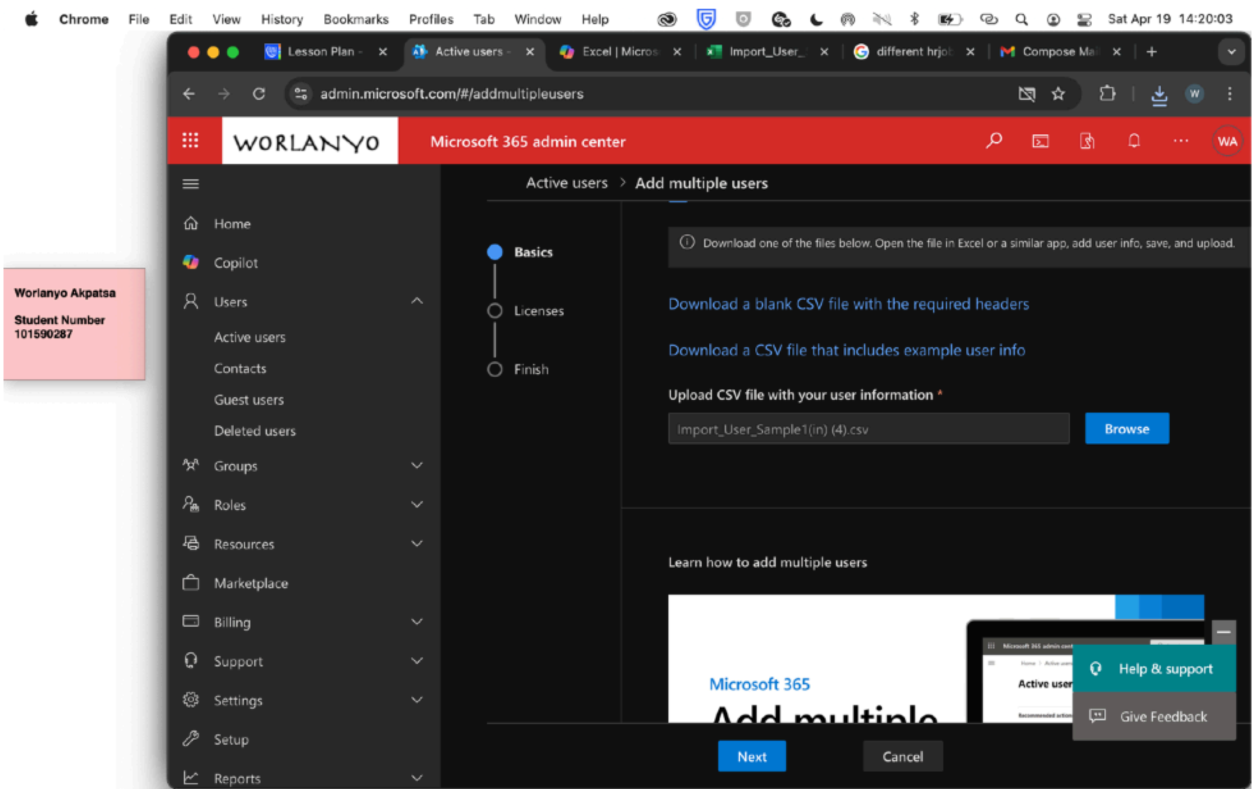


F: Downloading updated CSV file



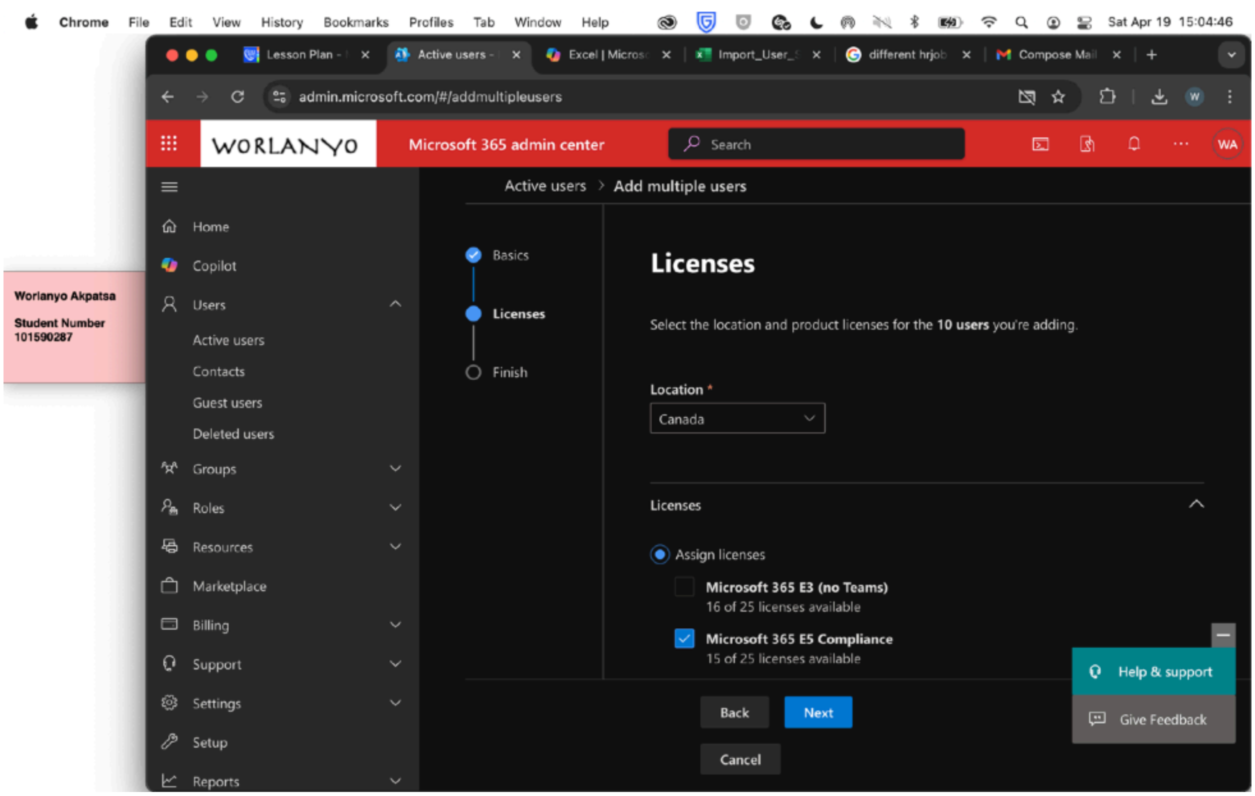


G: Uploading the file to Admin Center "Add multiple users"

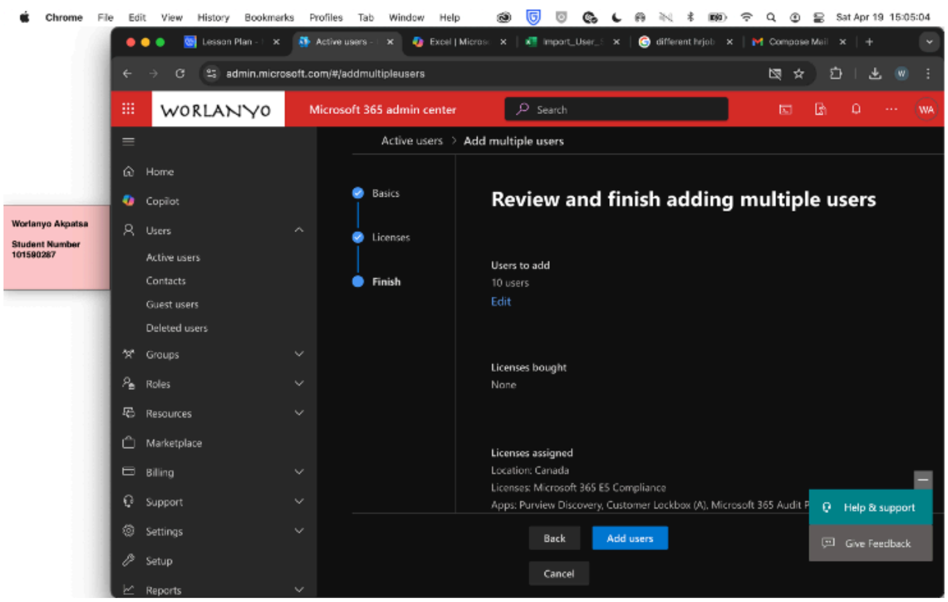


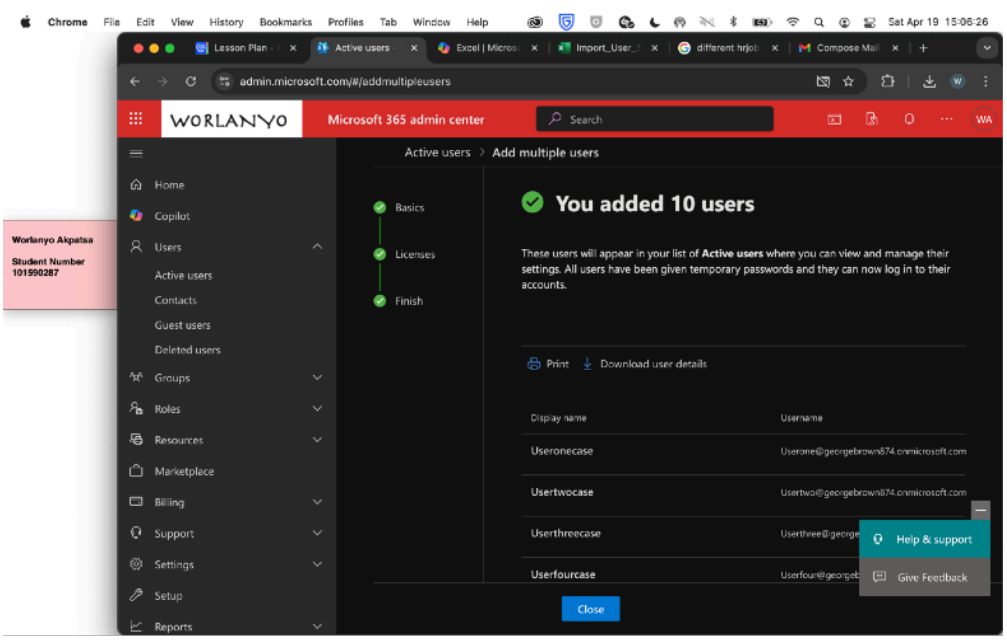
1.2: Assign appropriate licenses (Microsoft 365 E3 or E5) to the imported users

A: In the "Add multiple users" window, after adding CSV file, click next to assign licenses



B: Finalize adding users





~~~~~~

Student Name: Worlanyo Akpatsa Term: Winter 2025
Student ID: 101590287

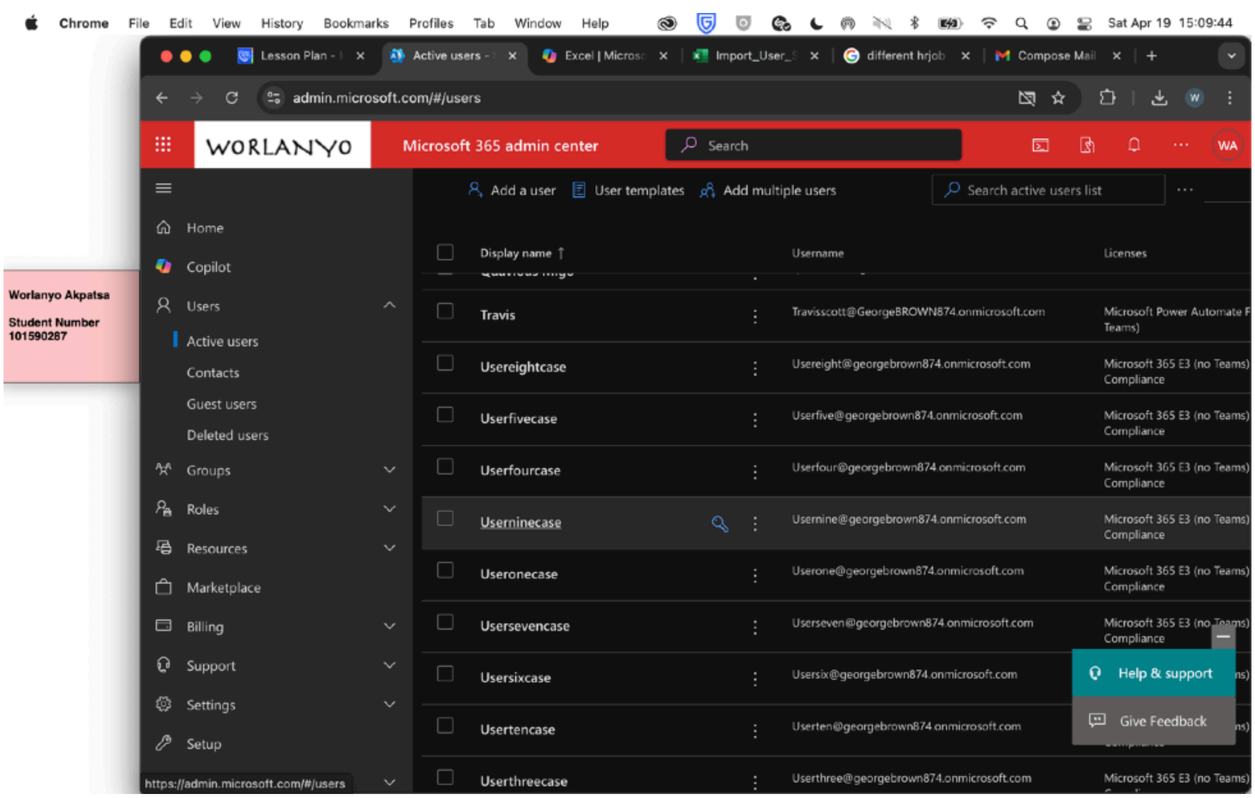
~~~~~~

2: Configure user profiles

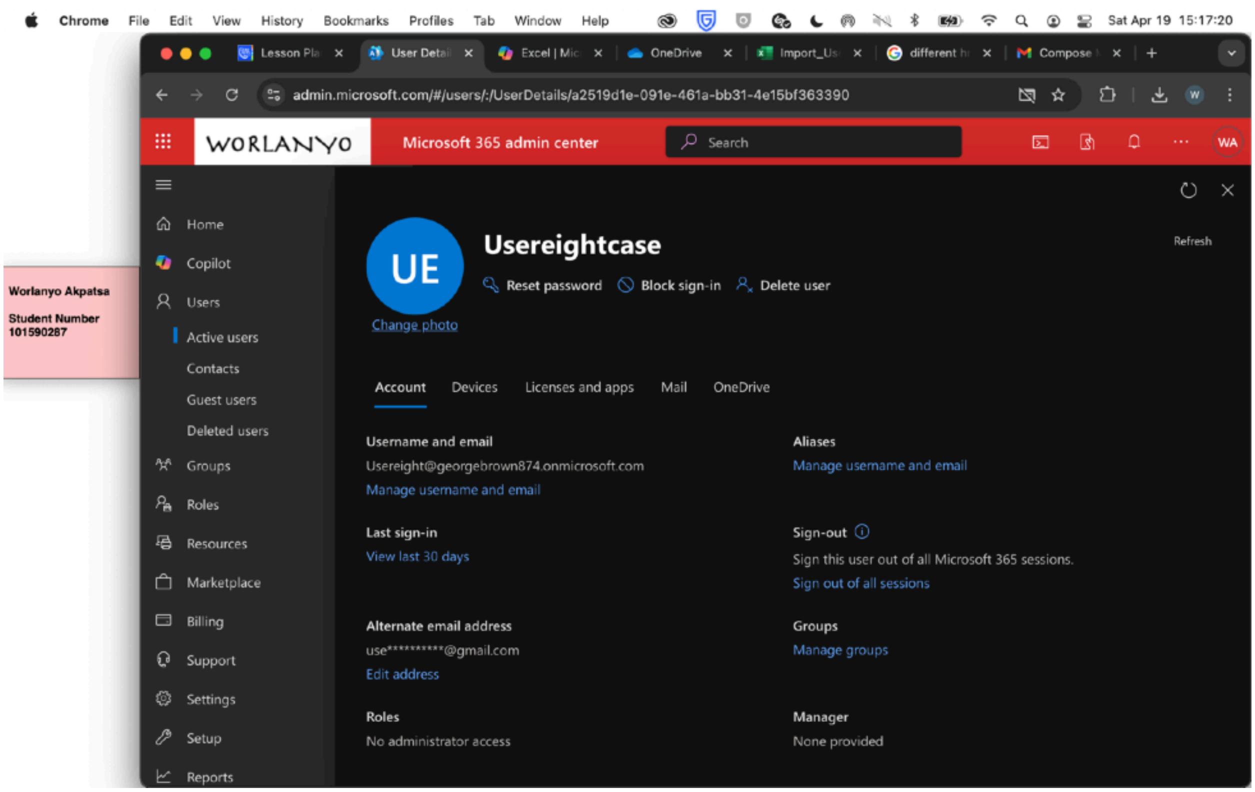
2.1: Ensure each user has a profile picture, contact information and job title set

2.2: Configure user settings to include organization-specific information

A: Navigate to users->active users and click on profile of added users



B: Click Change Photo under the user's display picture to change their photo



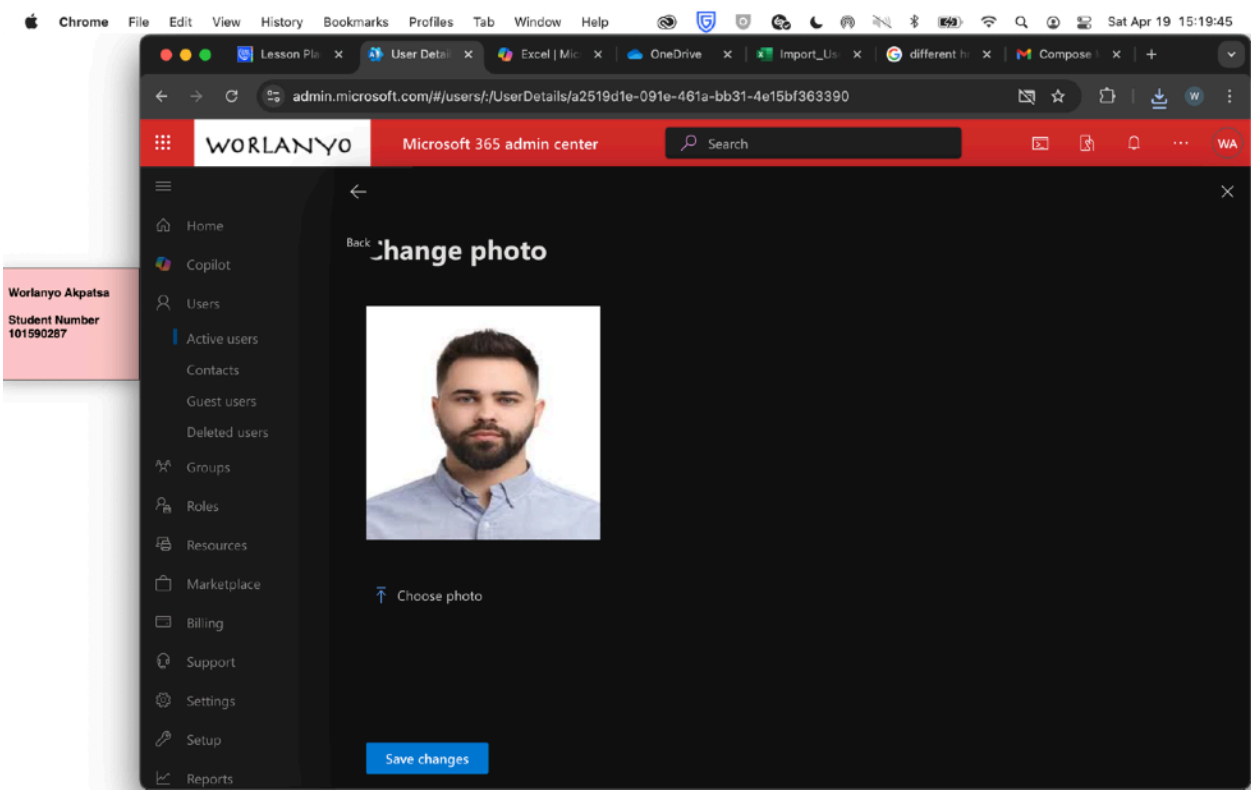
~~~~~~

Student Name: Worlanyo Akpatsa
Student ID: 101590287

Term: Winter 2025

~~~~~~

C: Upload photo for user and click save changes



~~~~~~

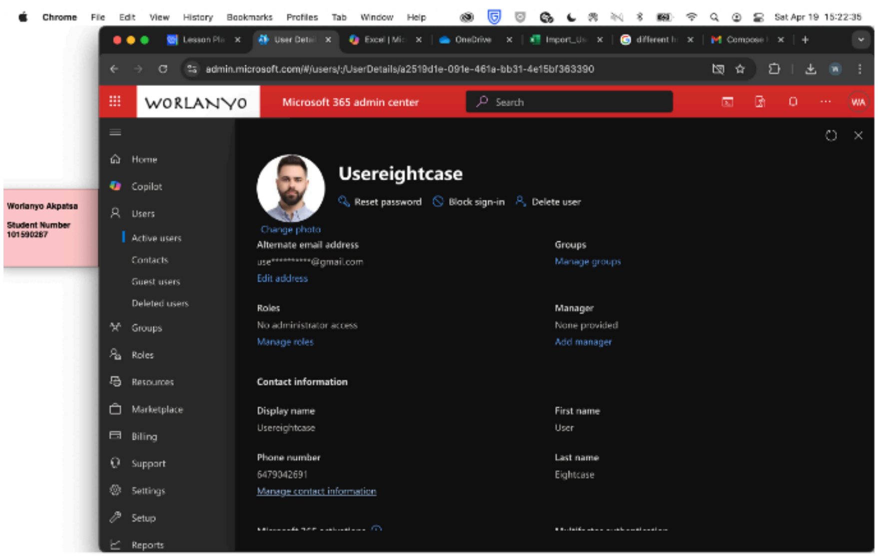
Student Name: Worlanyo Akpatsa
Student ID: 101590287

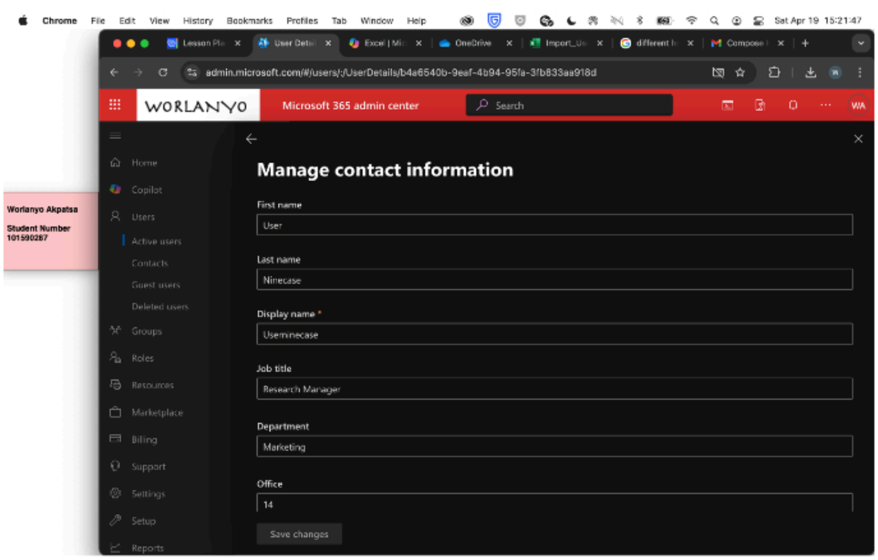
Term: Winter 2025

~~~~~~

D: Scroll down on user page and click “Manage contact information” to edit contact info and company-related info.

Since I uploaded all necessary info in my csv file, all contact info and company info is already uploaded



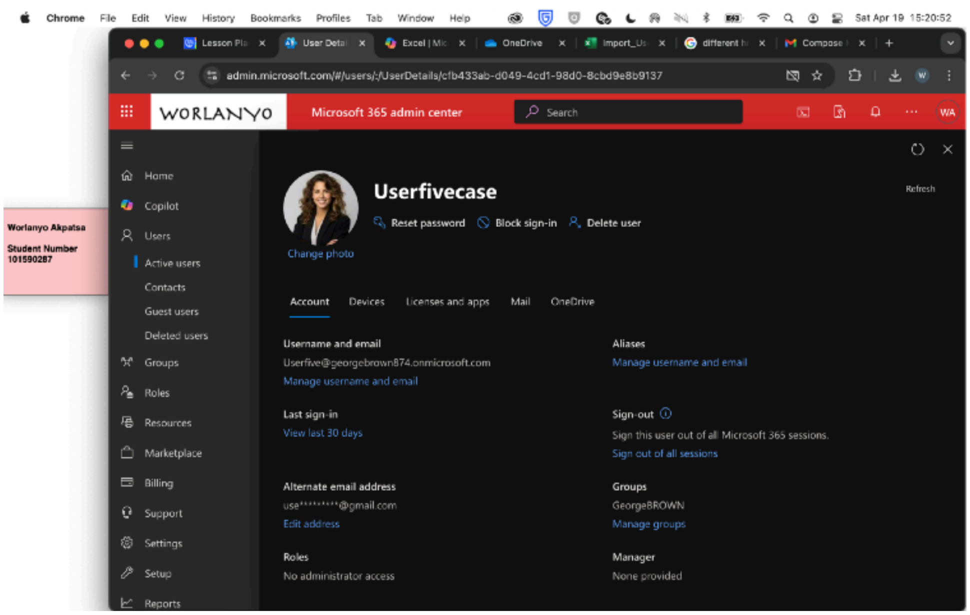


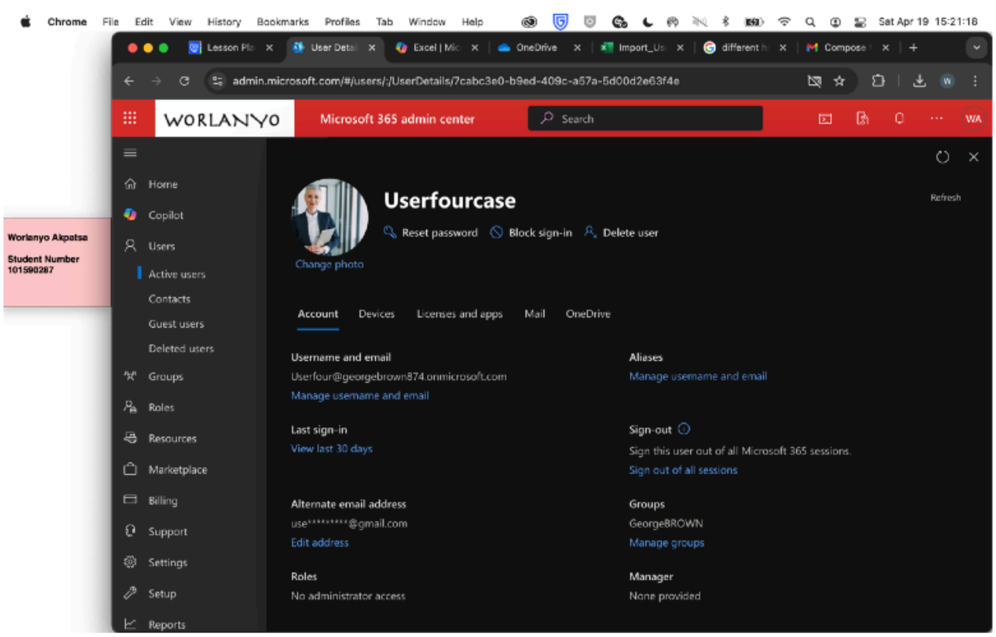
~~~~~~

Student Name: Worlanyo Akpatsa Term: Winter 2025
Student ID: 101590287

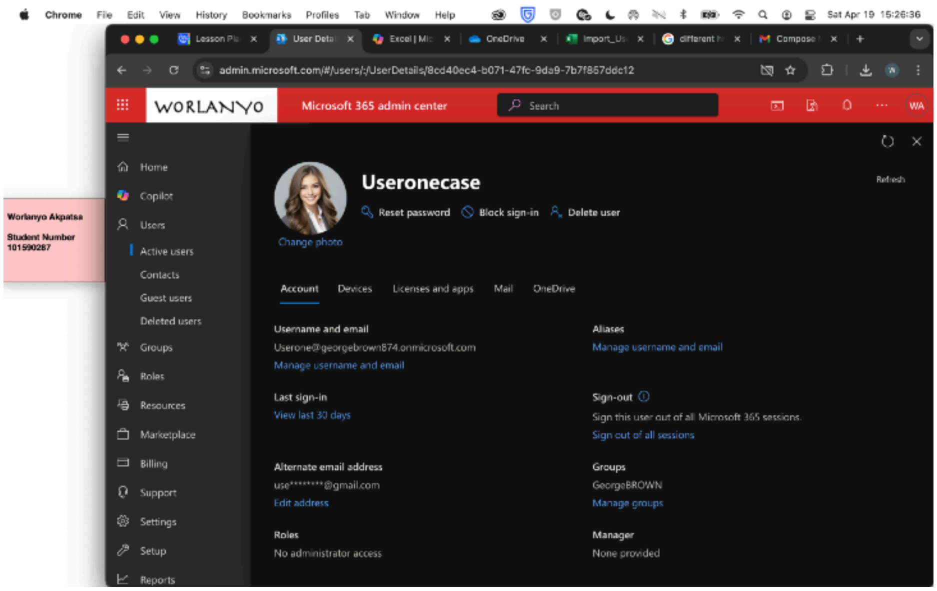
~~~~~~

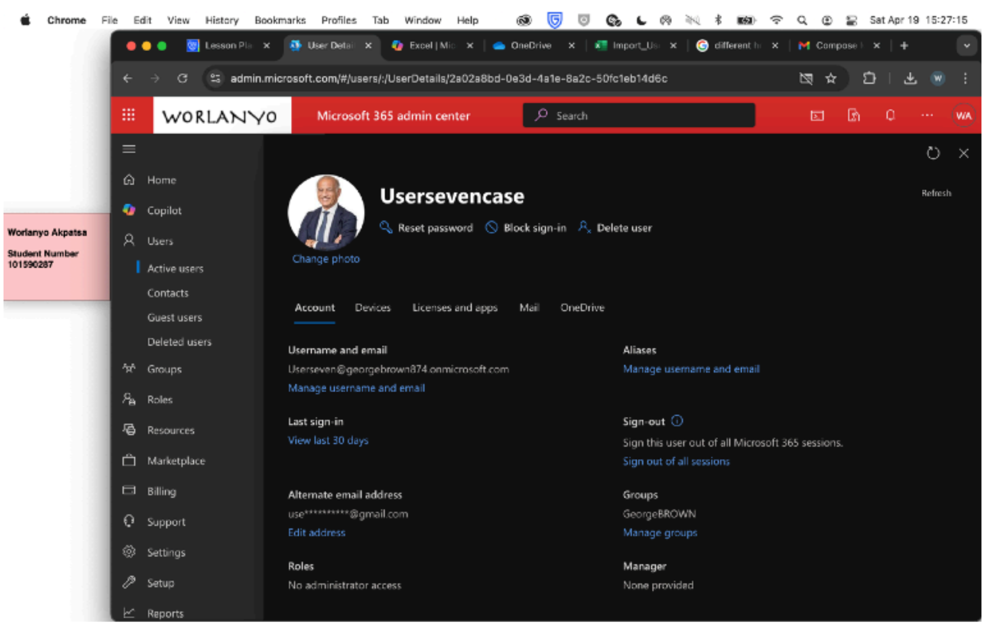
E: Photos for other users uploaded



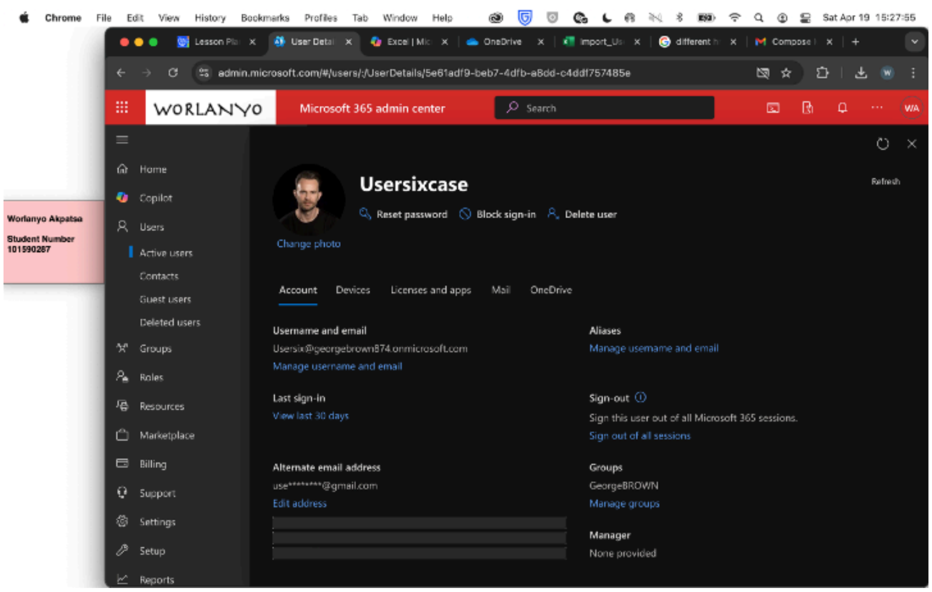


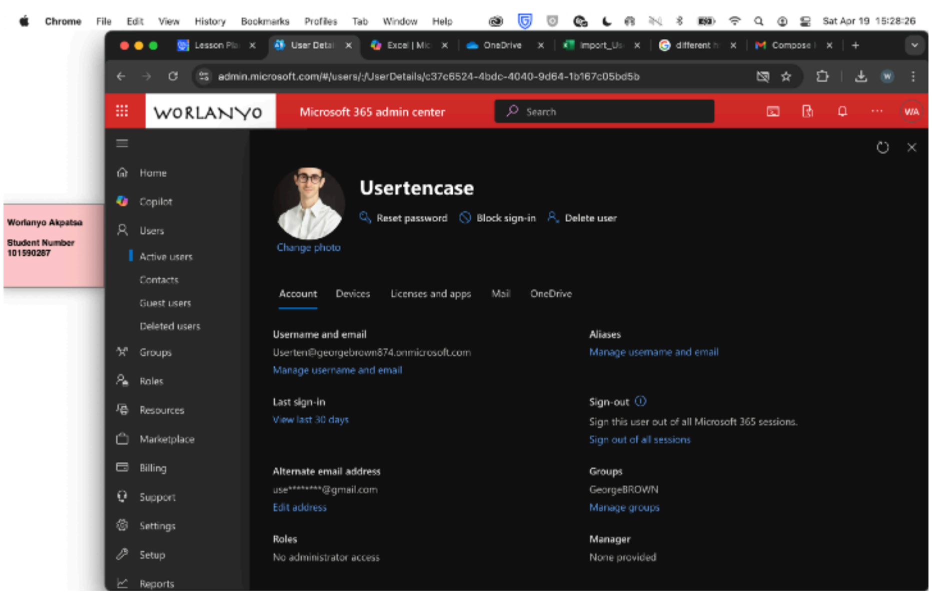
E: Photos for other users uploaded



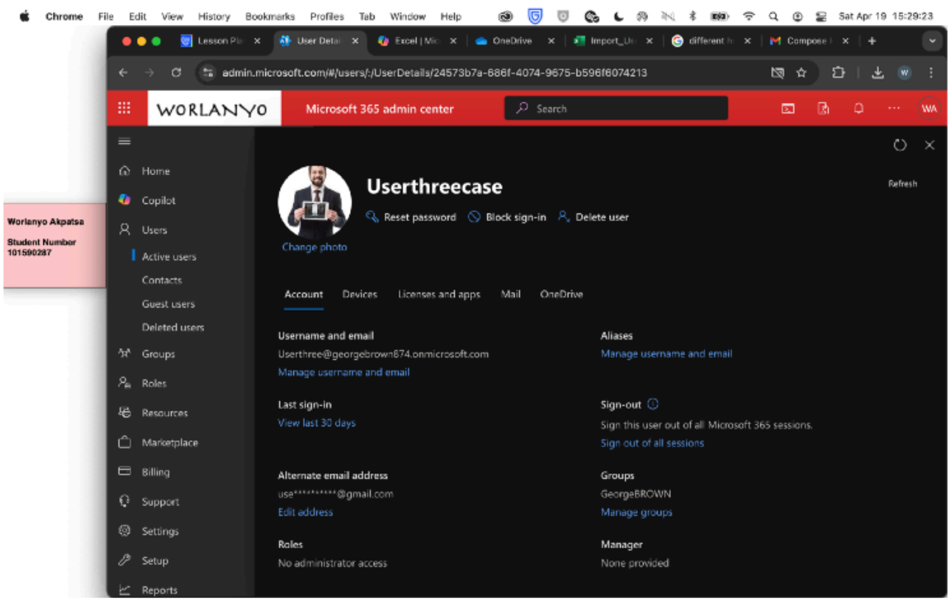


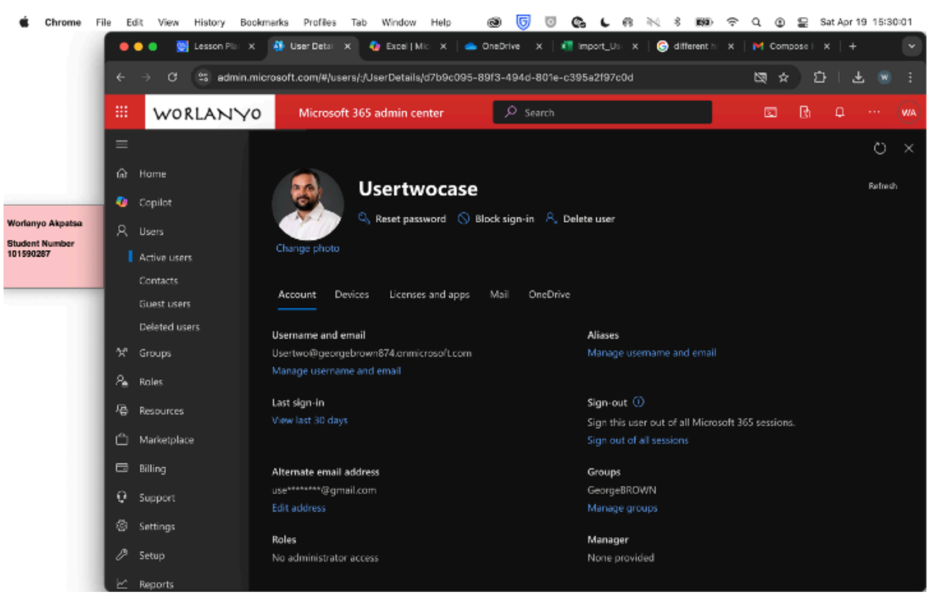
E: Photos for other users uploaded





E: Photos for other users uploaded





~~~~~~

Student Name: Worlanyo Akpatsa | Term: Winter 2025
Student ID: 101590287

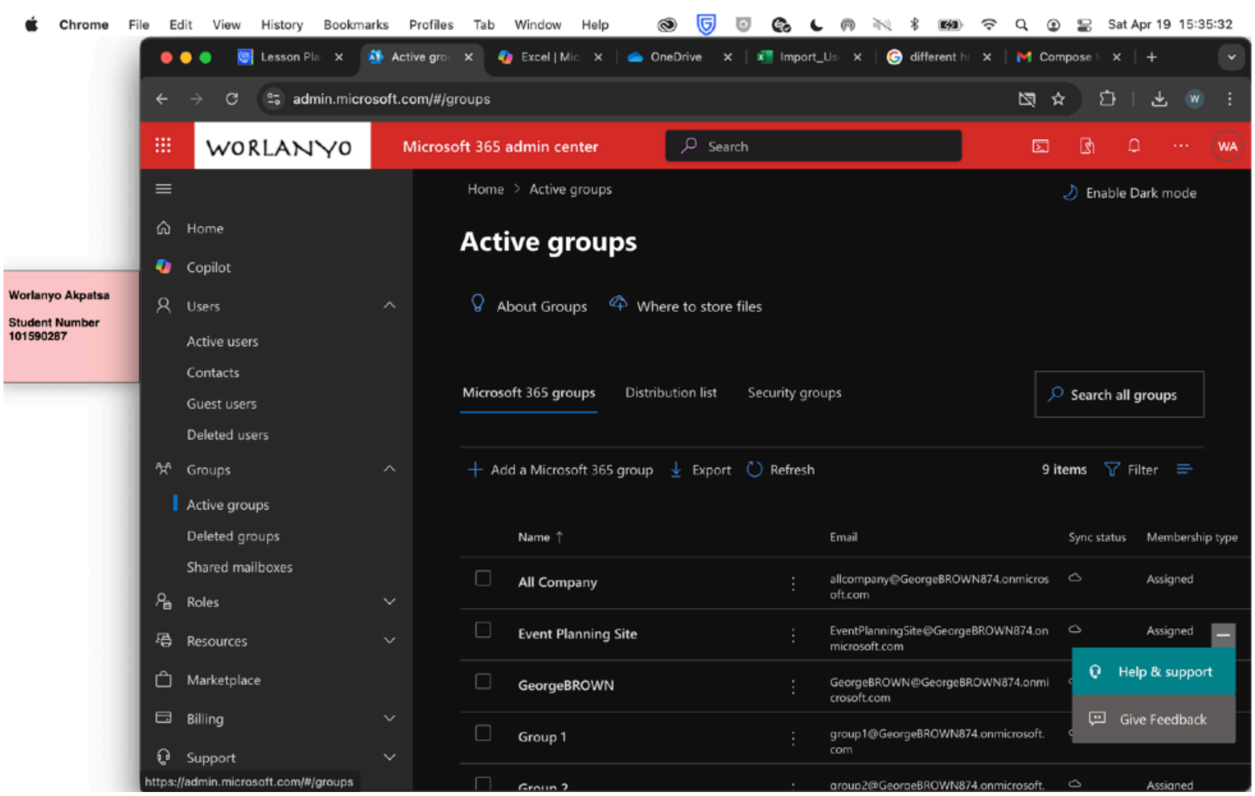
~~~~~~

3: Create Office 365 Groups

3.1: Create three Office 365 groups for different departments: IT, HR and Marketing

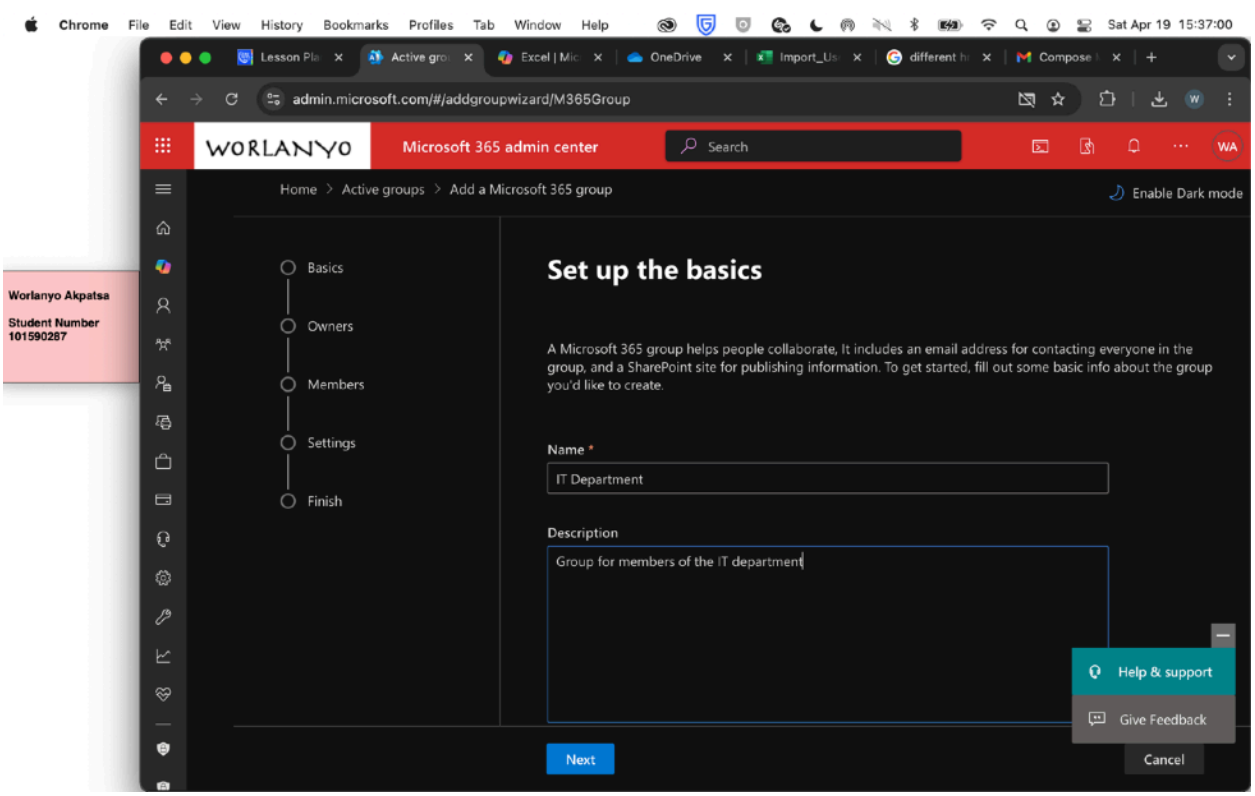
3.2: Add users to respective groups

A: Navigate to groups->active groups in the left pane of the admin center

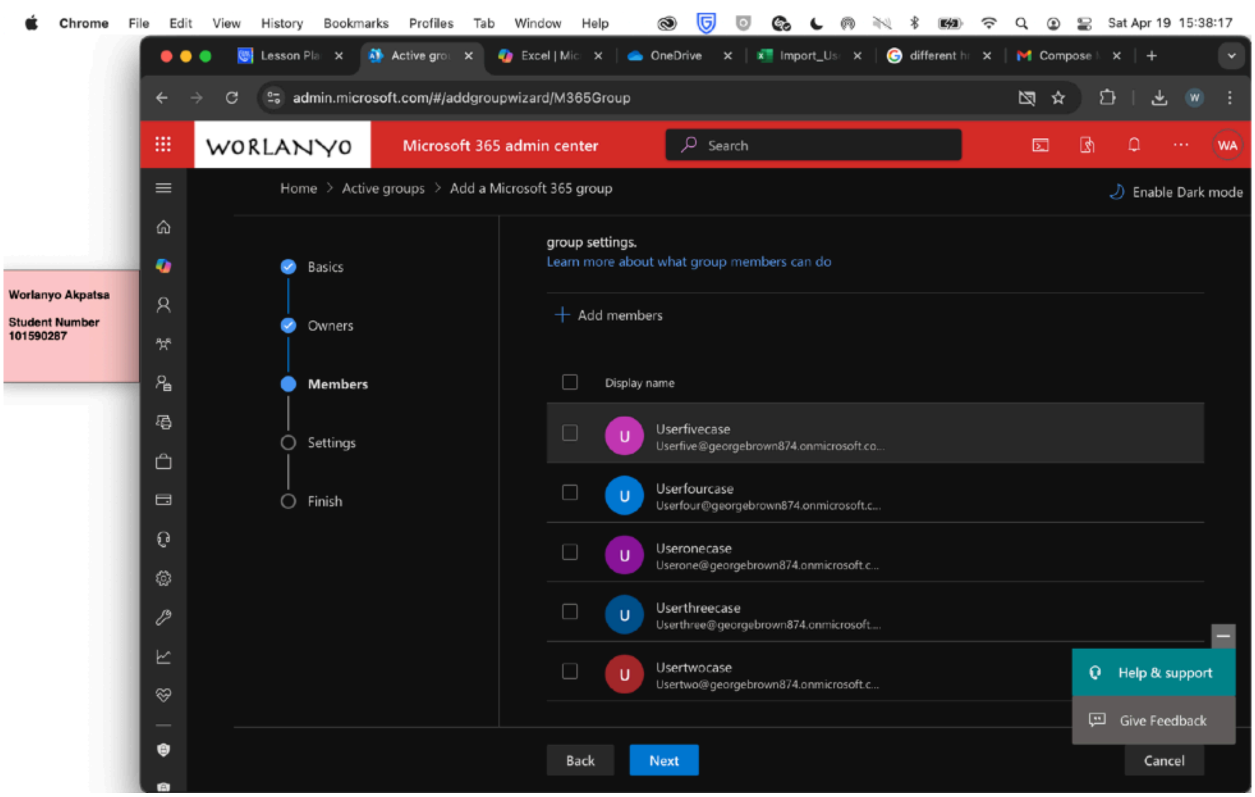


B: Creating group for IT department.

Click “Add a Microsoft 365 group” and set up name and description

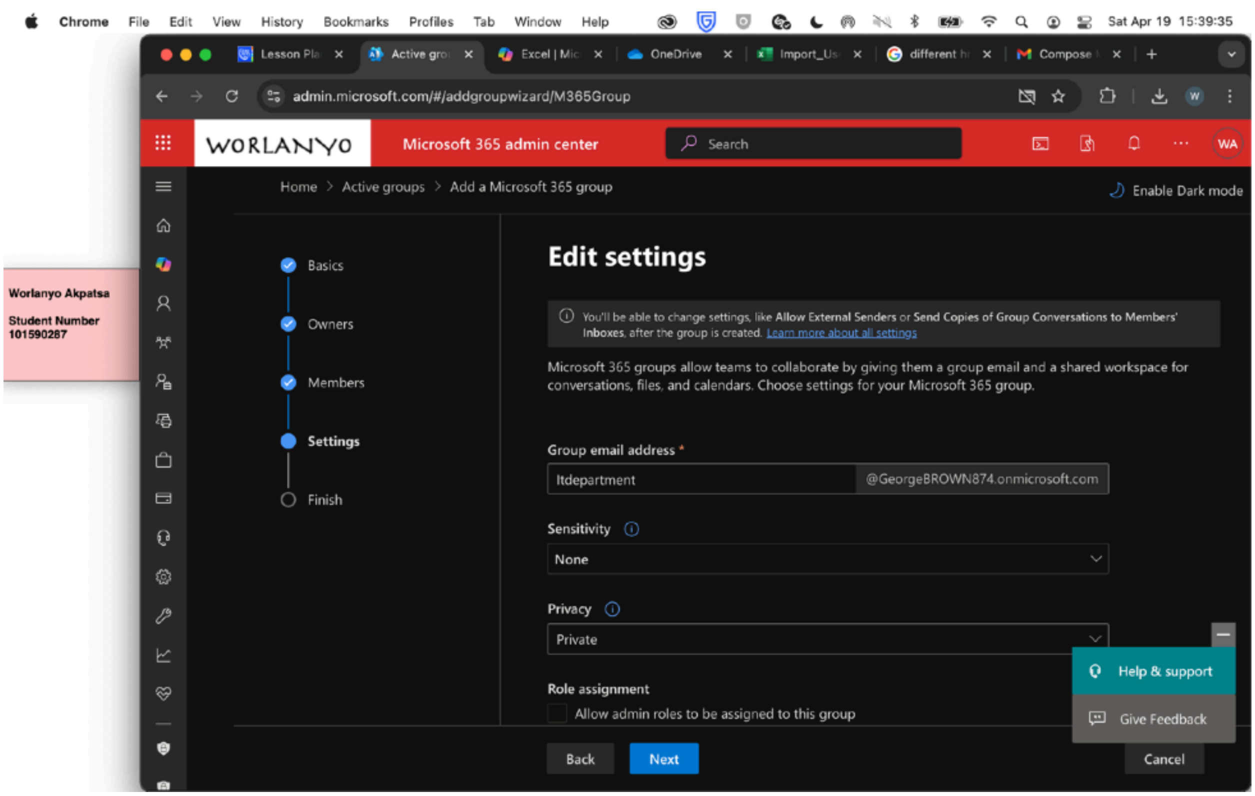


Adding members to IT department group as per my CSV file

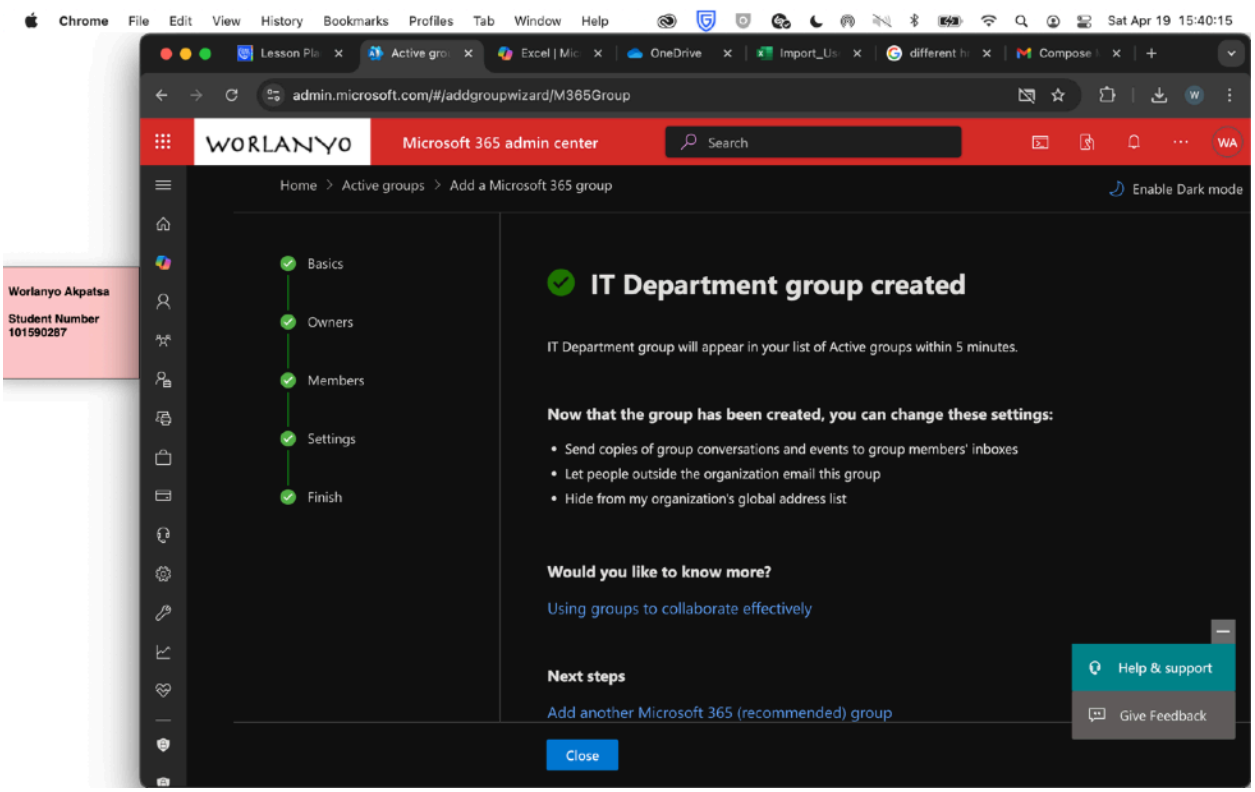


Student Name: Worlanyo Akpatsa Term: Winter 2025
Student ID: 101590287

Final settings for IT department group



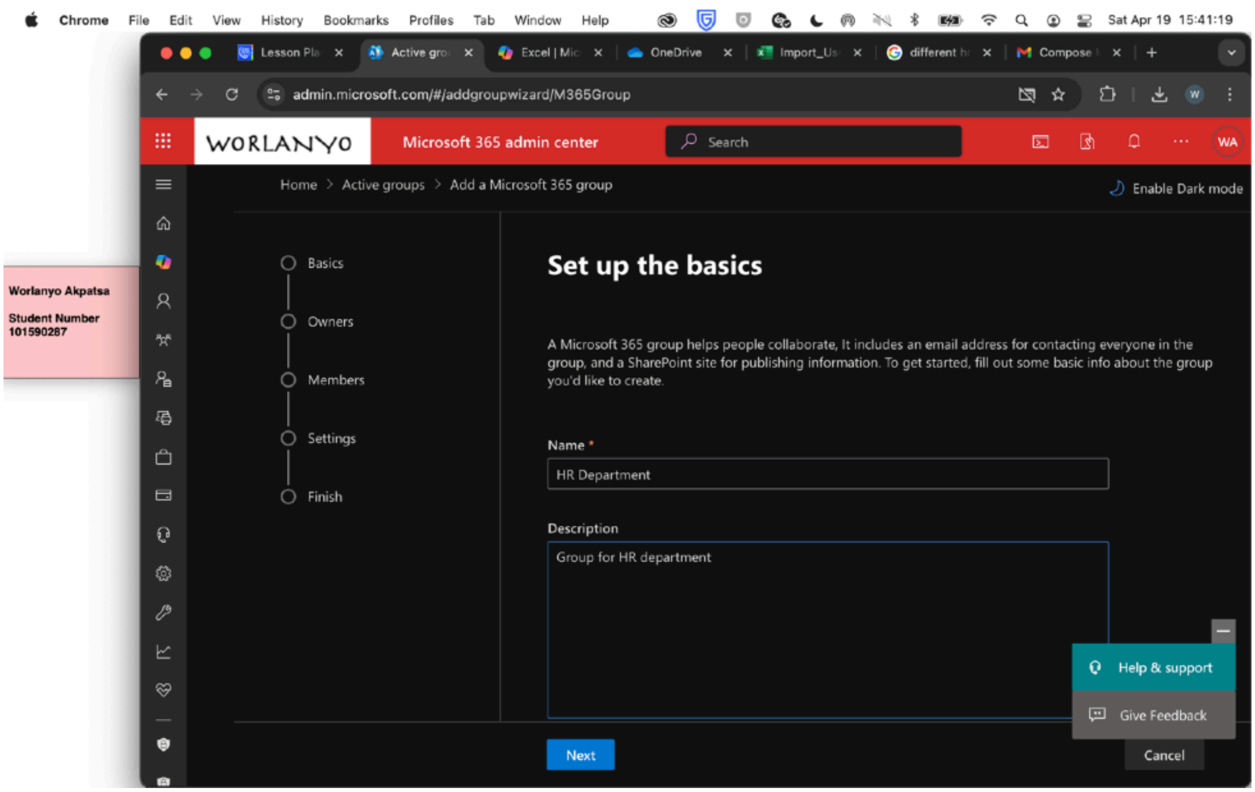
IT department Group Created



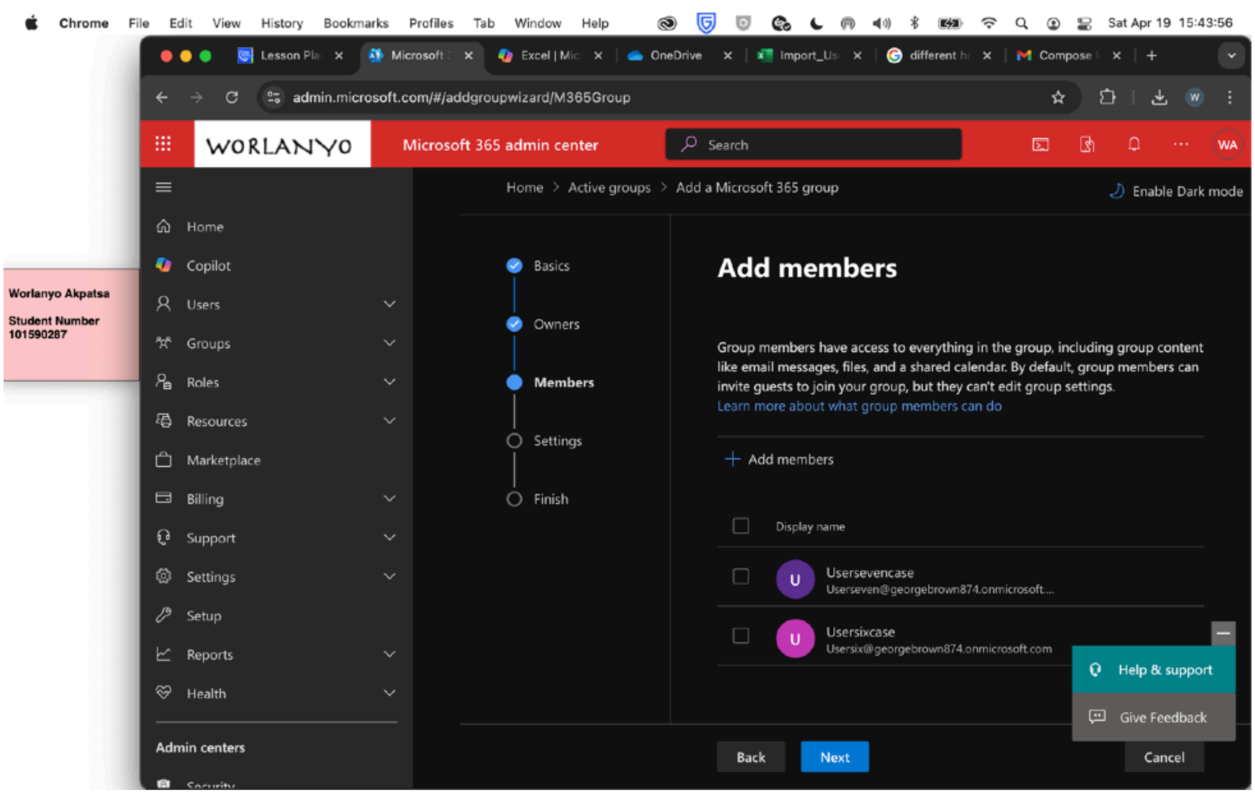
Student Name: Worlanyo Akpatsa Term: Winter 2025
Student ID: 101590287

C: Creating group for HR department.

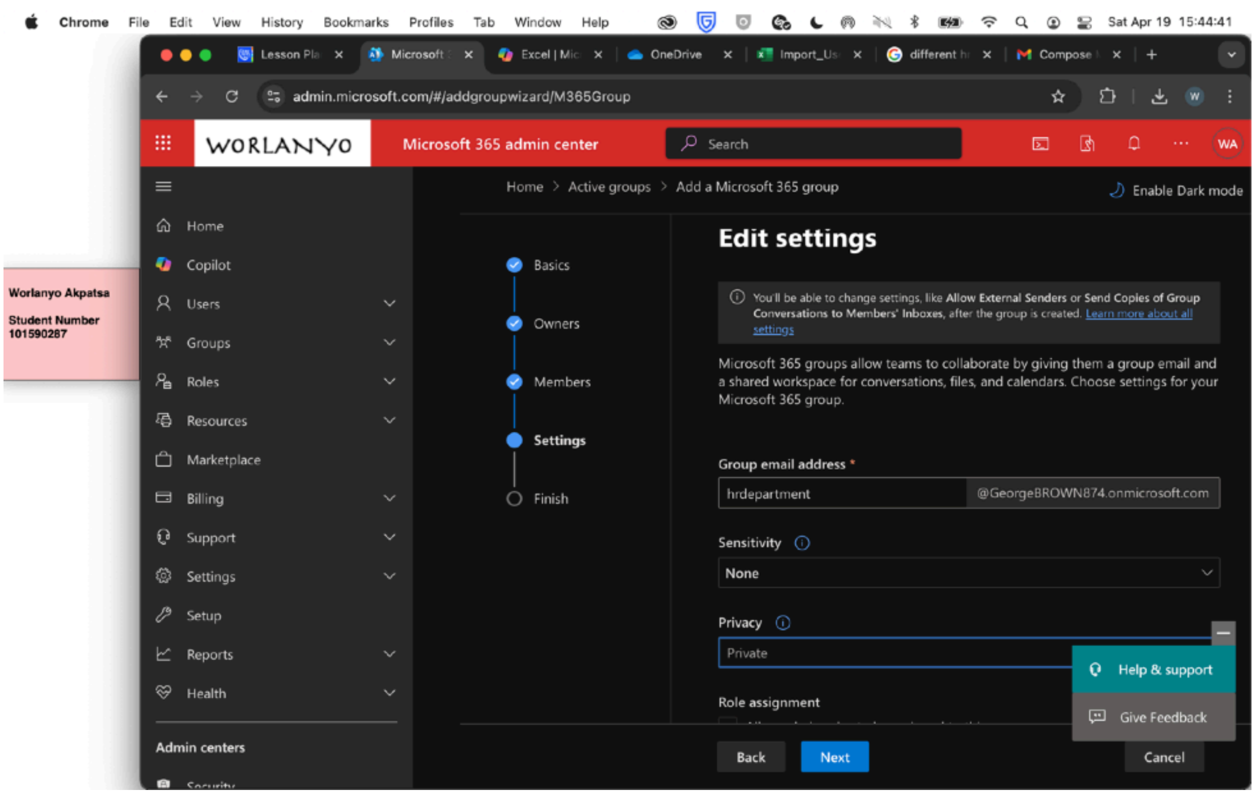
Click "Add a Microsoft 365 group" and set up name and description



Adding members to HR department group as per my CSV file



Final settings for HR department group



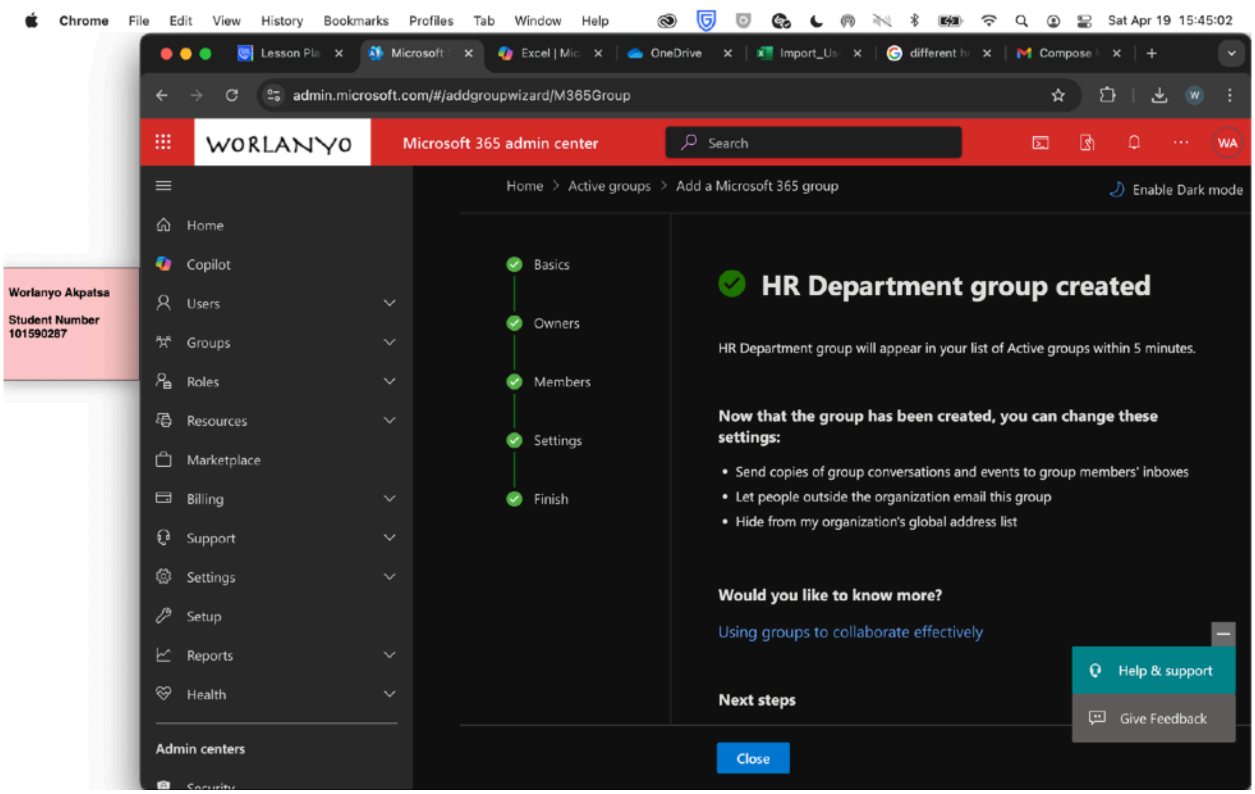
~~~~~~

Student Name: Worlanyo Akpatsa
Student ID: 101590287

Term: Winter 2025

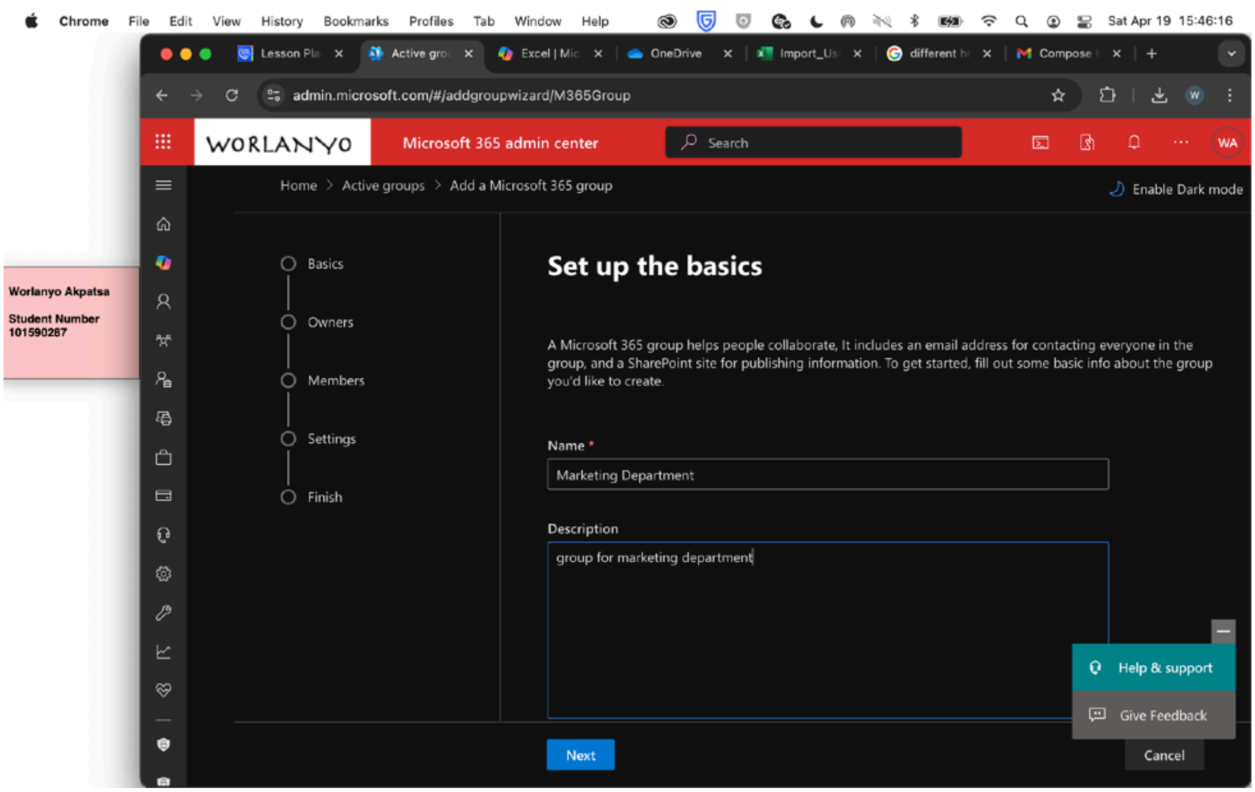
~~~~~~

HR department Group Created



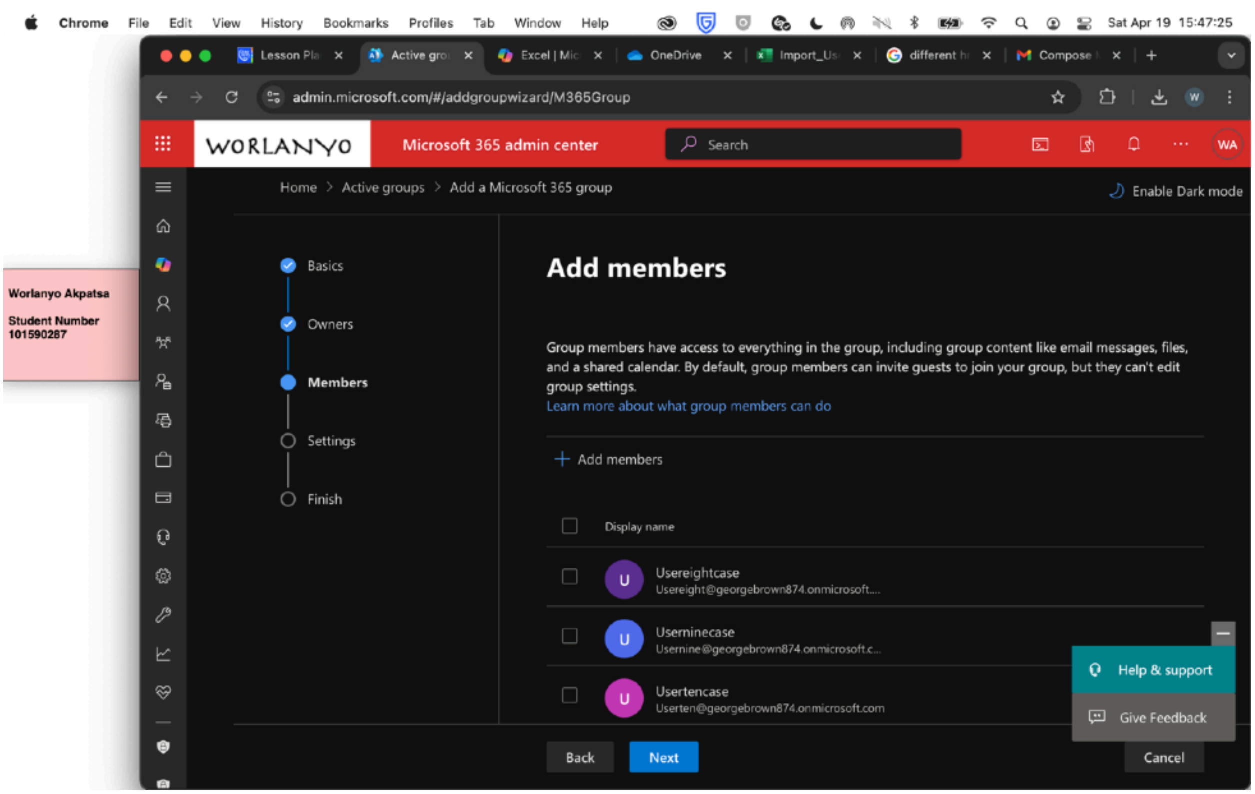
D: Creating group for Marketing Department

Click "Add a Microsoft 365 group" and set up name and description



Student Name: Worlanyo Akpatsa Term: Winter 2025
Student ID: 101590287

Adding members to Marketing department group as per my CSV file

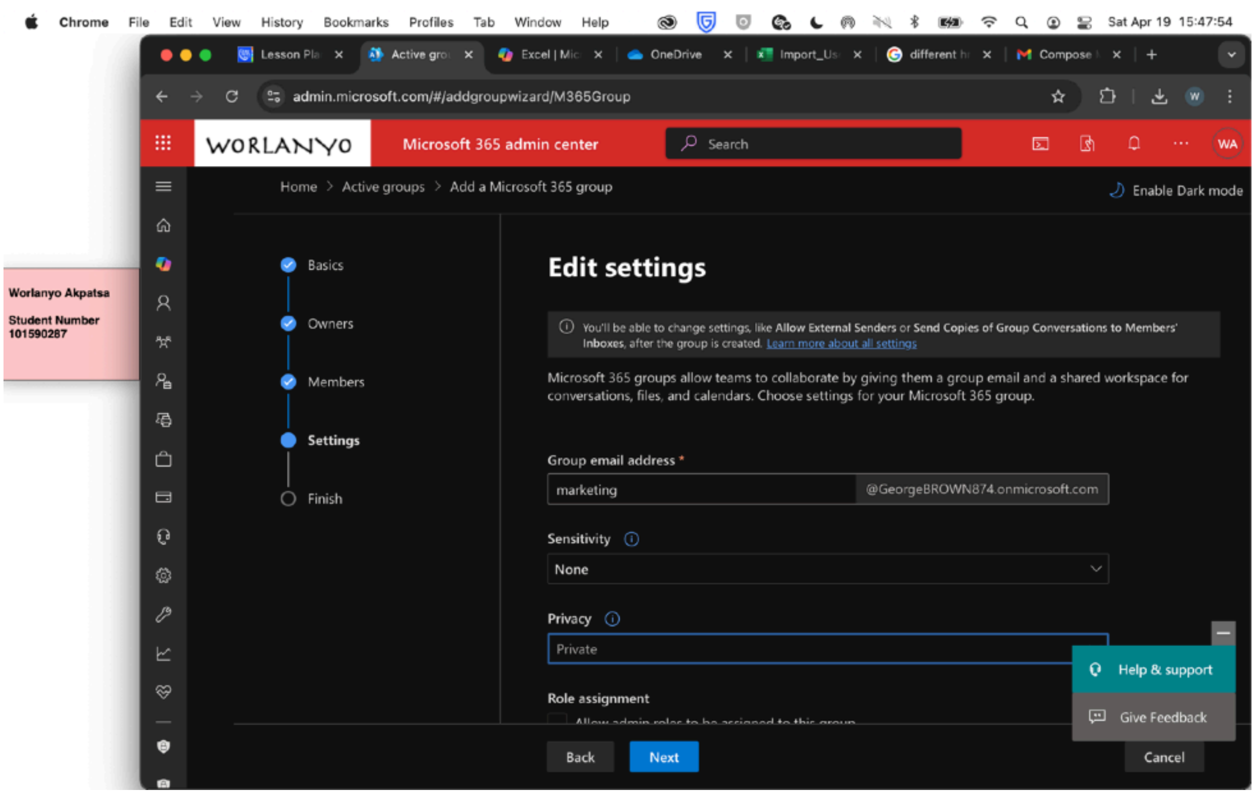


~~~~~~

Student Name: Worlanyo Akpatsa Term: Winter 2025
Student ID: 101590287

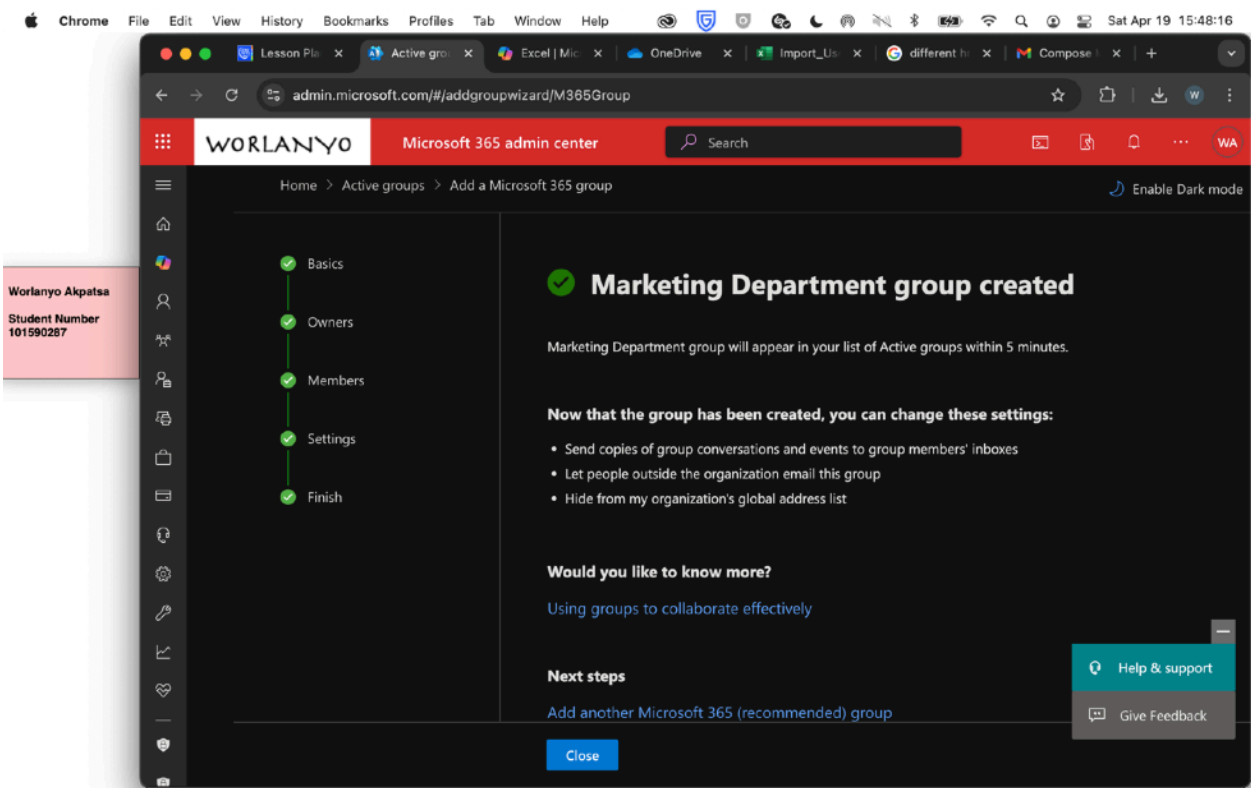
~~~~~~

Final settings for Marketing department group



Student Name: Worlanyo Akpatsa Term: Winter 2025
Student ID: 101590287

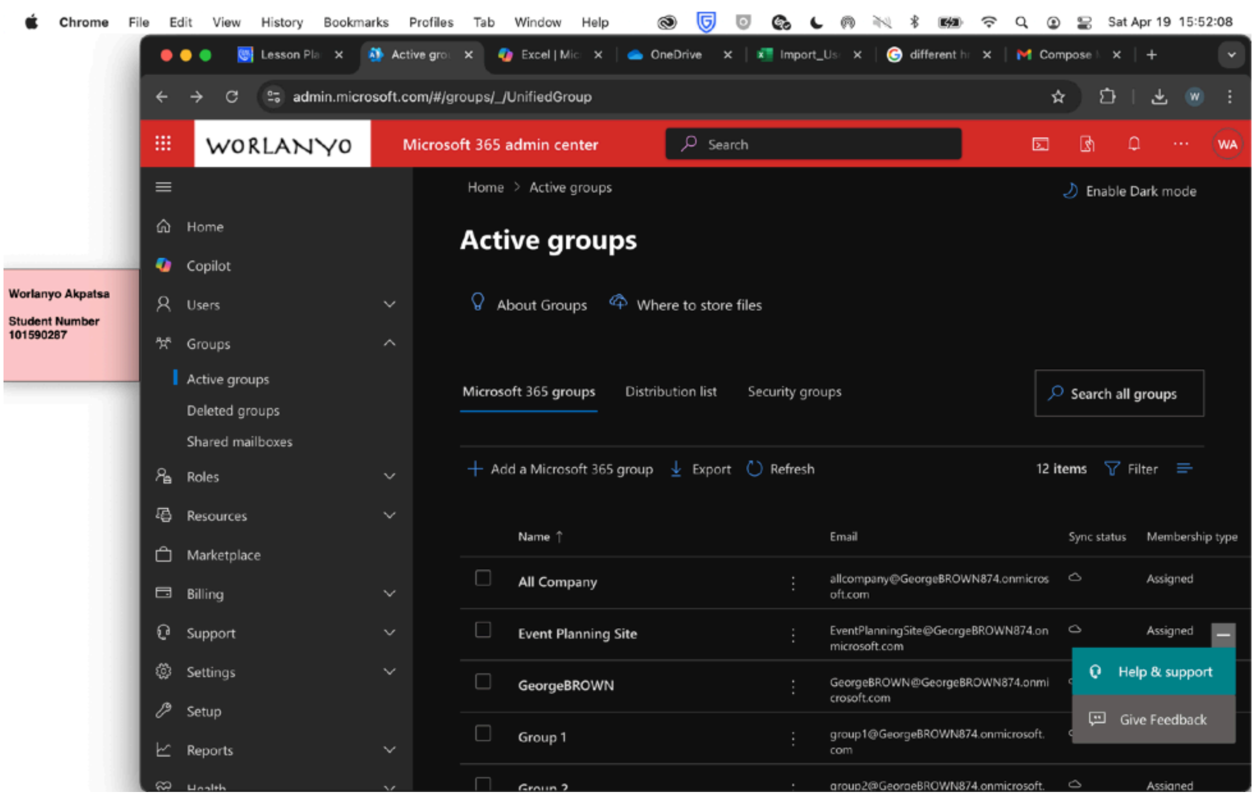
Marketing Department Group Created



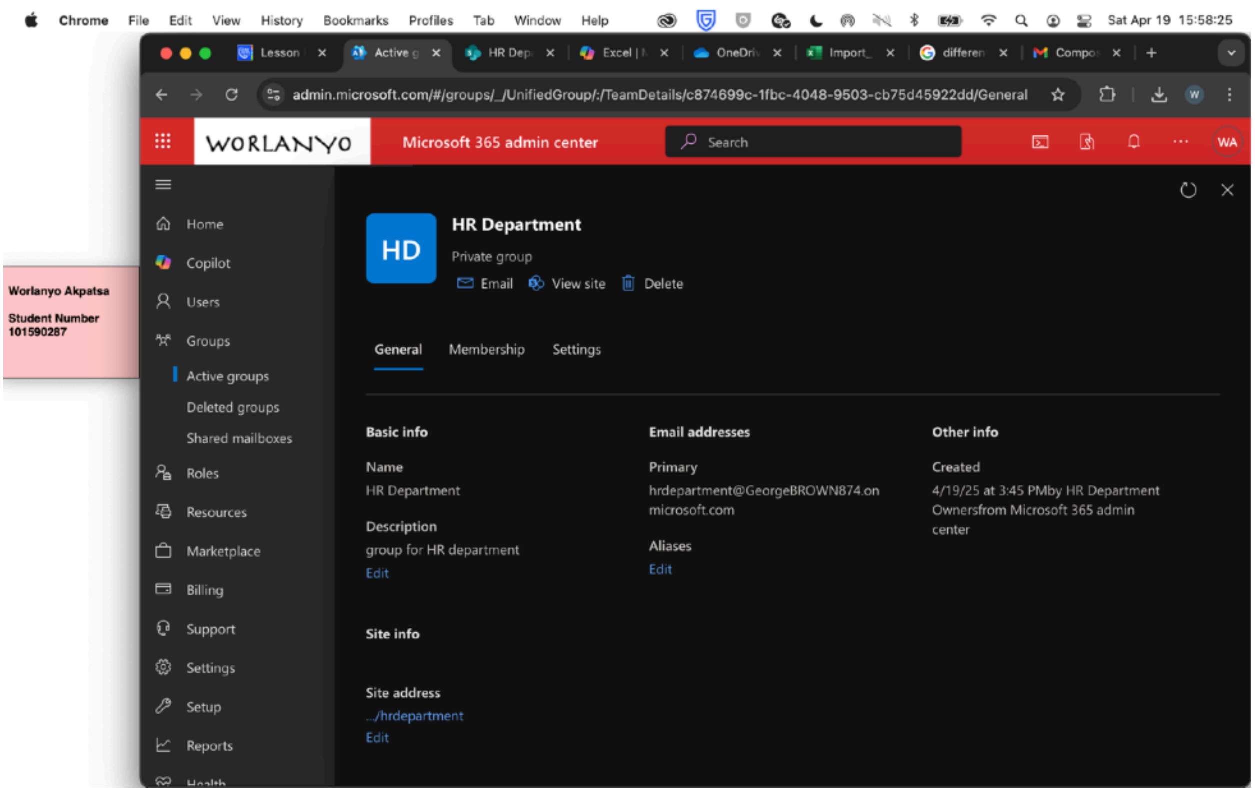
4: Configure User Permissions

4.1: Assign specific permissions to the HR group to access sensitive HR documents in Sharepoint

A: Navigate to groups->active groups



B: Select HR department group and open settings

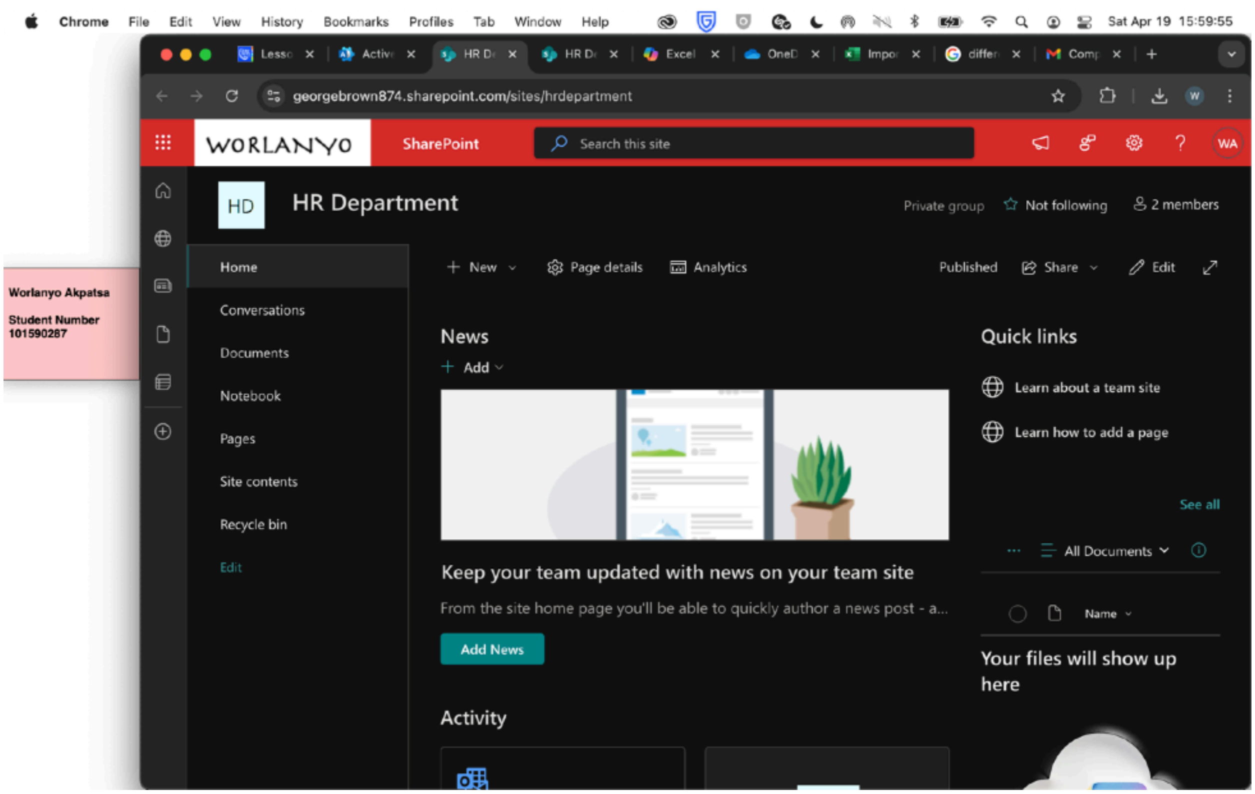


~~~~~~

Student Name: Worlanyo Akpatsa Term: Winter 2025
Student ID: 101590287

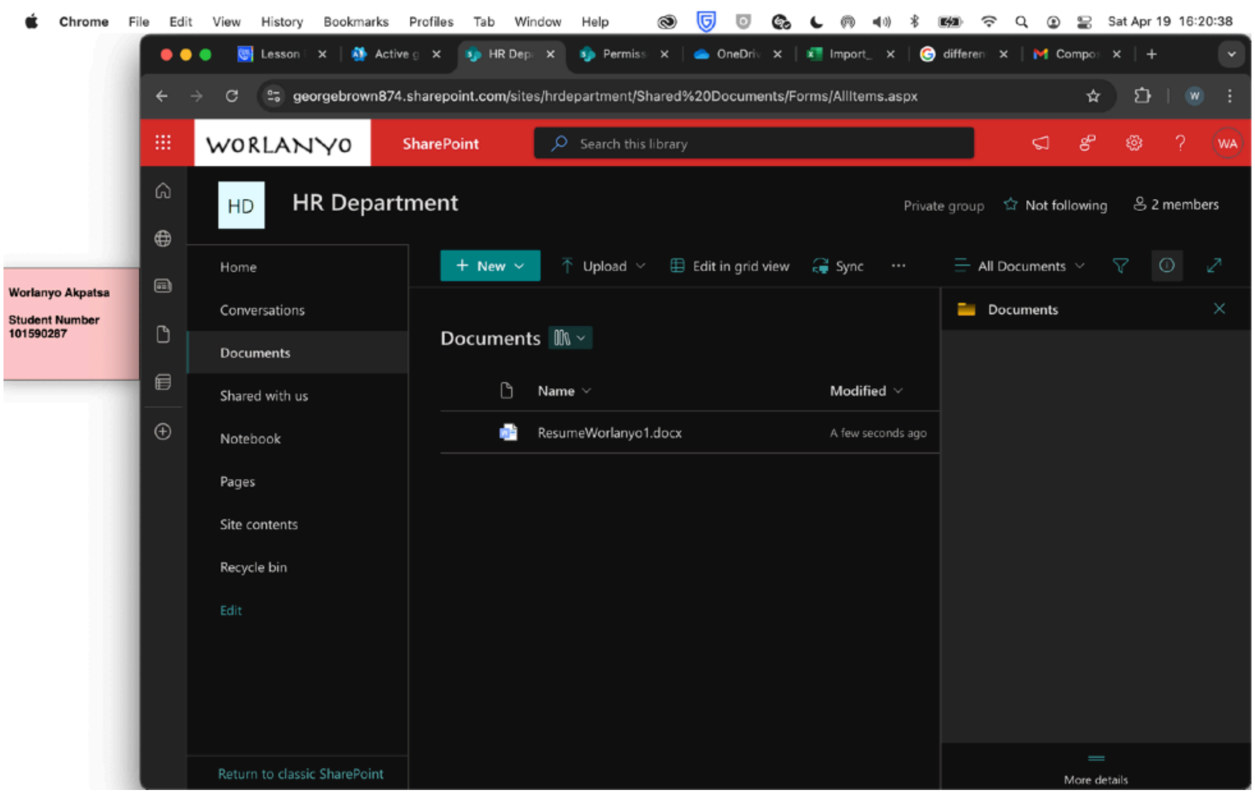
~~~~~~

C: Open the site where HR documents will be stored by clicking on link under "site address" in HR department group page

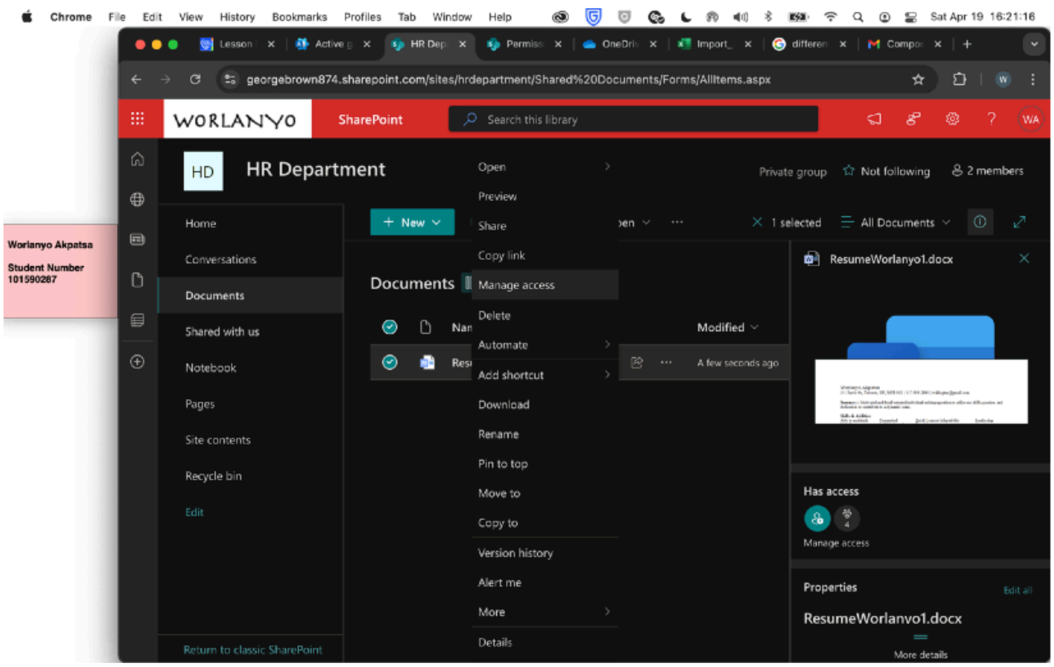


Student Name: Worlanyo Akpatsa
Student ID: 101590287
Term: Winter 2025

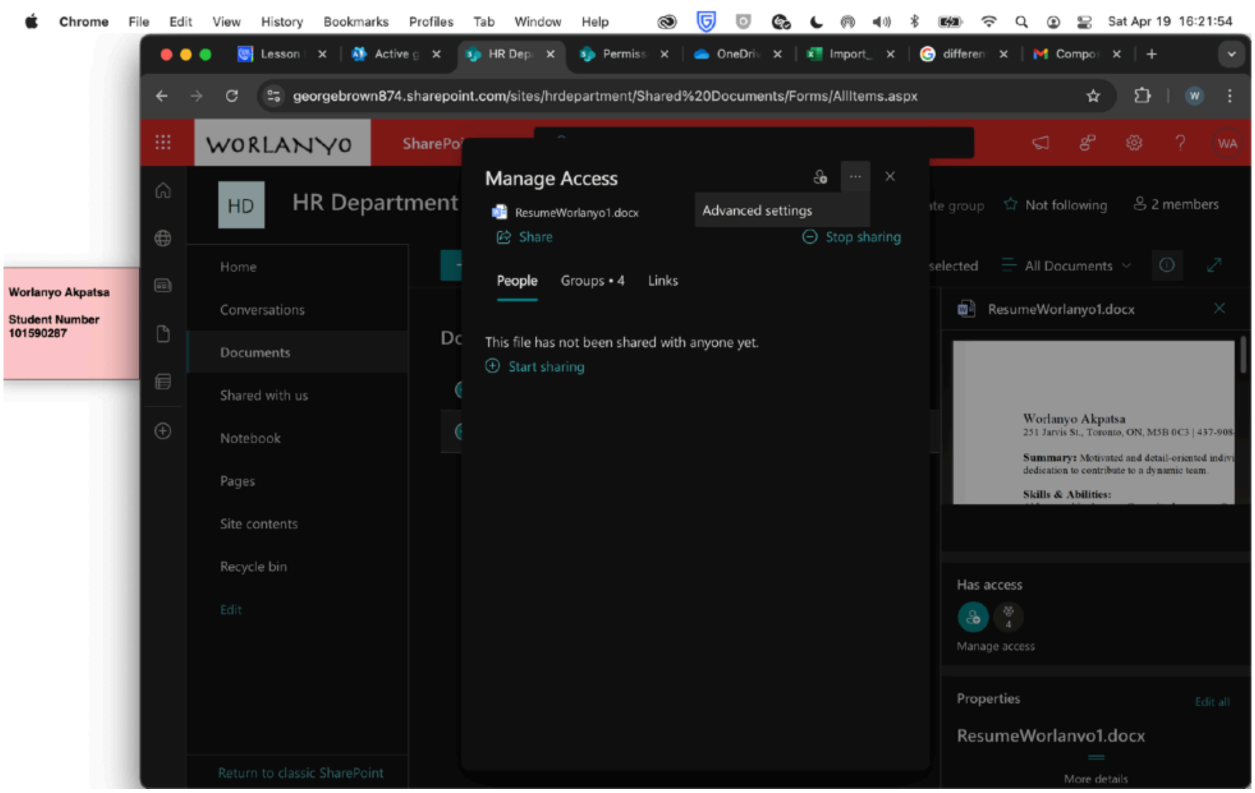
D: Upload Document to Documents tab on left pane



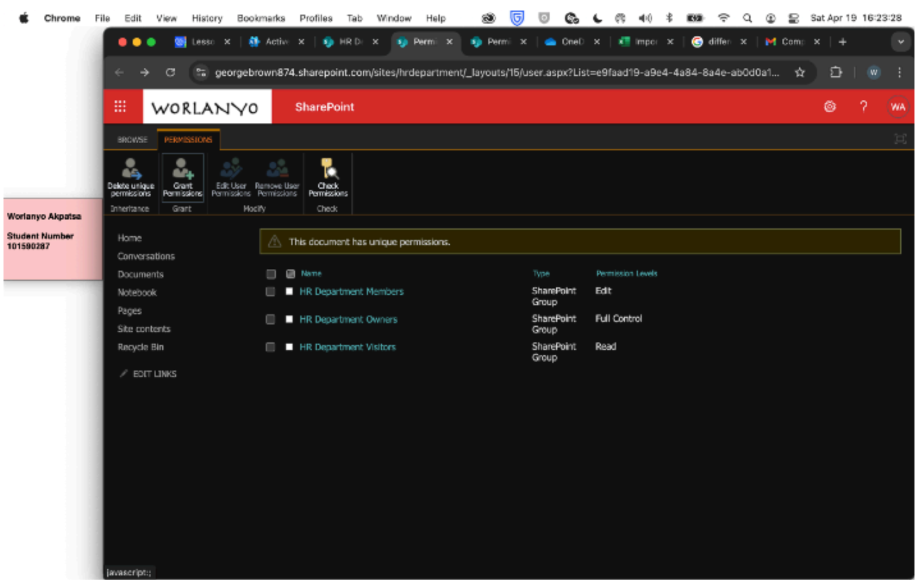
E: Right Click on Document and select Manage Access

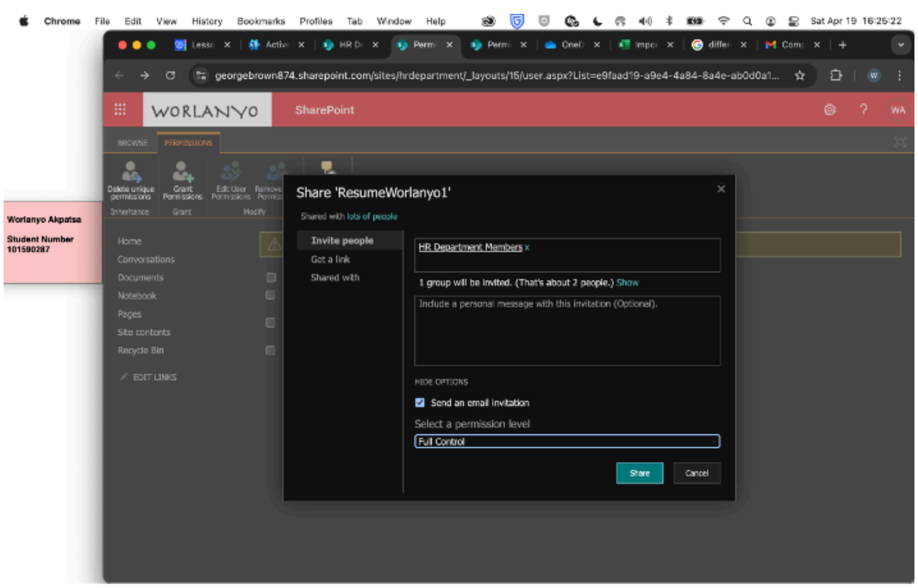


F: In manage access window, click on three dots and select Advanced Settings



G: In the advanced settings window, click on Grant Permissions and give HR department Members full control to document access





The above procedure is a way to assign specific permissions to the HR group for them to access sensitive documents in the Sharepoint Site.

You can also edit site permissions in general to manage permissions. To do this, you have to visit the Sharepoint site for the group and click on settings icon and then select site permissions->advanced permission settings.

Task 1 Summary:

The opening task for this case project was something I have made myself really familiar with (Setting up and Configuring User Accounts) so I did not really have a problem doing it. The only thing that was quite new to me was importing users using a CSV file but I was able to do it so it was something very interesting I learnt.

To begin, I had to bulk import ten users to my organization. To do this, I navigated to users->active users in my 365 Admin Center and selected Add multiple users in the header.

When this window opens, one can either add the multiple users using the admin center or via a CSV file template provided by Microsoft.

The task called to use a CSV file so that's what I did.

On the add multiple users window, I scrolled down and checked the box "Id like to upload a CSV with user information". When you do this, it shows two different hypertext links which allow you to download templates.

I downloaded the template and had to edit it using Excel. Due to the fact that my MacOS is quite old, I was not being allowed to open excel so i though of something else to do; I opened Excel using 365 Admin Center and edited my CSV template on the web Excel. I'm glad I thought of that so quick.

I had no problem inputting all the information for my ten new users but when I tried to upload, at first I was getting errors pertaining to my username. I didn't realize that all usernames had to have the domain attached to them. I made this correction and my CSV file uploaded to the admin center no problem.

Next I assigned Microsoft licenses to all the users so they have access to most of the Microsoft 365 services.

The next task was to configure the user profiles by adding profile pictures, contact info and organization-specific info. Luckily for me, while editing my CSV file, I made sure to include all organization-specific info like a user's department, their job title, contact info, etc. This means all I had to do here was upload profile pictures.

I navigated to users->active users in the admin center and clicked on a users name which opens a window containing all their info. Under their avi, it says "change photo". I clicked on this and uploaded a photo for my new user. I repeated this same process for all other users.

The next thing was to create three groups for the different departments (IT, HR MARKETING) which I found easy to do to be honest. Lucky for me too, I divided my users into different departments in my CSV file (users 1-5 in IT, users 6 and 7 in HR and users 8-10 in marketing.) This really helped me when assigning my users to groups.

I navigated to groups->active groups in the left pane of the admin center and selected add a microsoft 365 group. I then added chose the name for the groups and added the users per my csv file. I edited settings to make them private groups so only the users could access.

Last thing in this task was to configure user permissions. The first thing I had to do was assign specific permissions to the HR group to access sensitive HR documents. To do this, I opened the HR group window by accessing groups->active groups and then clicked the link under site address which took me to the sharepoint site for the group.

I uploaded a document to the documents tab and right clicked on that document and selected manage access. I chose the advance settings in the manage access window and clicked on grant permissions after. Here, I gave HR members group full access to the document.

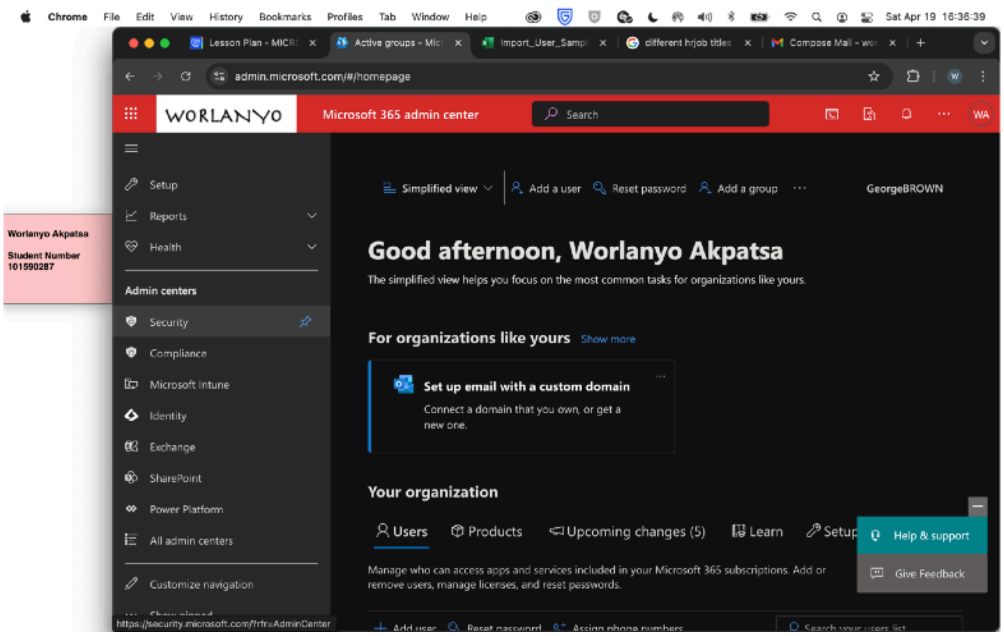
This task was quite easy to do. Very nice to revisit the things I learnt earlier.

TASK 2: IMPLEMENTING SECURITY MEASURES

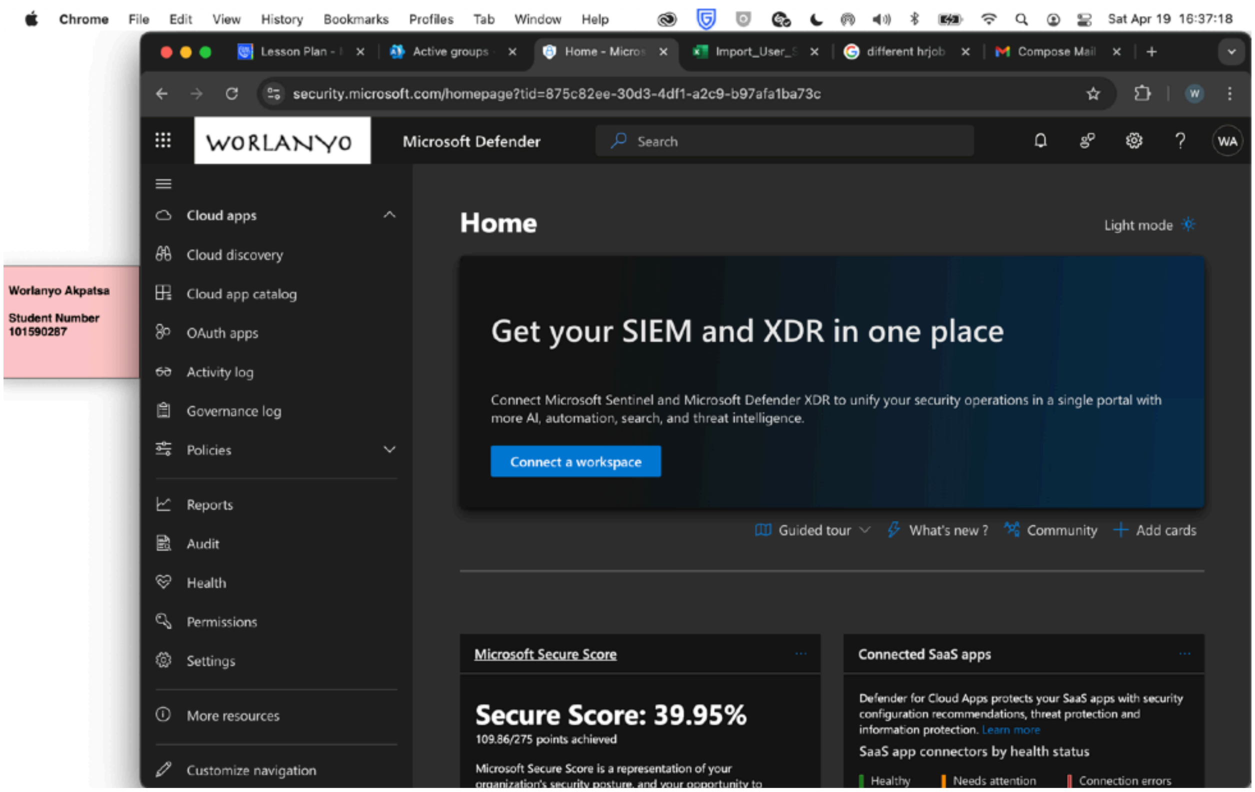
1: Set up and configure Microsoft Defender for Office 365

1.1: Access the MS Defender and navigate to Secure Score

A: Navigate to Admin Center Homepage and select Security under Admin Centers



B: Microsoft Defender Homepage

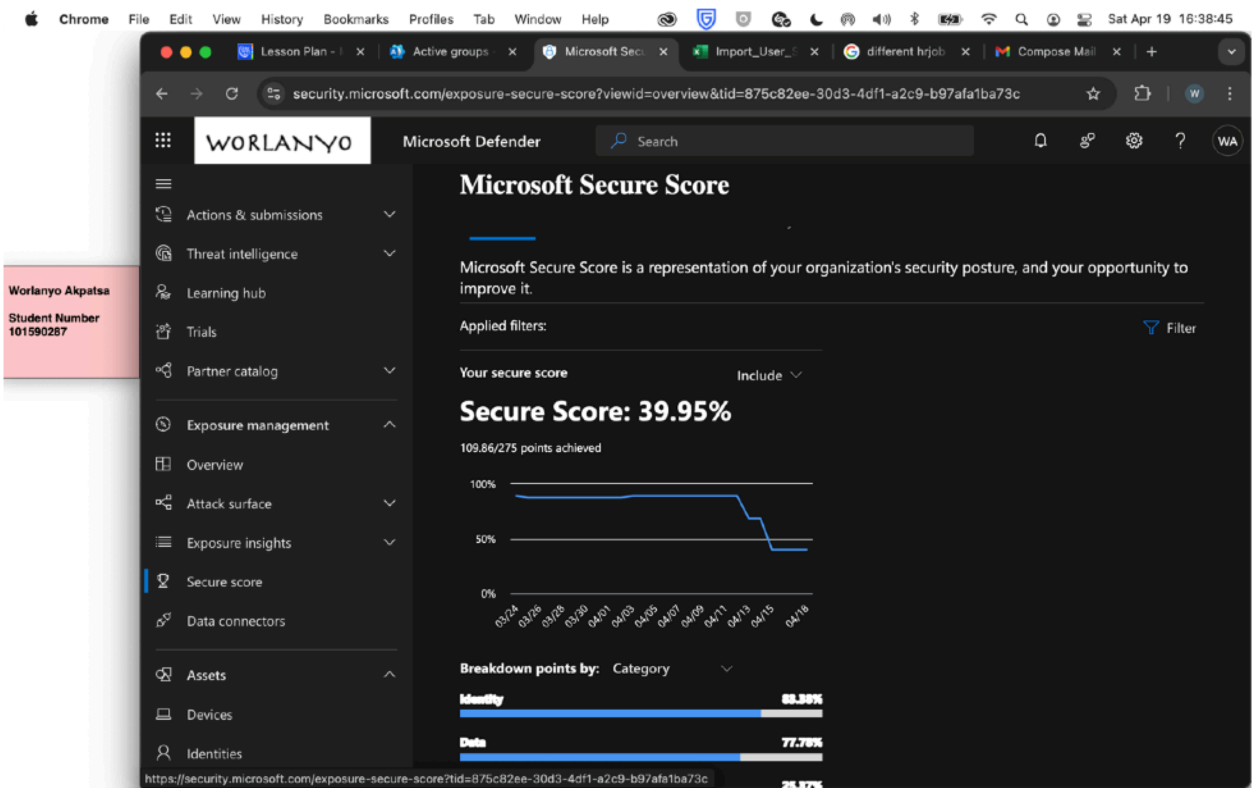


C: Navigate to Secure Score in the left Pane

~~~~~~

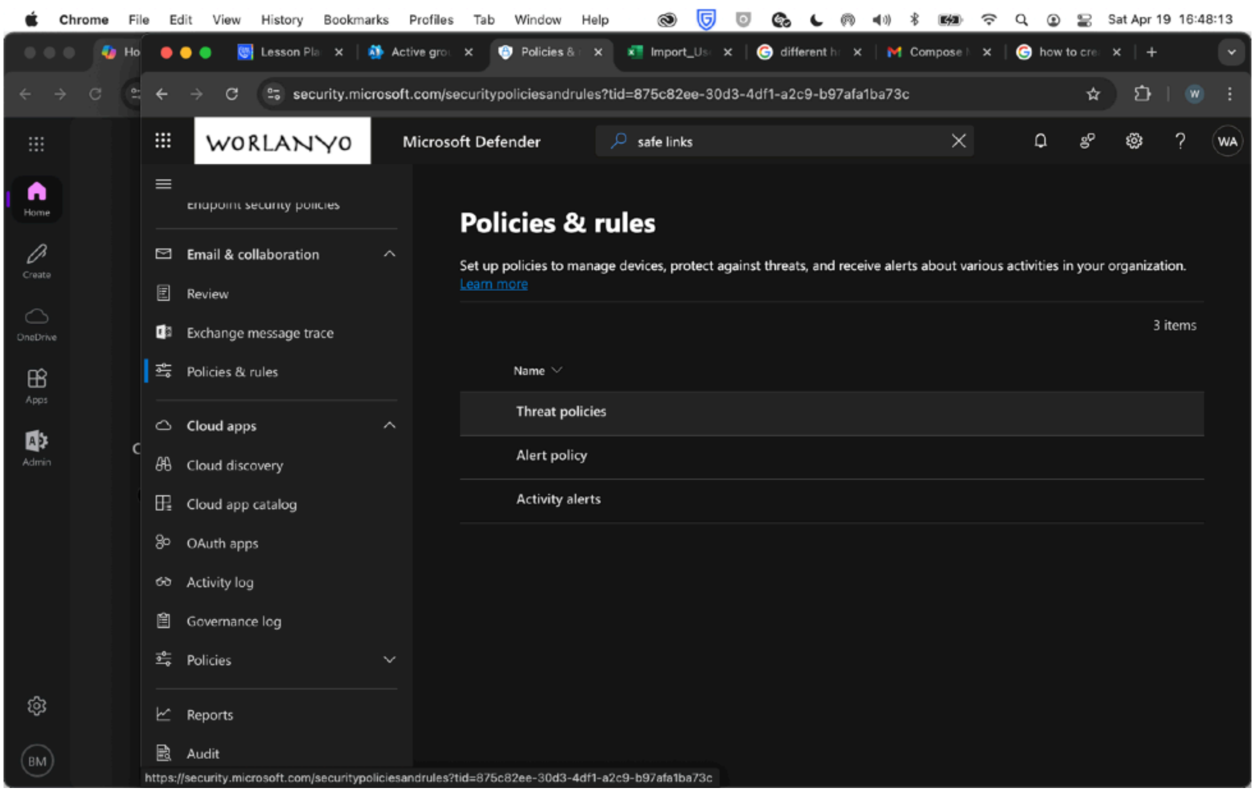
Student Name: Worlanyo Akpatsa Term: Winter 2025
Student ID: 101590287

~~~~~~



1.2: Ensure that Safe Links and Safe Attachments have been enabled for all users

A: Navigate to Policies & Rules and select threat policies



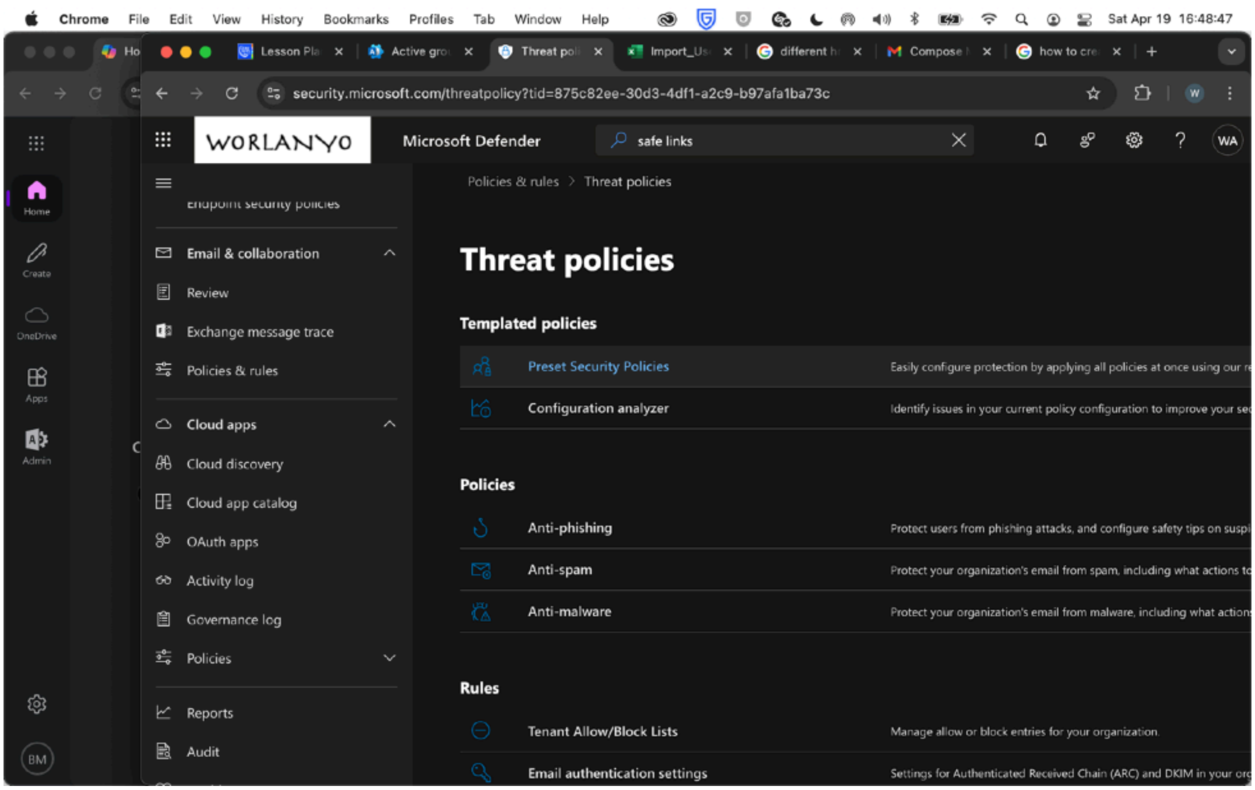
~~~~~~
~~~~

Student Name: Worlanyo Akpatsa
Student ID: 101590287

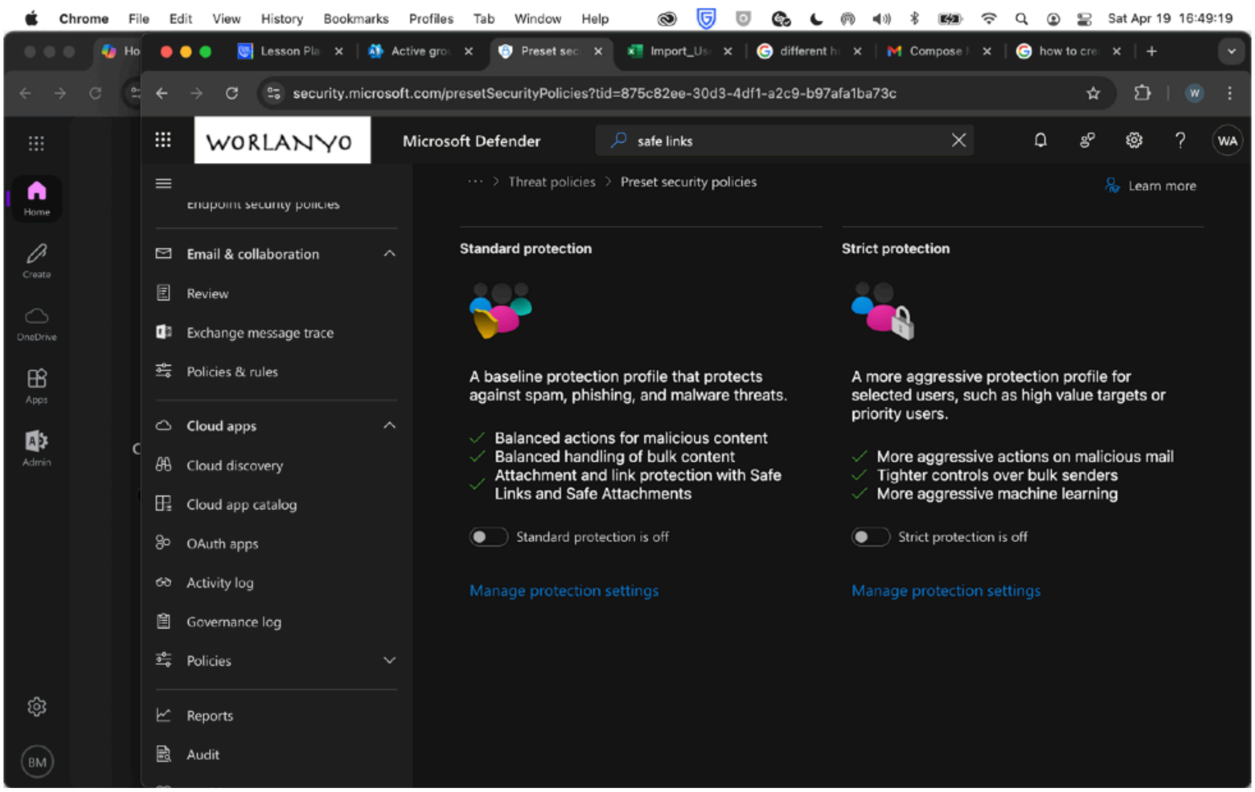
Term: Winter 2025

~~~~~~
~~~~

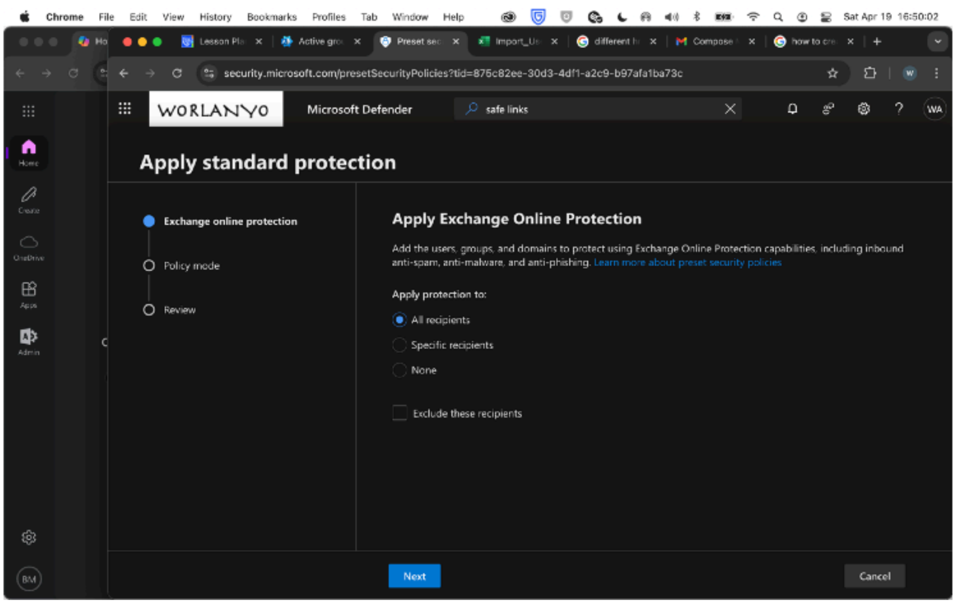
B: In Threat Policy Window, select Preset Security Policies

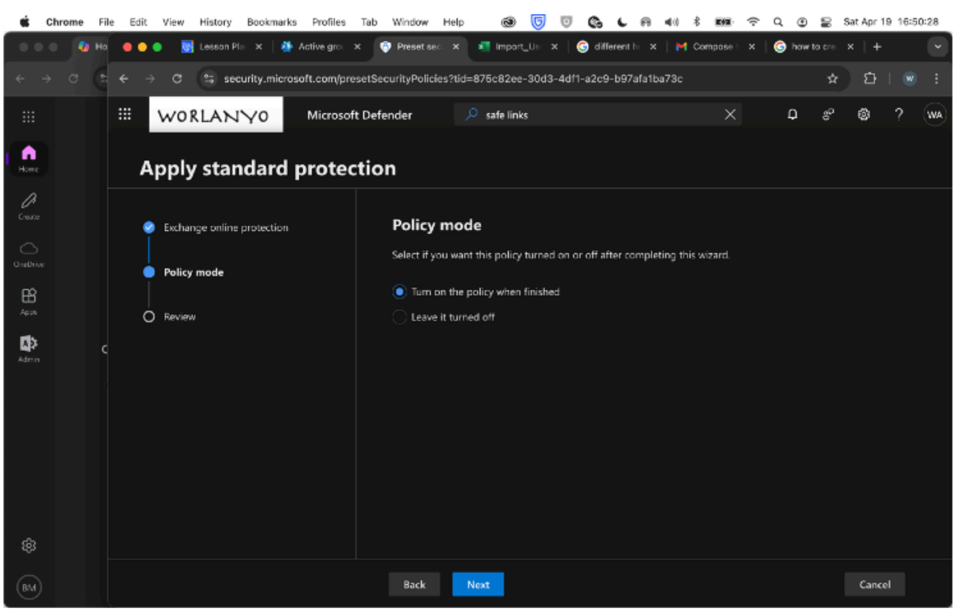


C: Turn on Standard Protection and click "Manage Protection Settings"

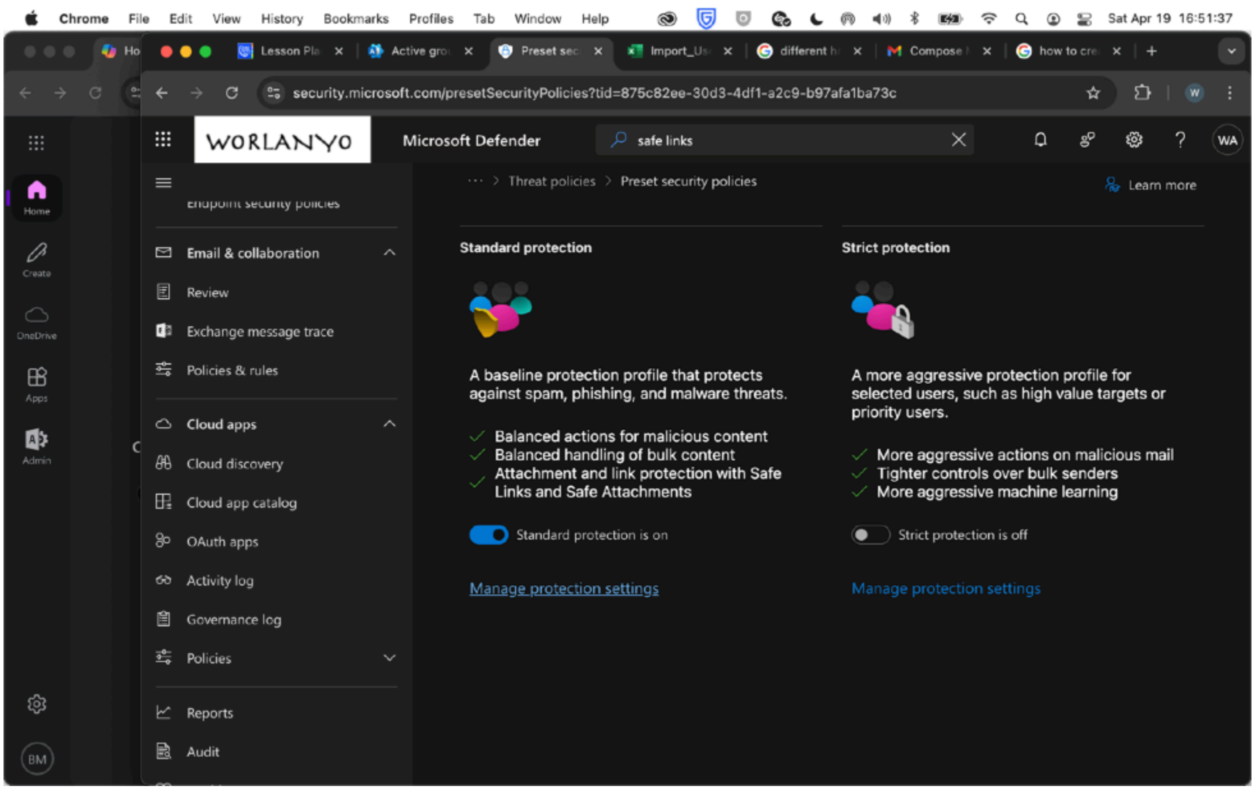


D: Applying protection to all recipients and turning policy on





E: Safe Links and Safe Attachments protection is turned on for all users



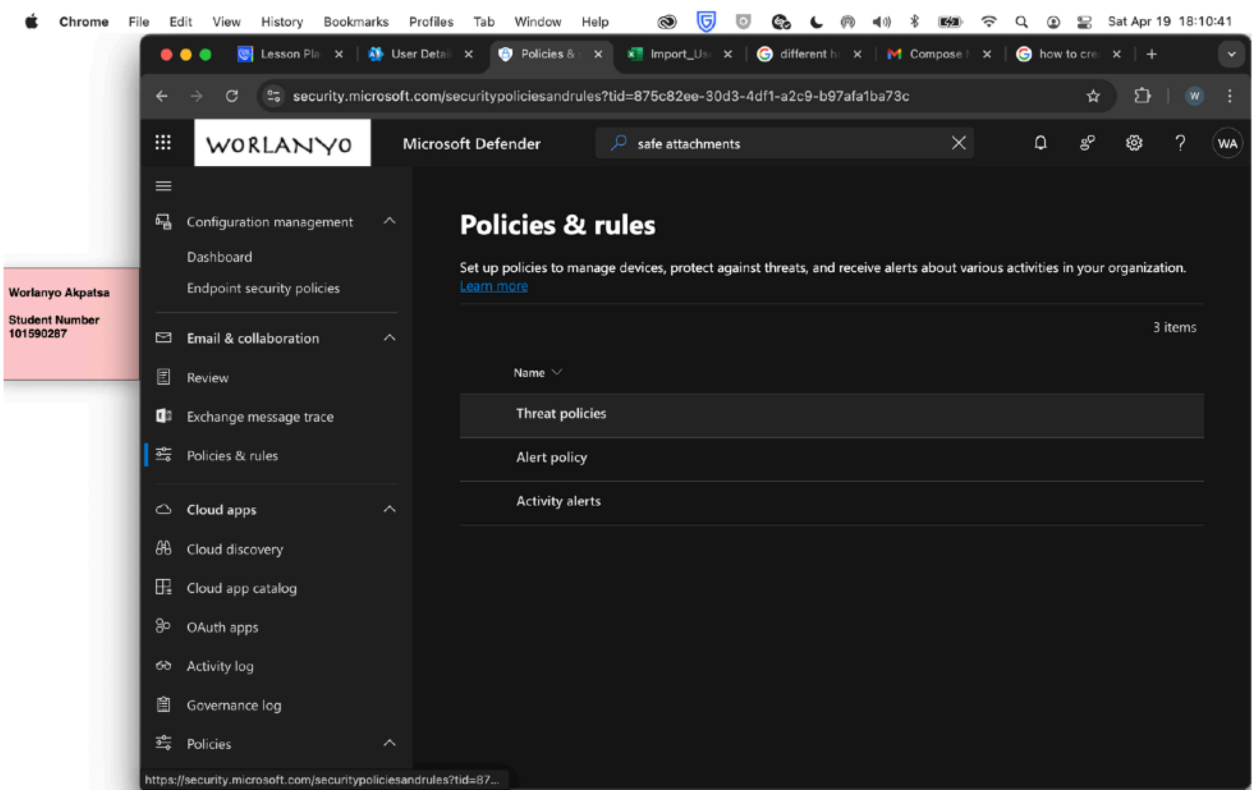
~~~~~~

Student Name: Worlanyo Akpatsa Term: Winter 2025
Student ID: 101590287

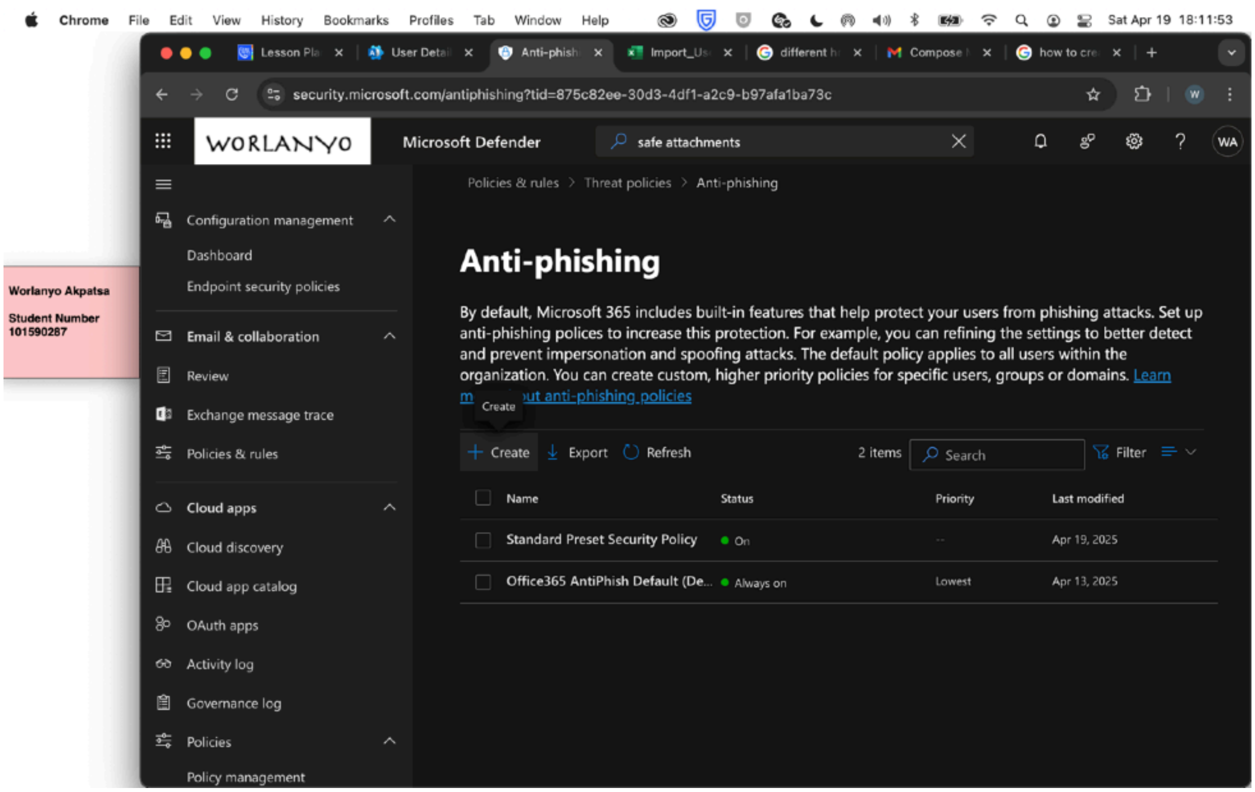
~~~~~~

1.3: Navigate to Policies and Rules then configure at least one policy to protect against phishing, malware or spam.

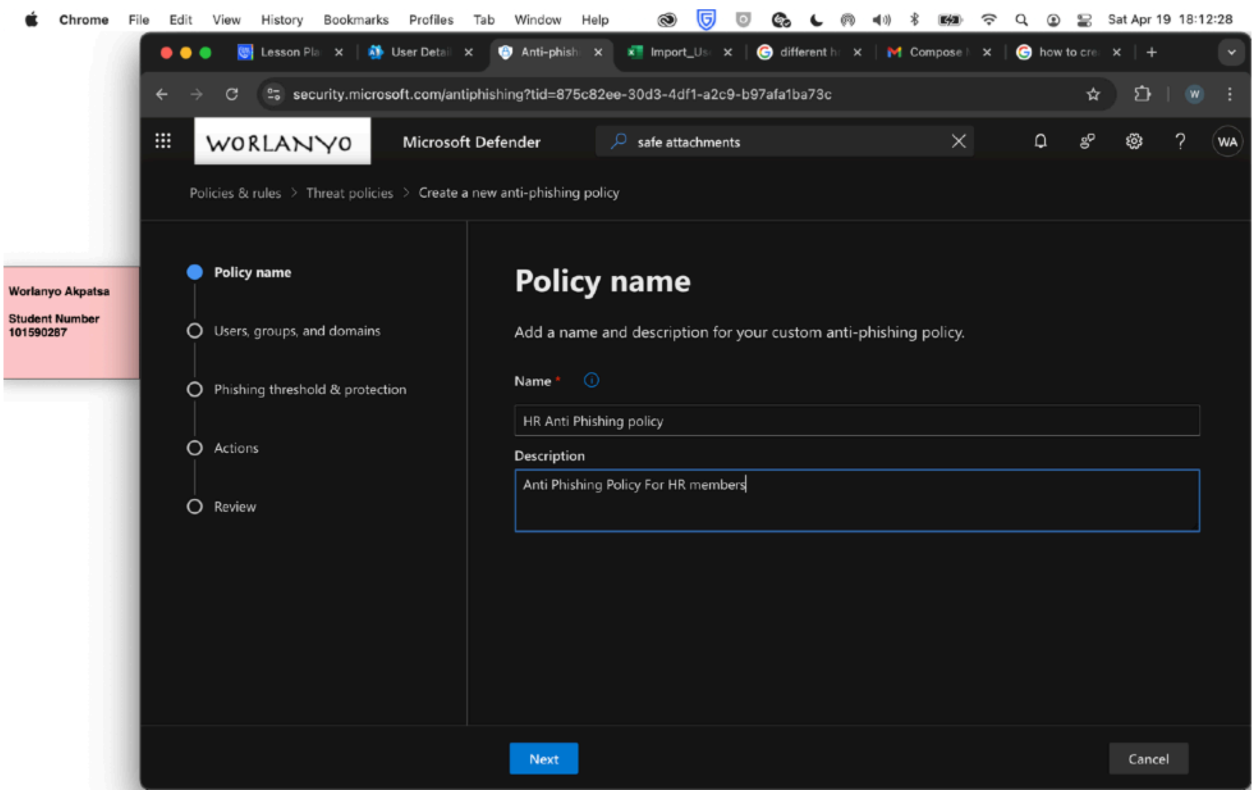
A: Navigate to Policies and Rules in Microsoft Defender and select Threat Policies



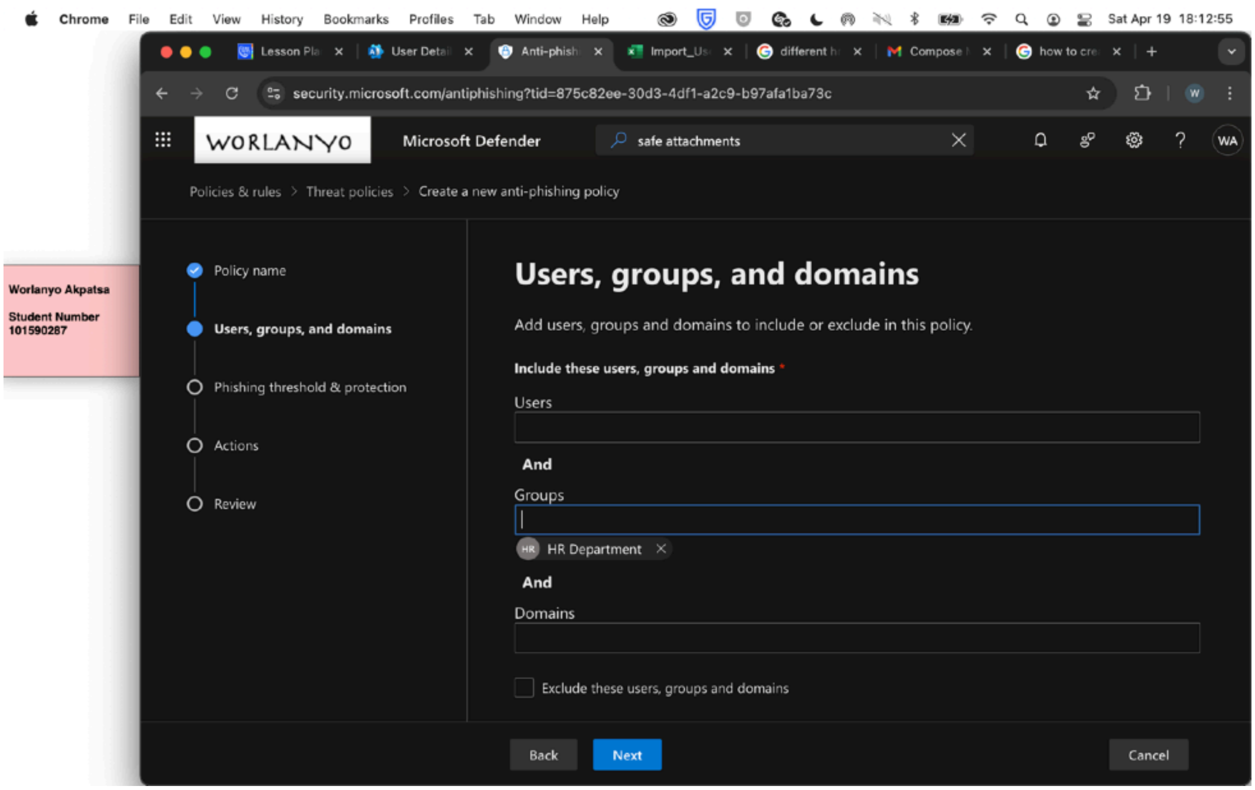
B: Configuring Anti-phishing policy by clicking create new policy



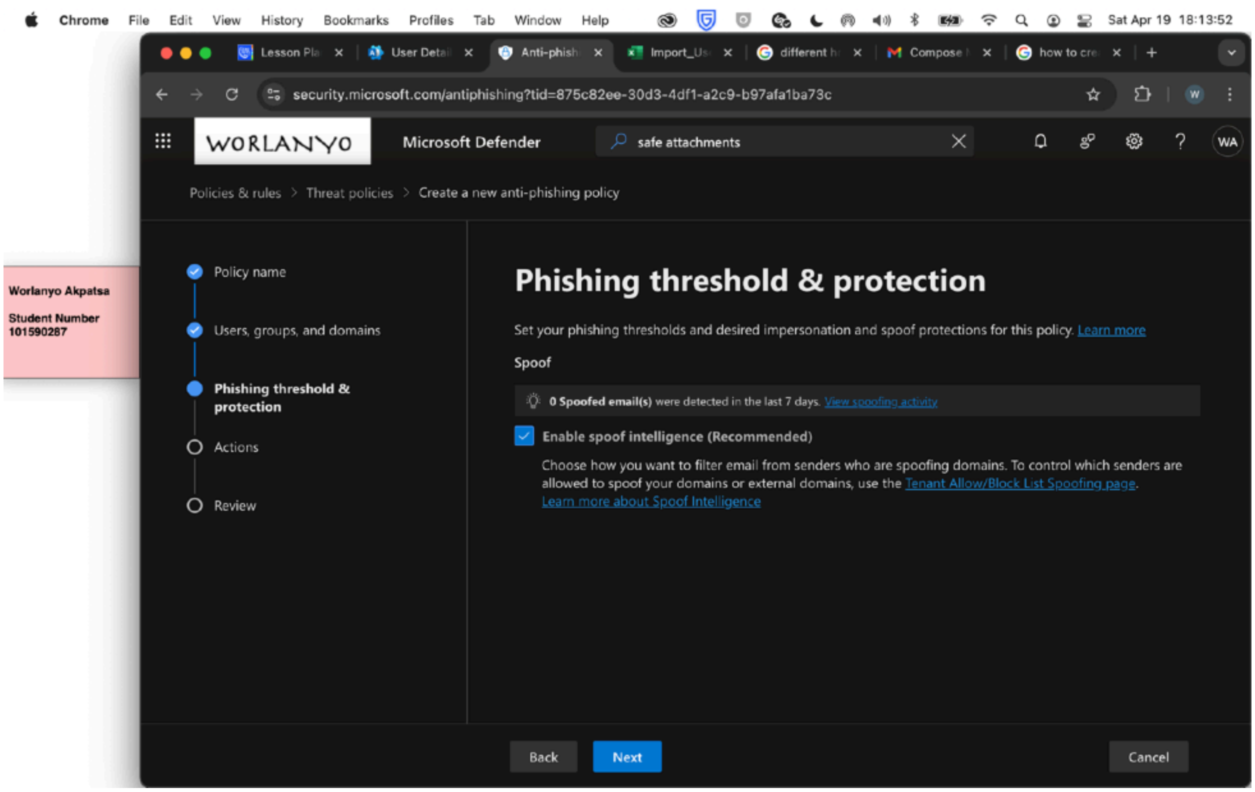
C: Policy Creation (Name and description)



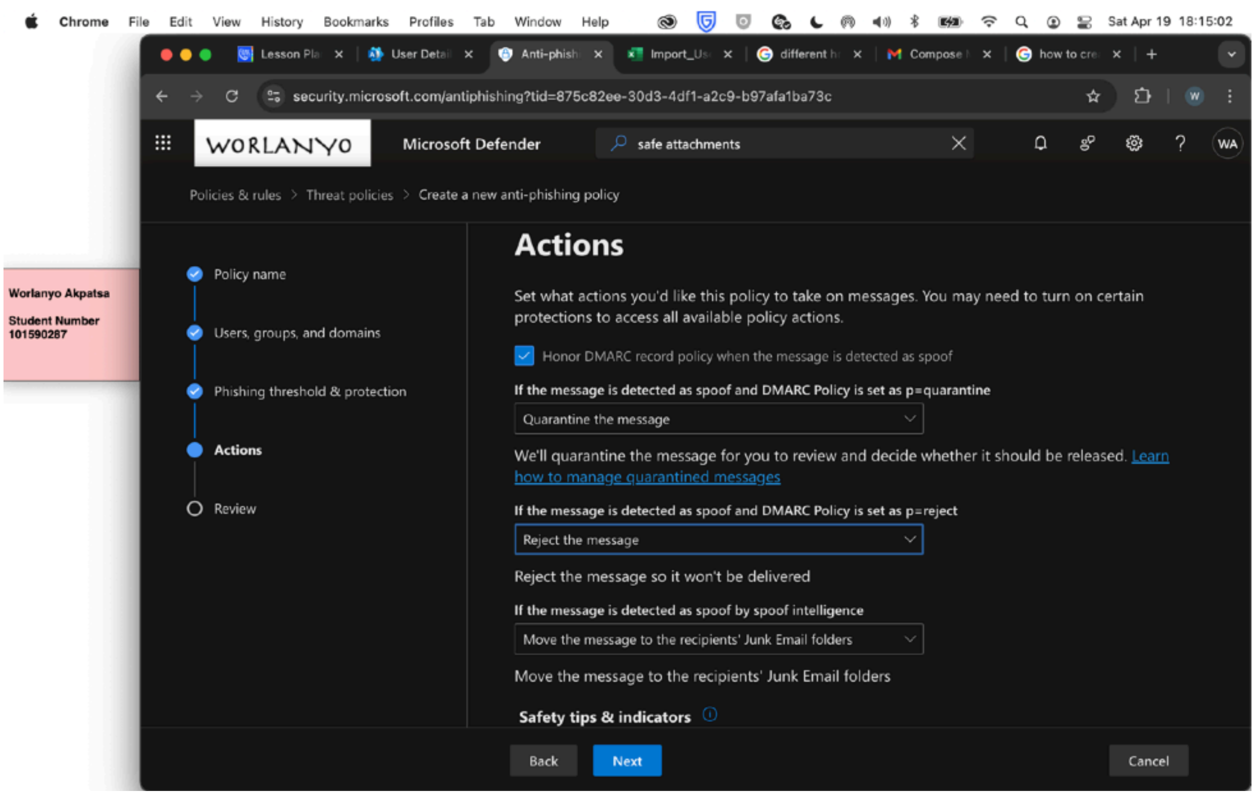
D: Adding HR department as target for policy



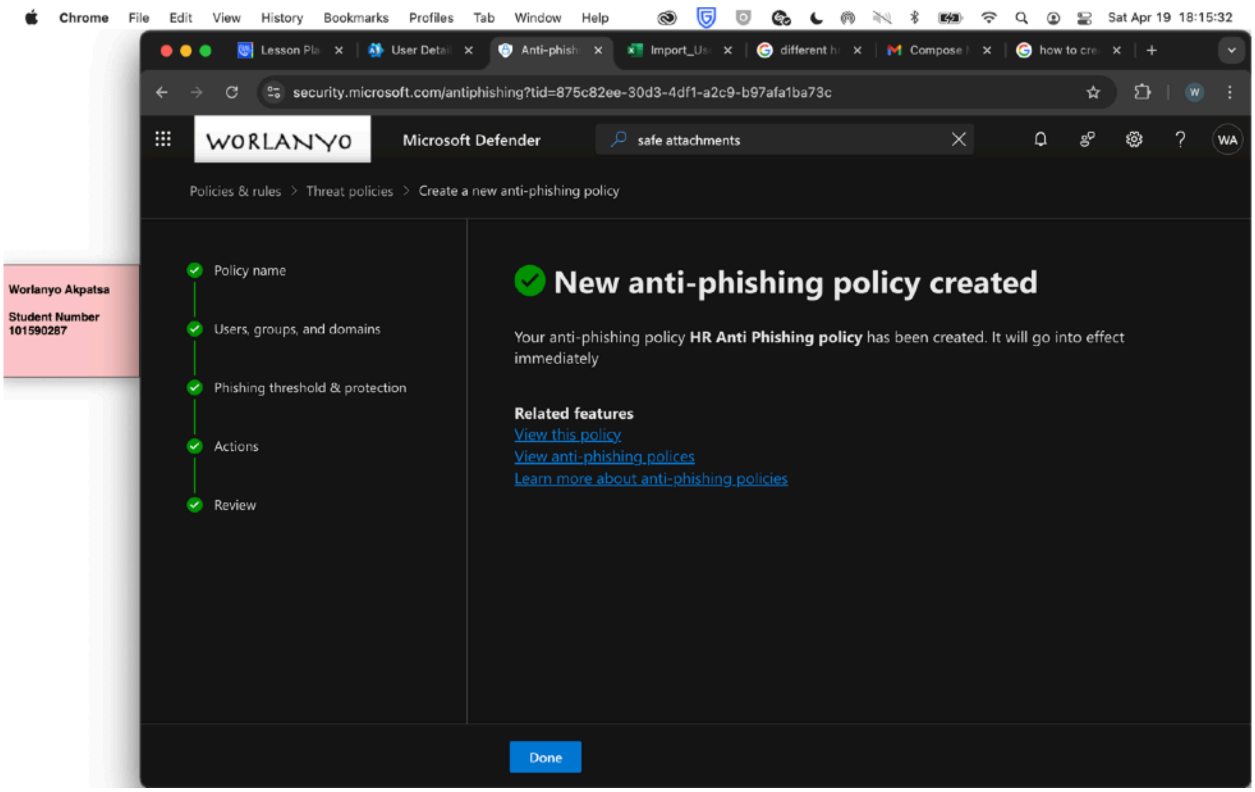
E: Adding phishing threshold and protection for policy



F: Configuring policy actions



G: Policy Created

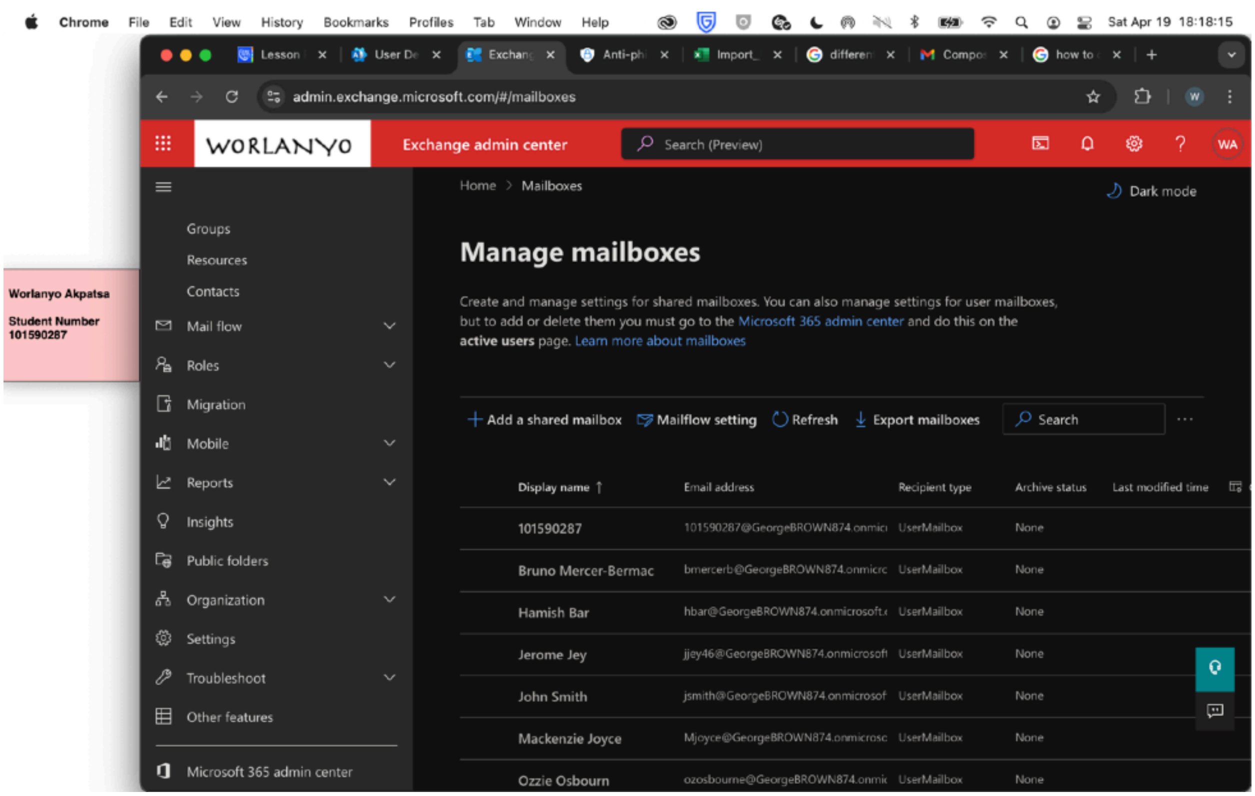


2: Set up Data Encryption

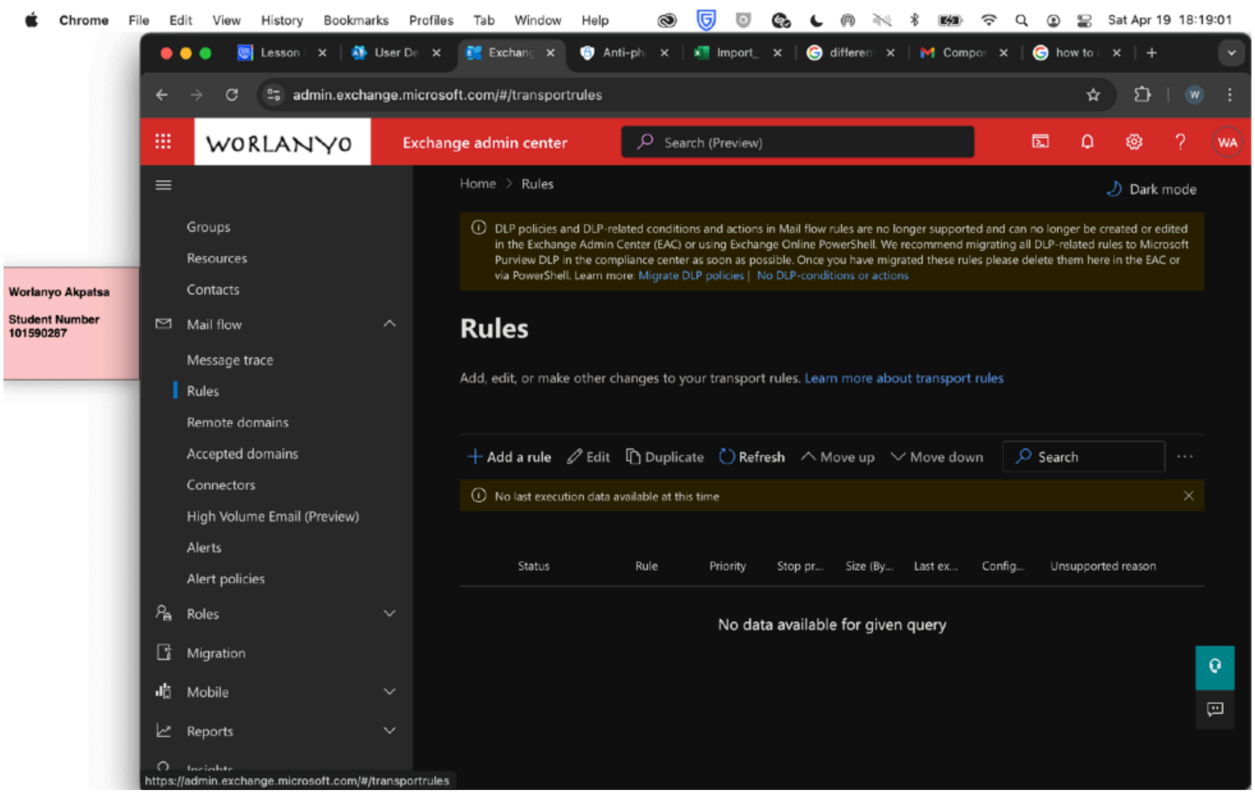
2.1: Configure Microsoft 365 Message Encryption

2.2: Ensure that emails inside the organization are automatically encrypted

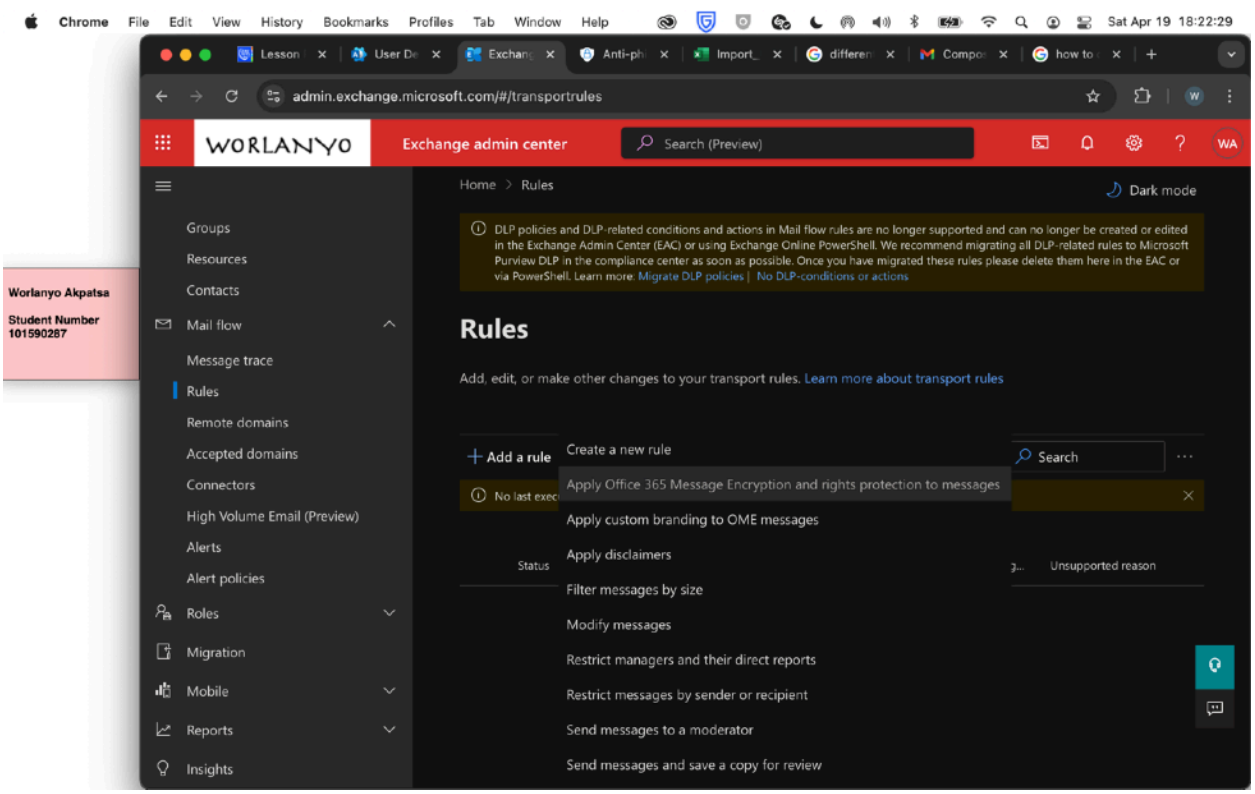
A: Navigate to Exchange Admin Center Homepage by clicking exchange under admin centers in 365 Admin Center



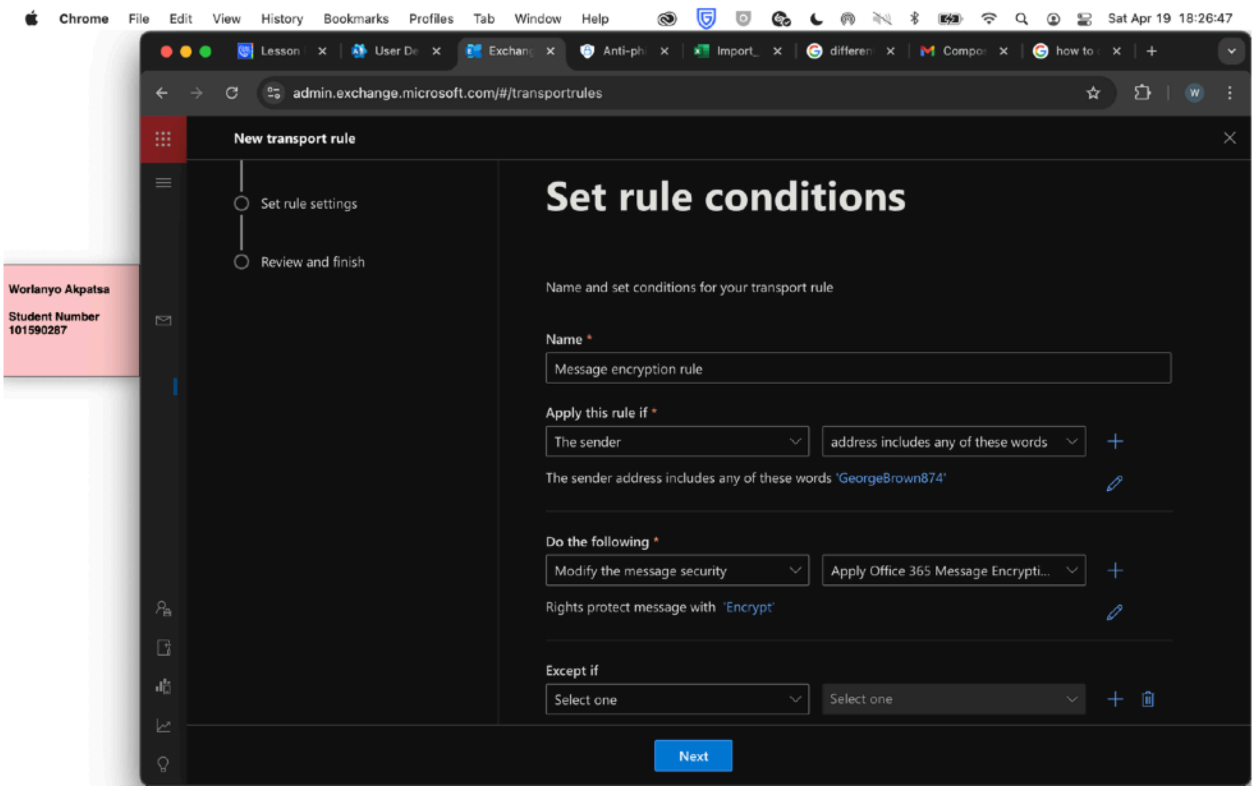
B: Select Mail Flow->rules in the left pane



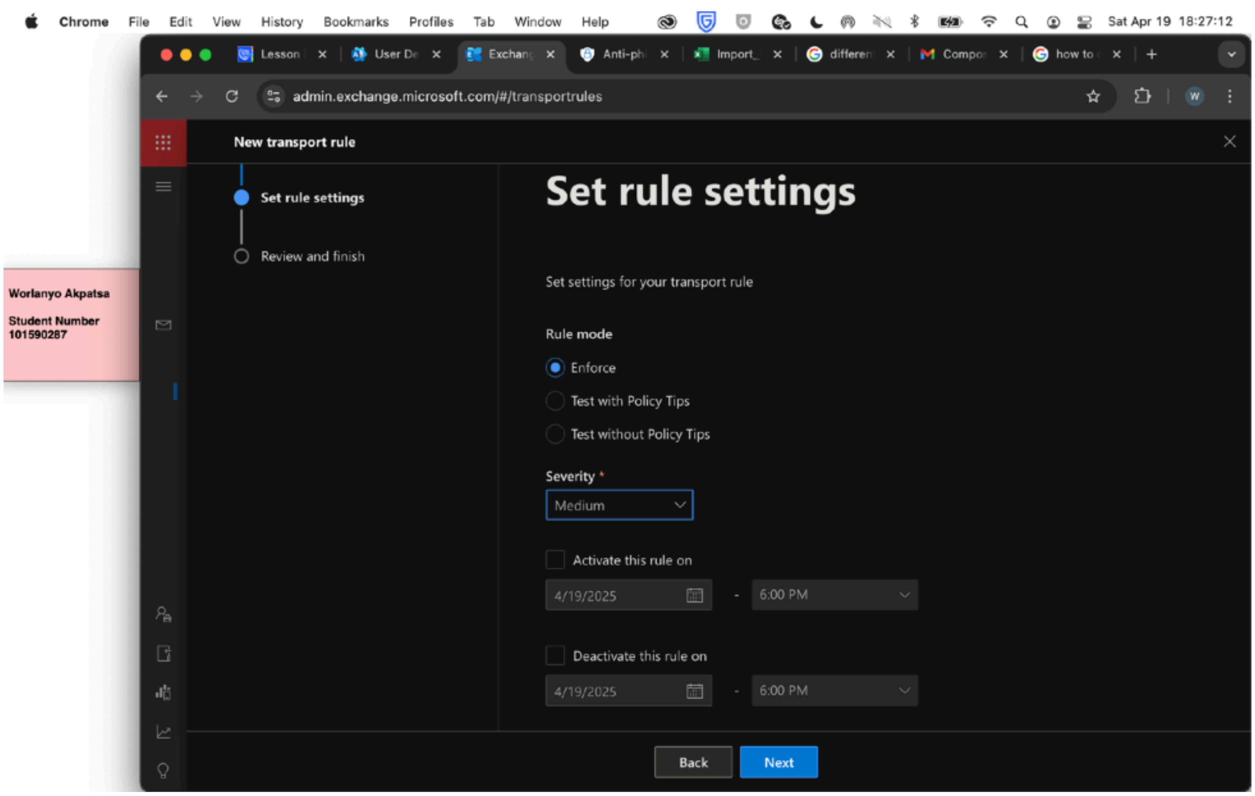
C: Create Rule to Encrypt Messages (Select "Apply Office 365 Message Encryption and rights protection to messages)



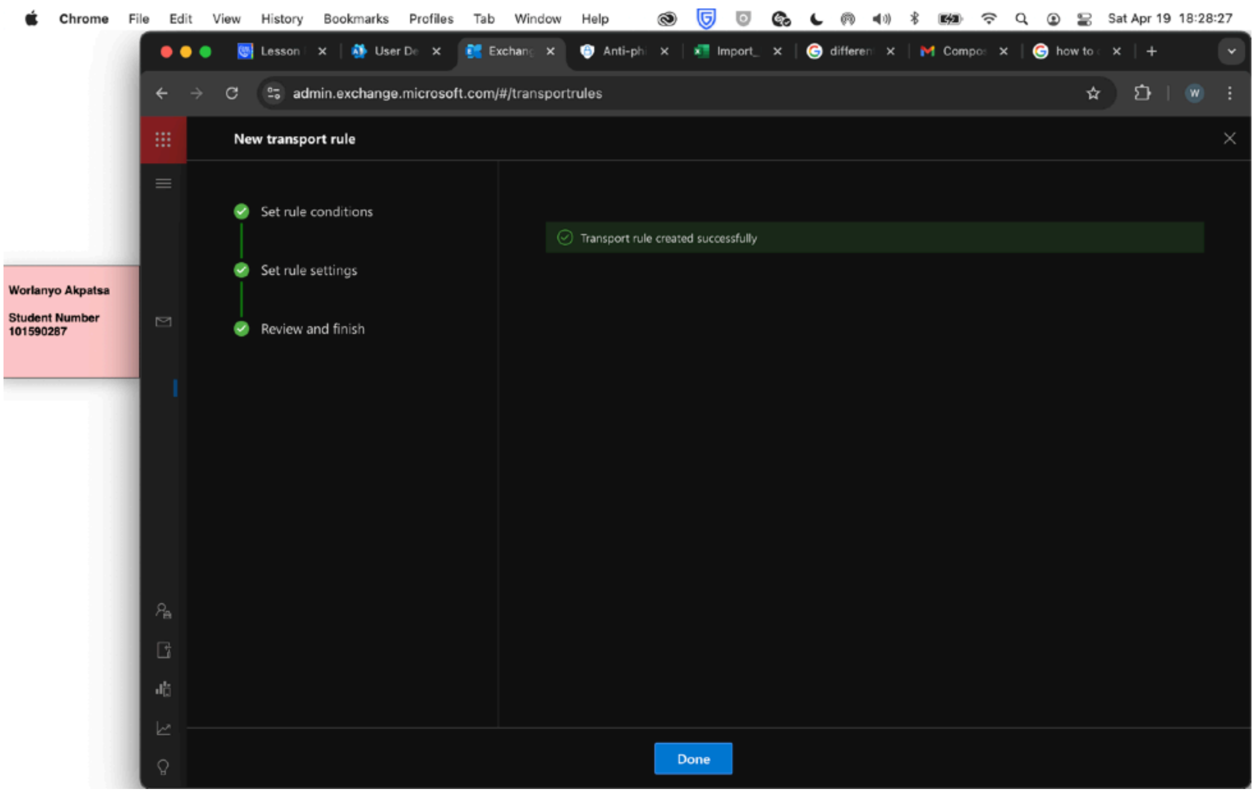
D: Setting Rule Name and Conditions



E: Final Rule Settings



F: Rule Created



Student Name: Worlanyo Akpatsa Term: Winter 2025
Student ID: 101590287

Task 2 Summary:

Task 2 was all about implementing security measures and to do this I had to use the Microsoft Defender. Another thing that is really key for companies is security so I am happy this was included in the project.

I navigated to my admin center and selected security under admin centers on the left pane. This takes me to the MS Defender homepage. In the left pane, I clicked on secure score to view the secure score page. I never knew about this; this page and everything in it shows a true representation of your companies security. My companies score is not that high so I made sure to make some changes and create some policies to increase this.

Next, I had to ensure that Safe links and attachments were enabled for all users. I clicked on policies and rules in the left pane and selected threat policies.

In this window, I chose preset security policies and enabled my standard protection. I could not believe this was off; maybe why my secure score was low.

I applied protection to all recipients and turned this policy on immediately. This enabled my safe links and safe attachments protection.

Next I had to configure a policy against phishing. Still in threat policies, I clicked on the anti phishing policy and chose to create a new one. I added my HR department as the target for this policy and added phishing threshold and protection. Next I reviewed the policy actions which were to reject a message if it was detected as spoof. I concluded and created my policy.

Next I had to set up data encryption; to be specific, configure ms 365 message encryption. For this, I had to use the exchange admin center. I navigated to my 365 admin center homepage and selected exchange under admin centers. This took me to my exchange admin center homepage. I chose mail flow->rules in the left pane and chose to create a new rule.

I named my rule and set my rule conditions to encrypt a message if the sender was a member of my organization. I then chose to enforce my rule immediately. I reviewed my settings and created my rule.

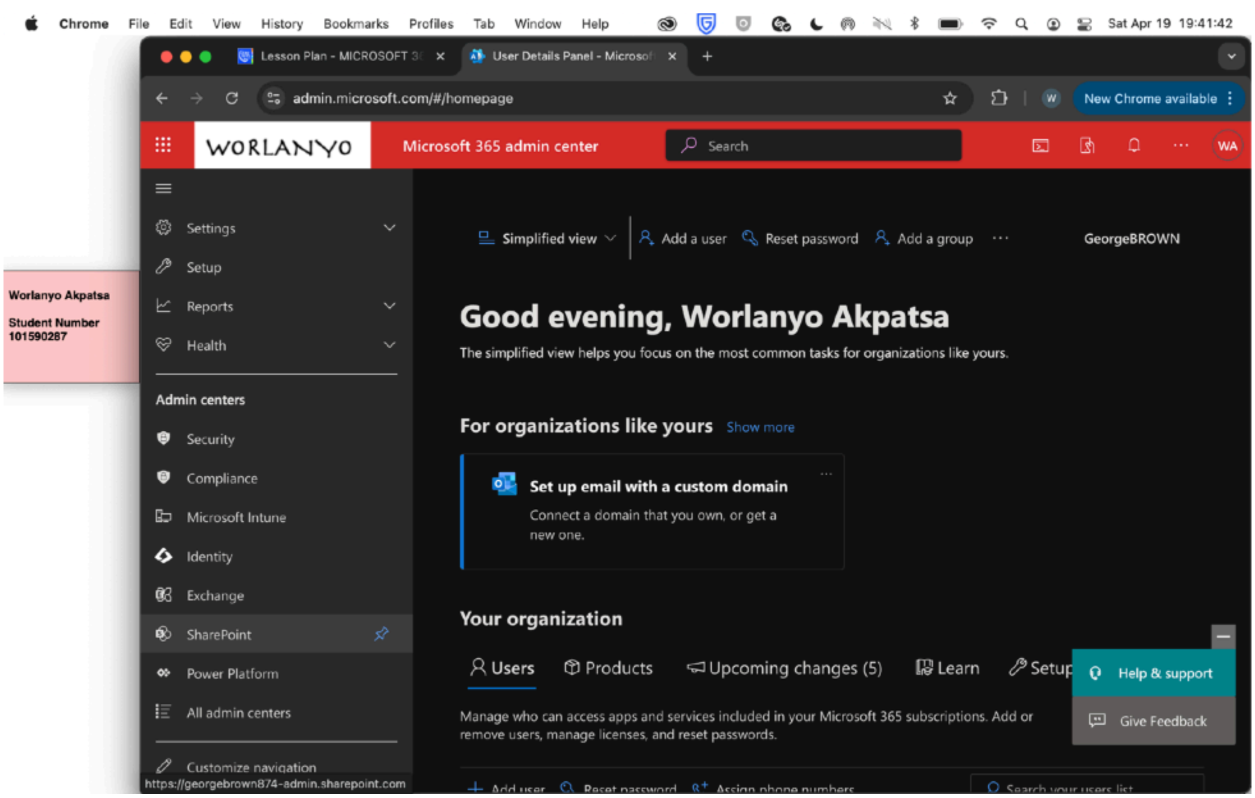
I am sure after this my security score will be increased.

TASK 3: CONFIGURING AND MANAGING COLLABORATION TOOLS

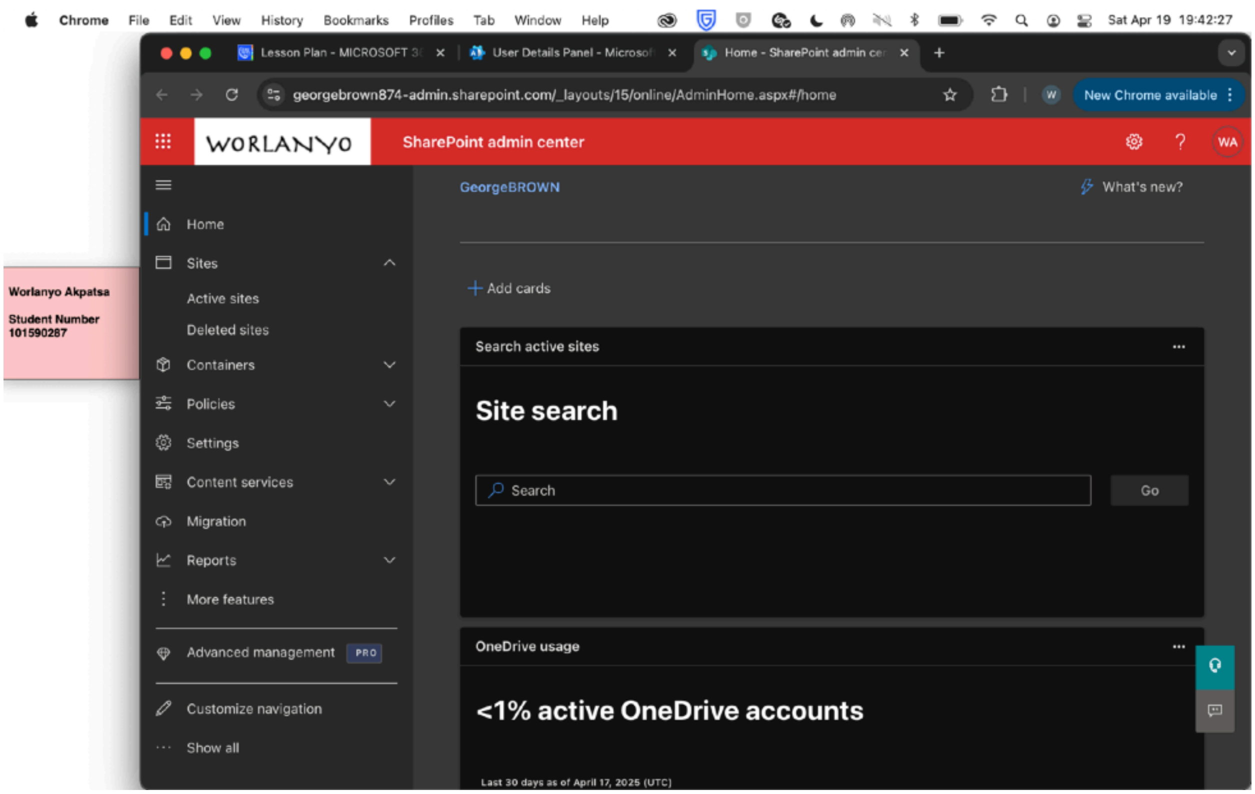
1: Set up Sharepoint Online

1.1: Create an Online Sharepoint Site for each department (IT, HR, Marketing)

A: Navigate to Sharepoint Admin Center by clicking Sharepoint under admin centers in 365 admin center



B: Sharepoint Homepage

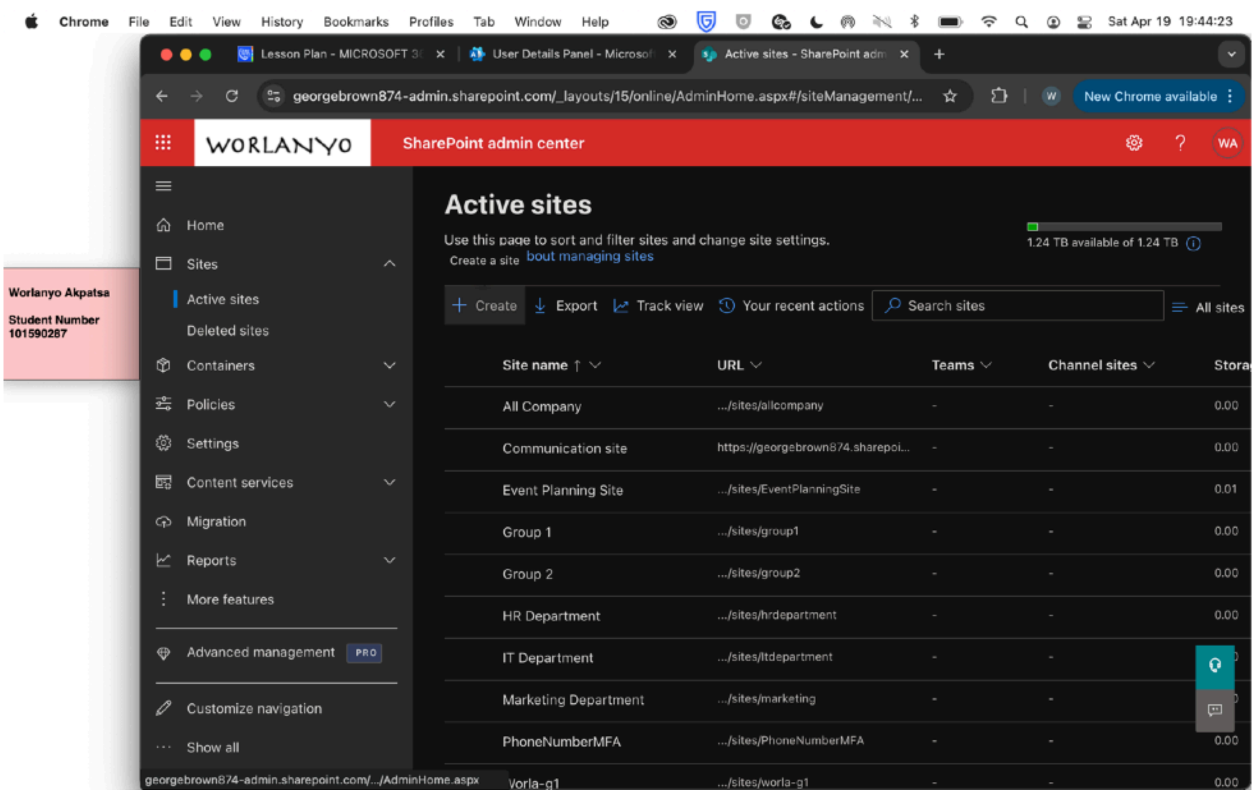


~~~~~~

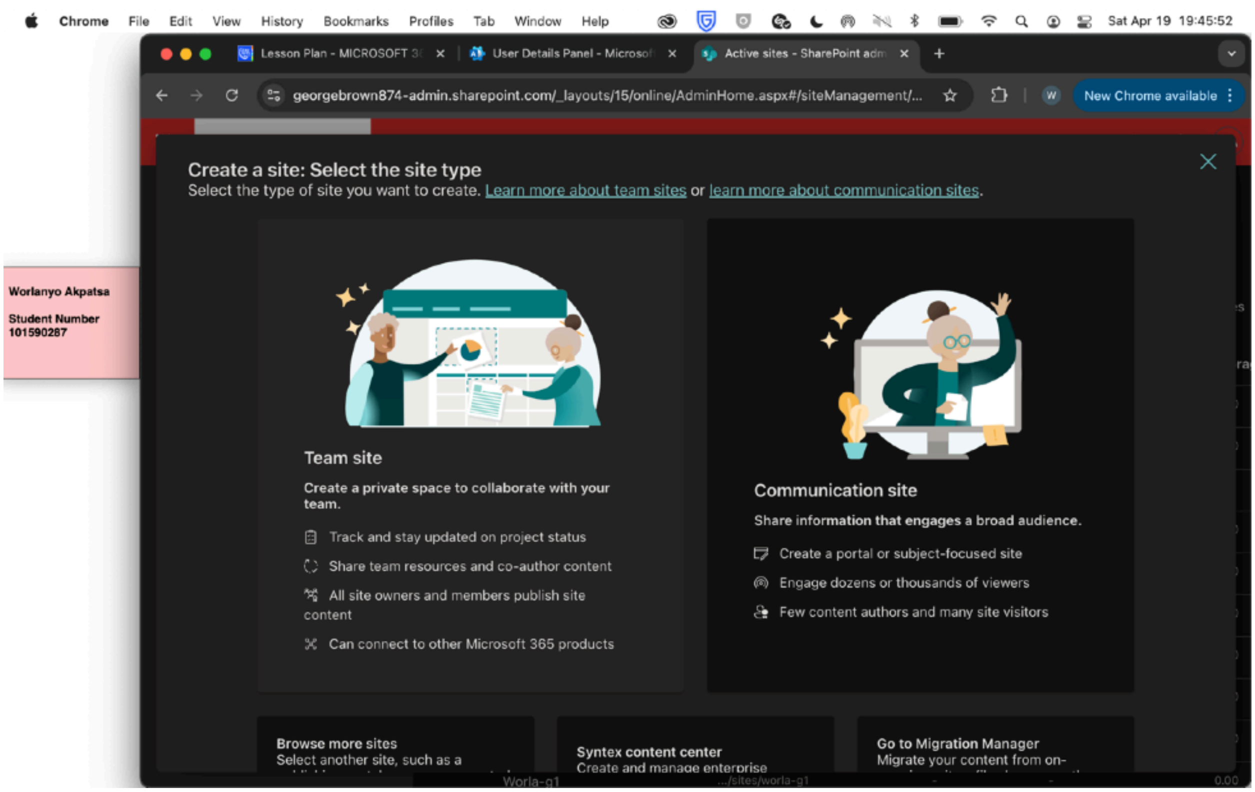
Student Name: Worlanyo Akpatsa Term: Winter 2025
Student ID: 101590287

~~~~~~

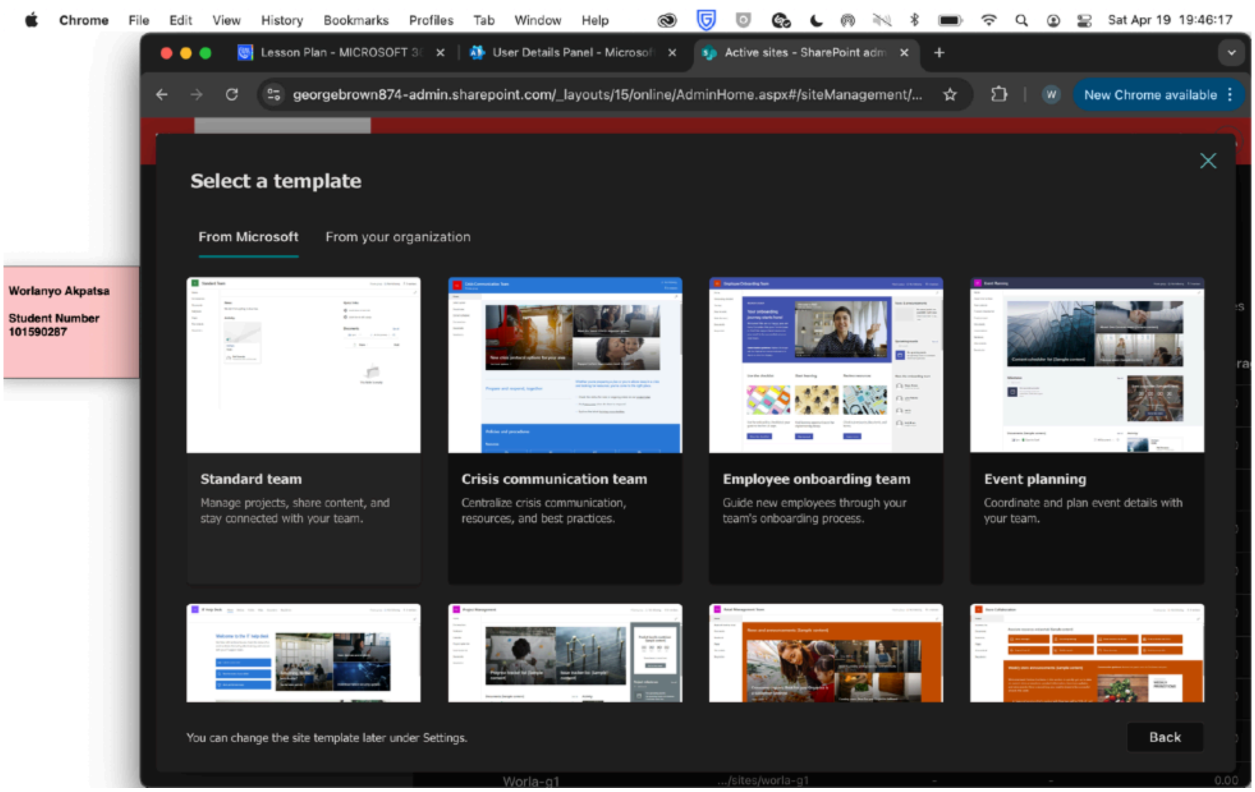
C: Navigate to sites->active sites on the left pane and click create to create new site



D: Creating site type (team site)

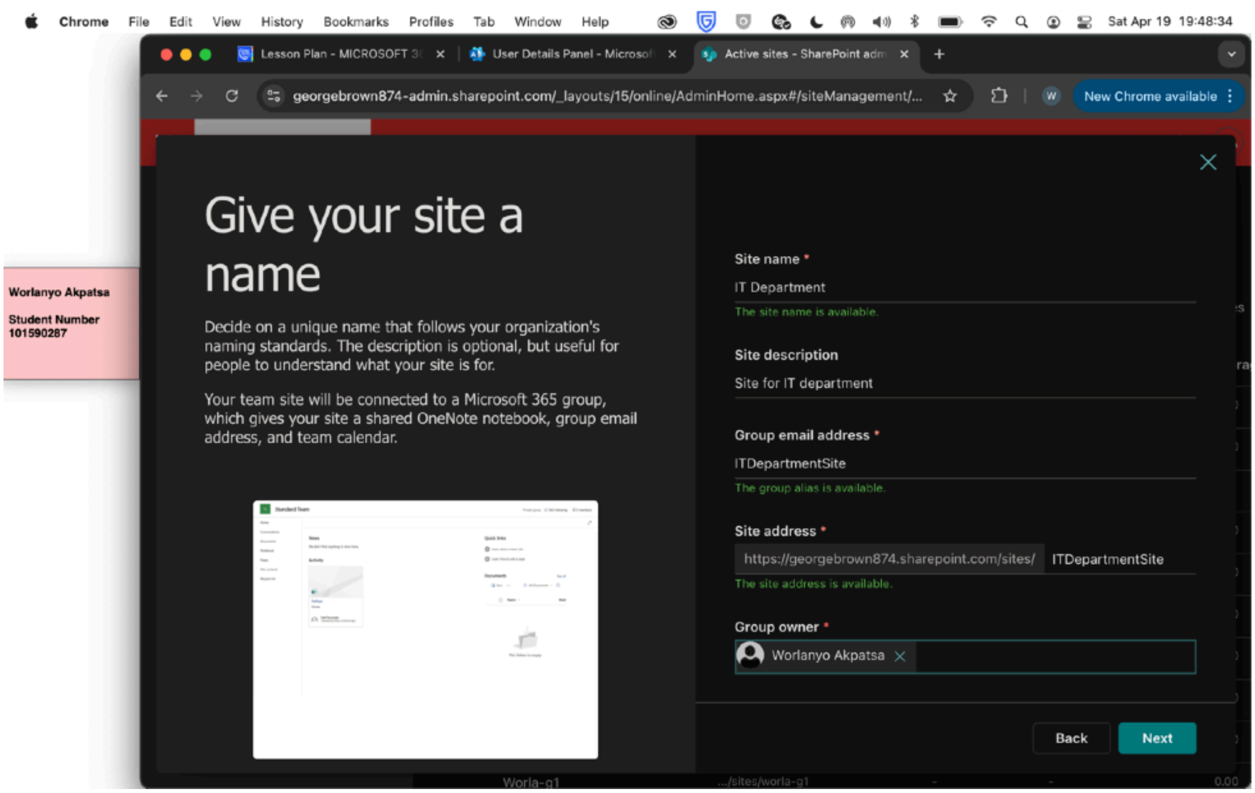


E: Choosing template for site

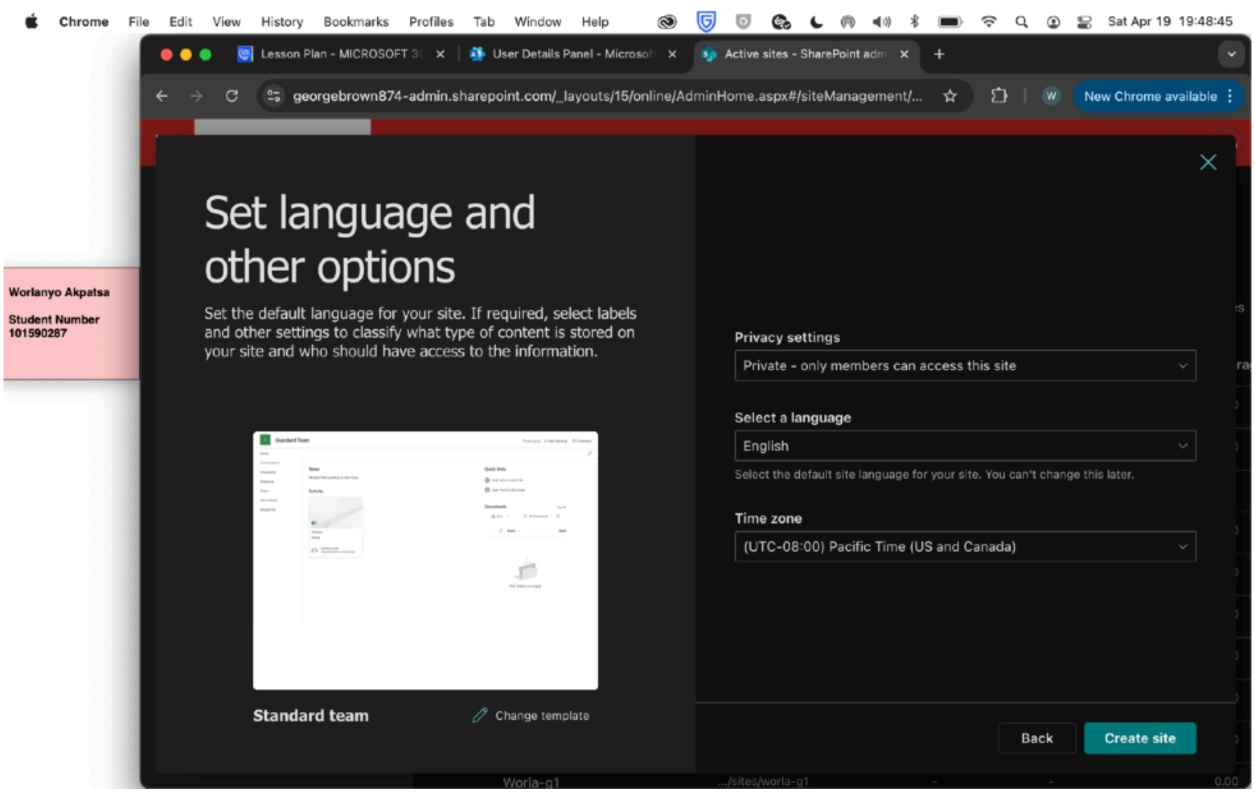


CREATING TEAM SITE FOR IT DEPARTMENT

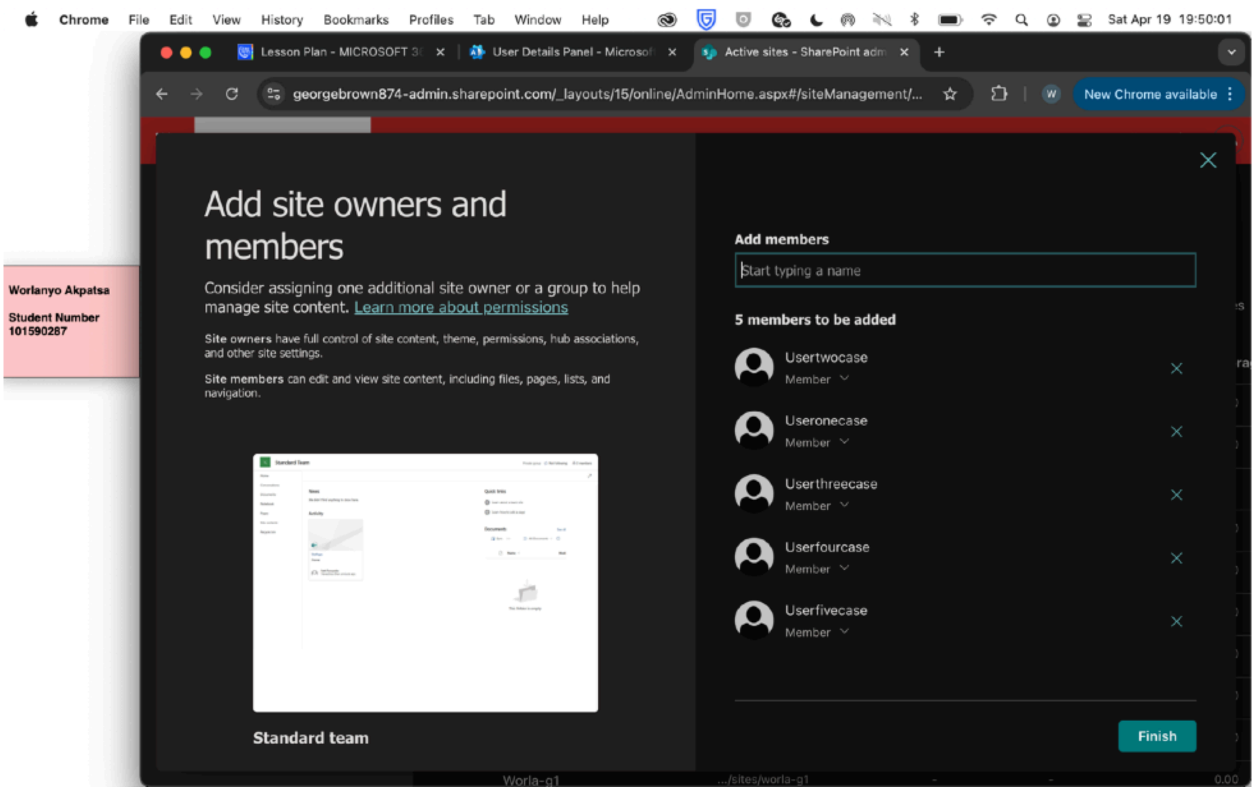
A: Choosing site name, description, and address



B: Setting Privacy Settings, Language and Time Zone



C: Adding members per CSV file



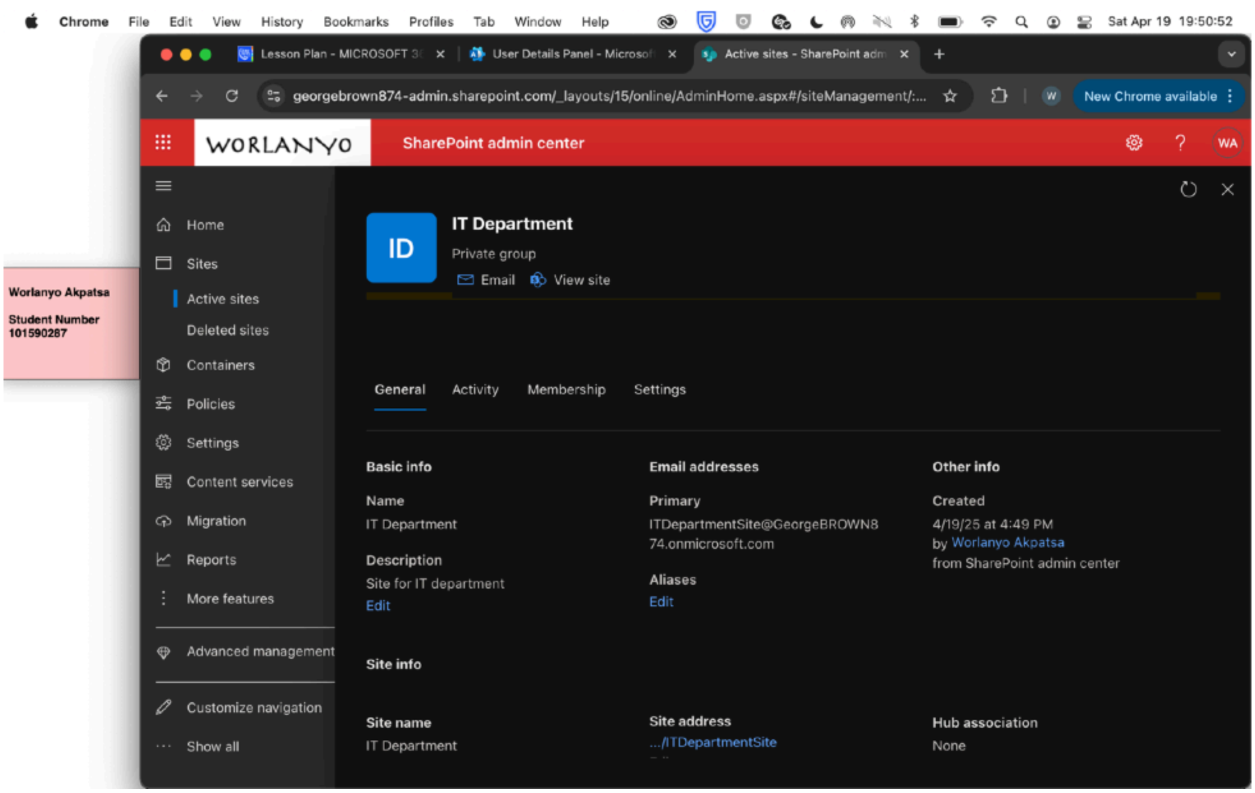
~~~~~~

Student Name: Worlanyo Akpatsa
Student ID: 101590287

Term: Winter 2025

~~~~~~

D: IT Site Created

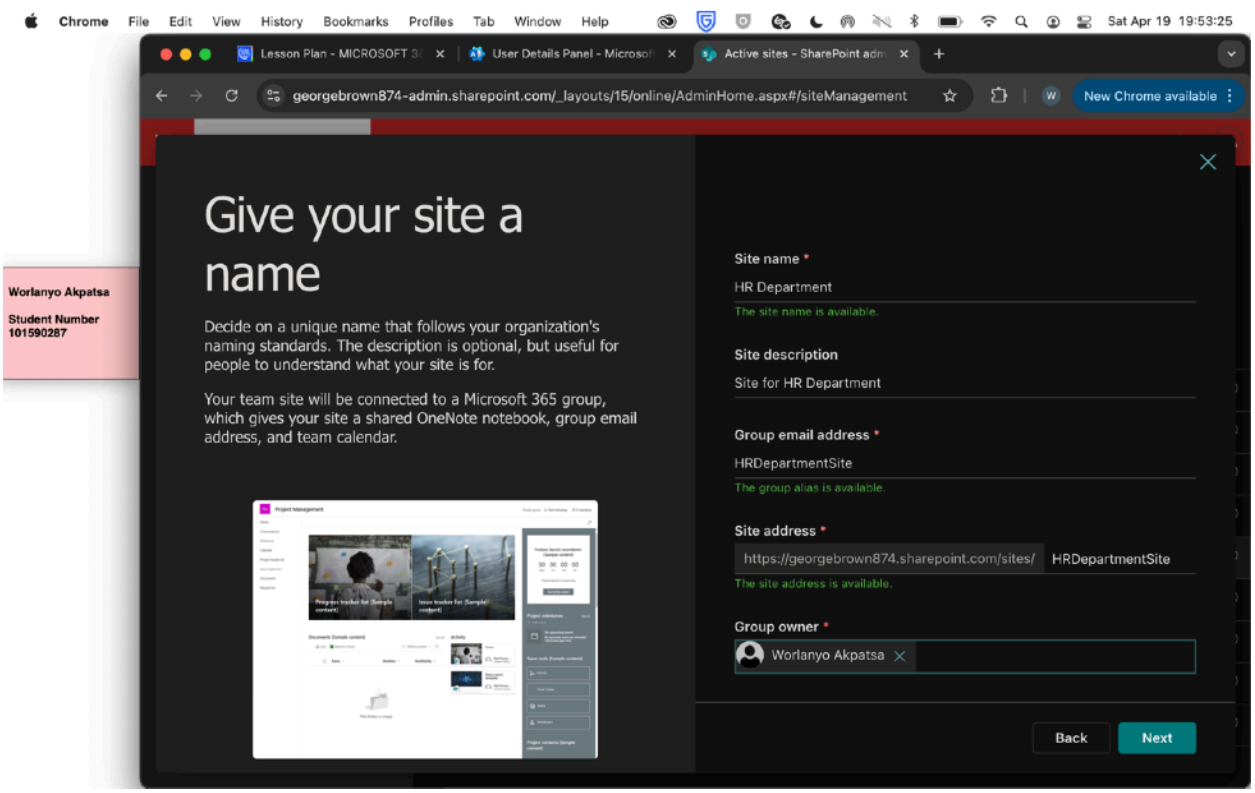


Student Name: Worlanyo Akpatsa
Student ID: 101590287

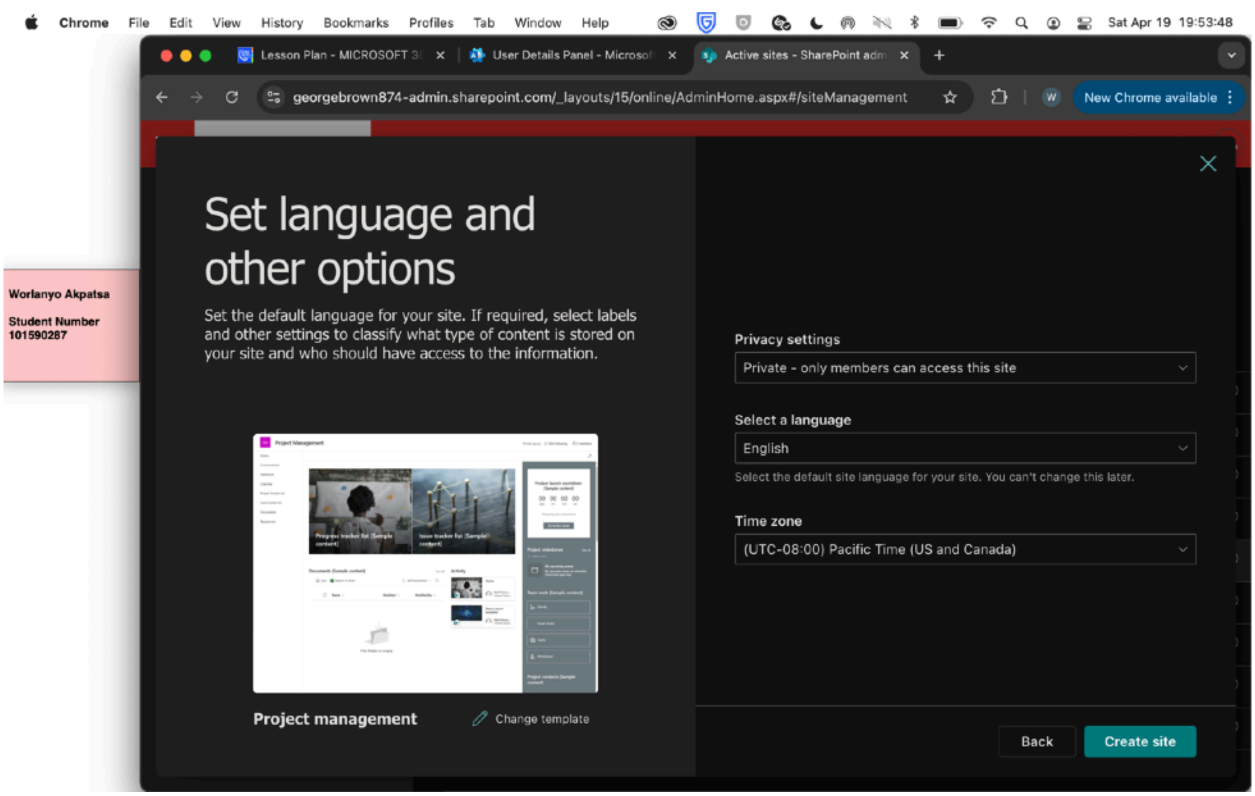
Term: Winter 2025

CREATING TEAM SITE FOR HR DEPARTMENT

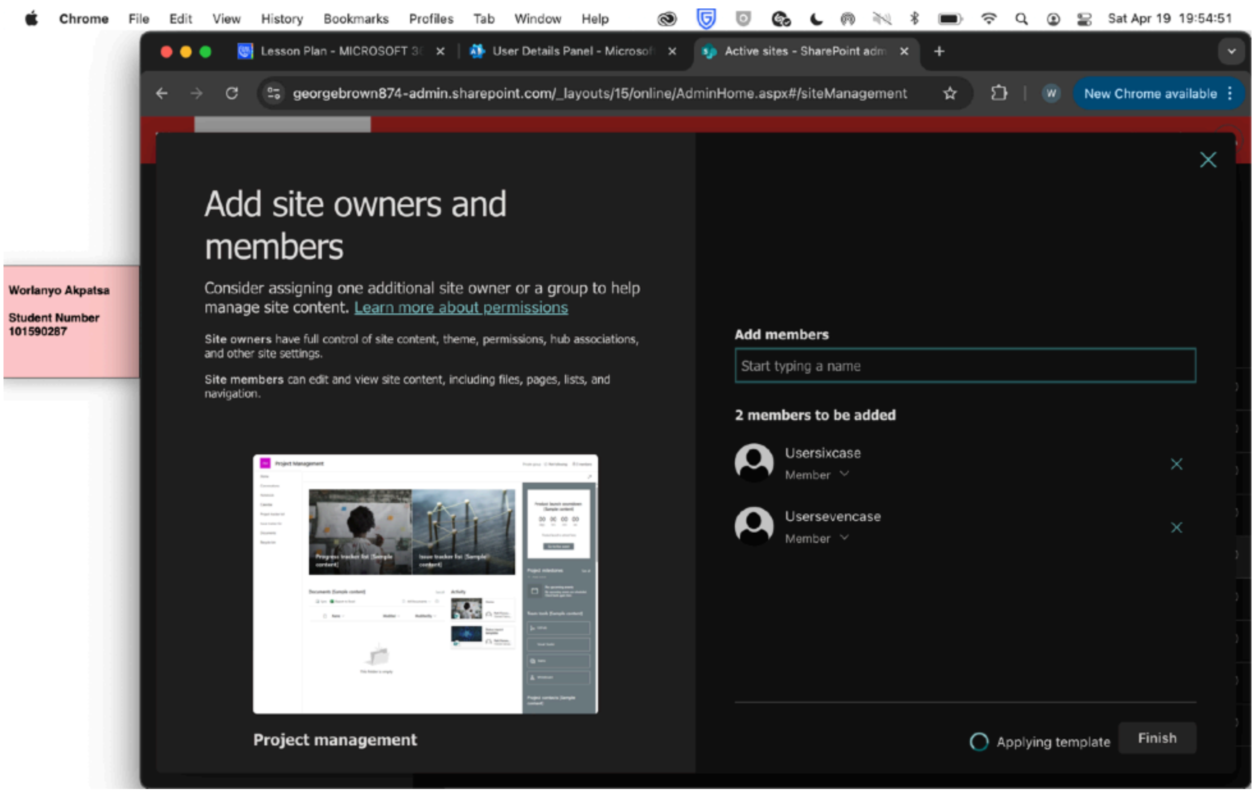
A: Choosing site name, description, and address



B: Setting Privacy Settings, Language and Time Zone

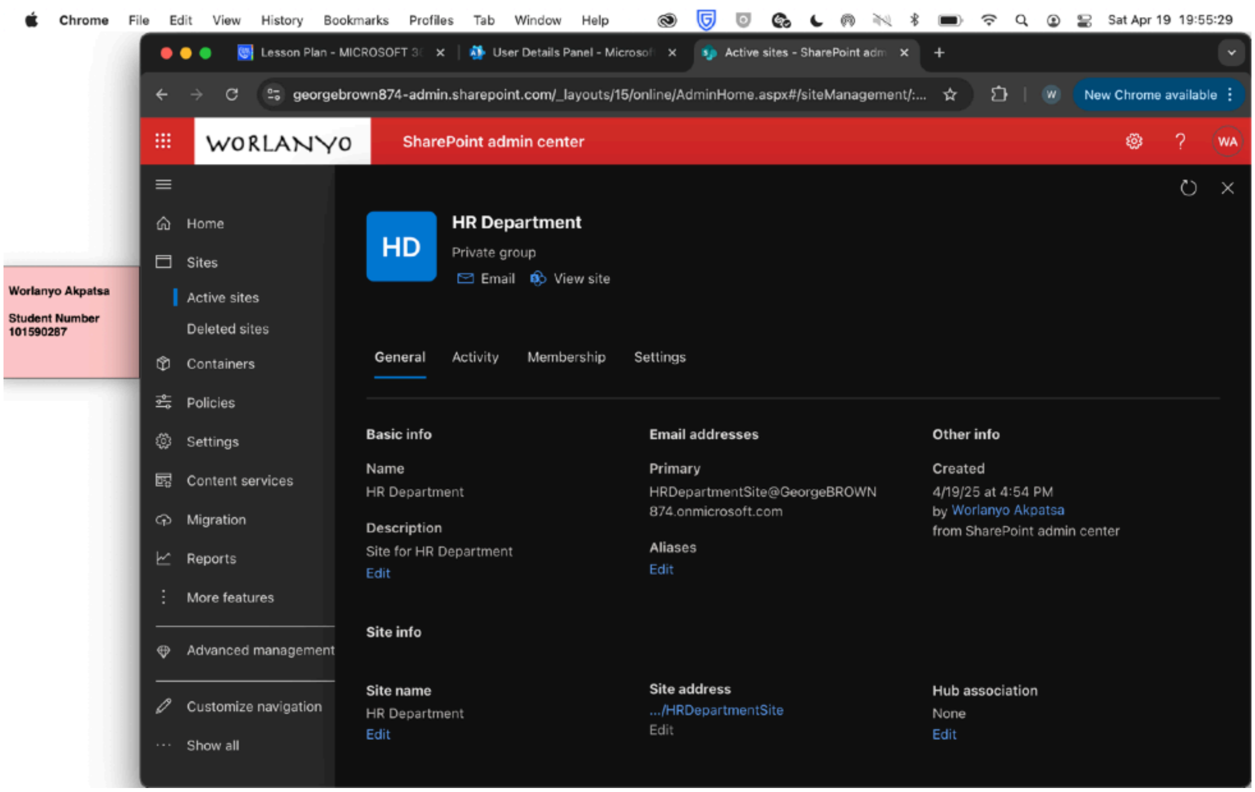


C: Adding members per CSV file



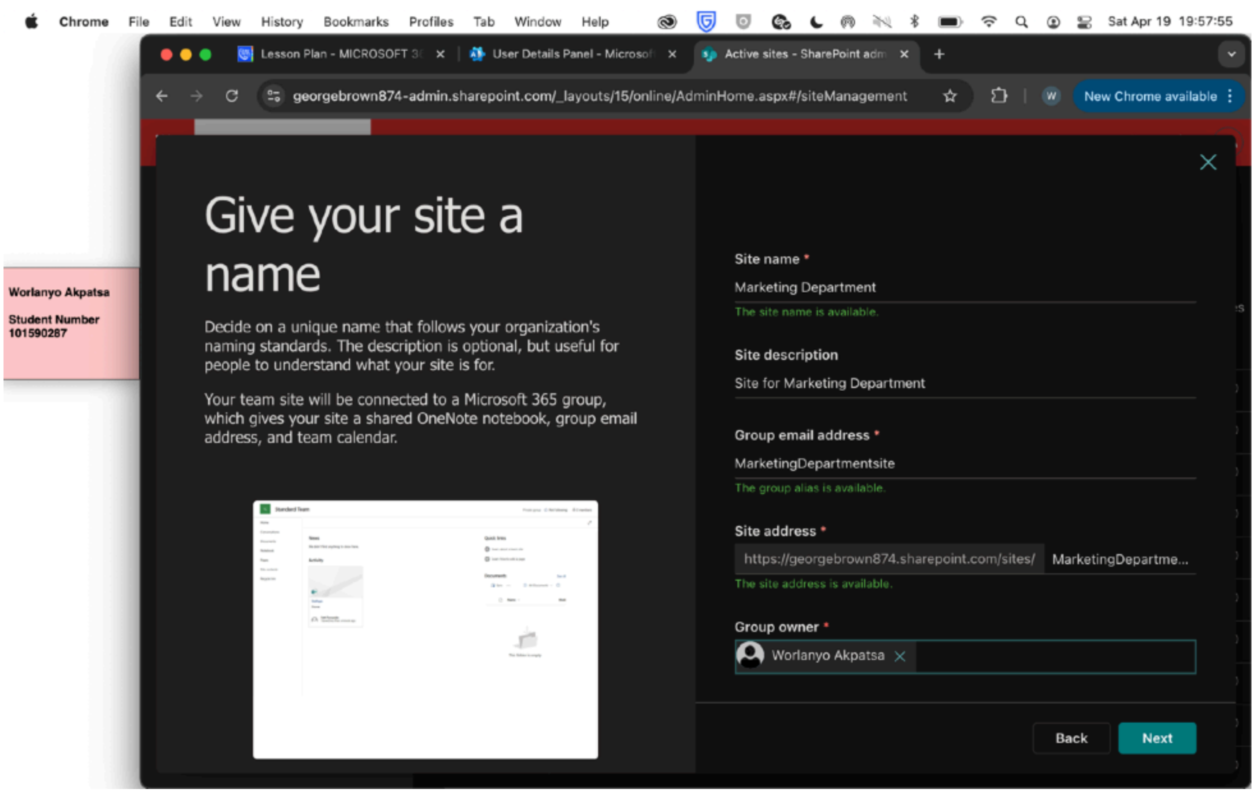
Student Name: Worlanyo Akpatsa Term: Winter 2025
Student ID: 101590287

D: HR Site Created



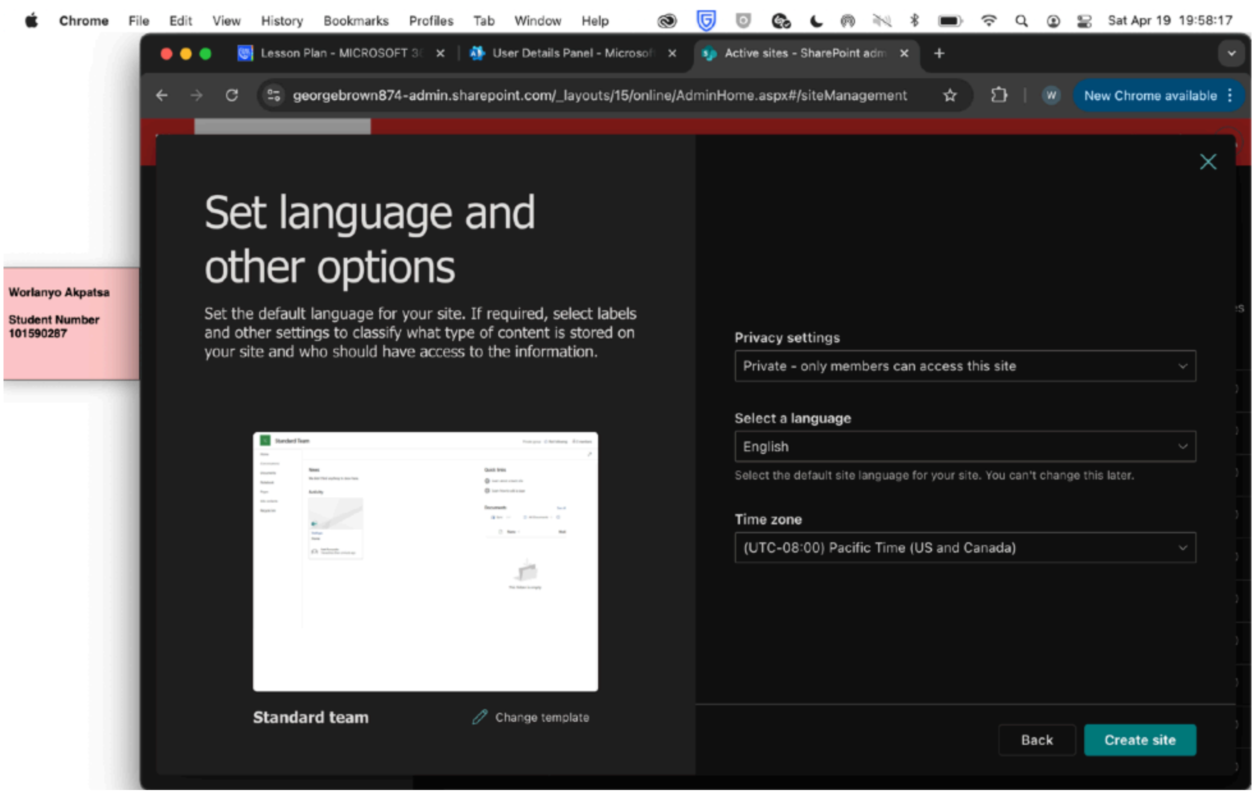
CREATING TEAM SITE FOR MARKETING DEPARTMENT

A: Choosing site name, description, and address



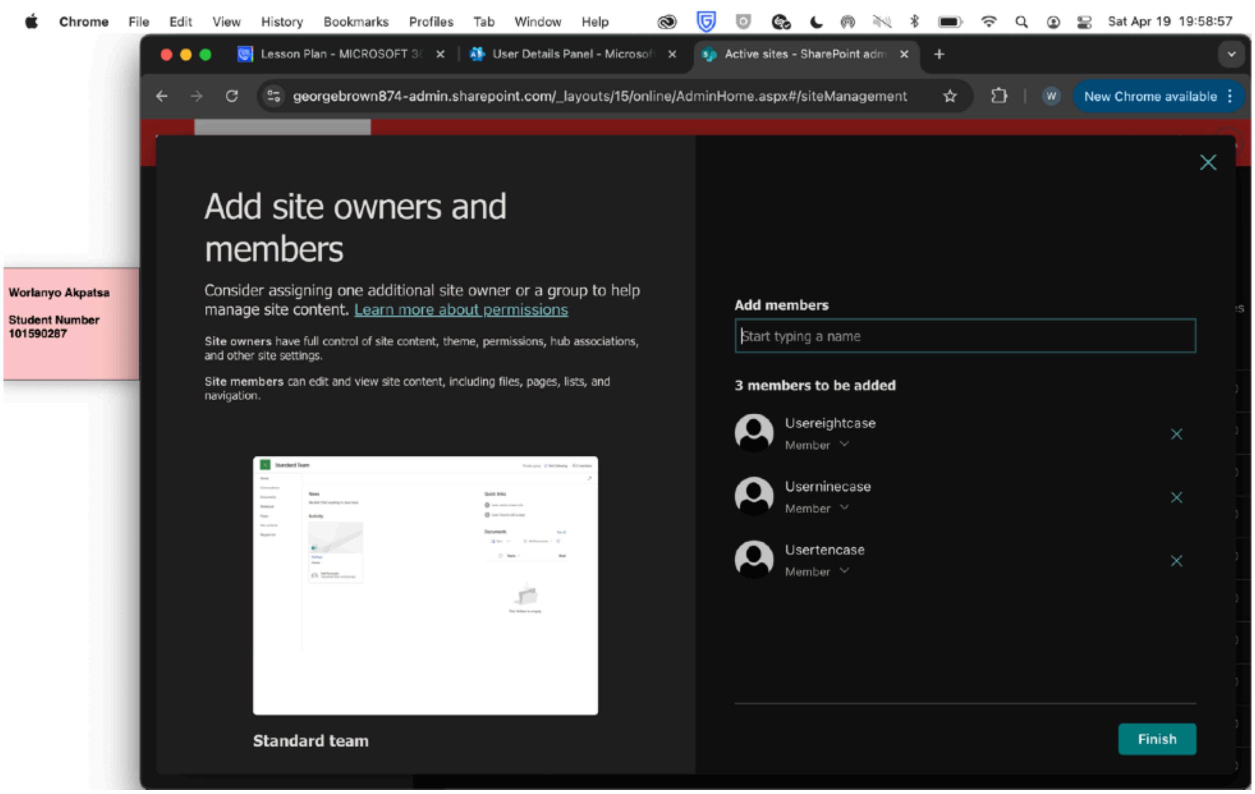
Student Name: Worlanyo Akpatsa
Student ID: 101590287
Term: Winter 2025

B: Setting Privacy Settings, Language and Time Zone



Student Name: Worlanyo Akpatsa
Student ID: 101590287
Term: Winter 2025

C: Adding members per CSV file

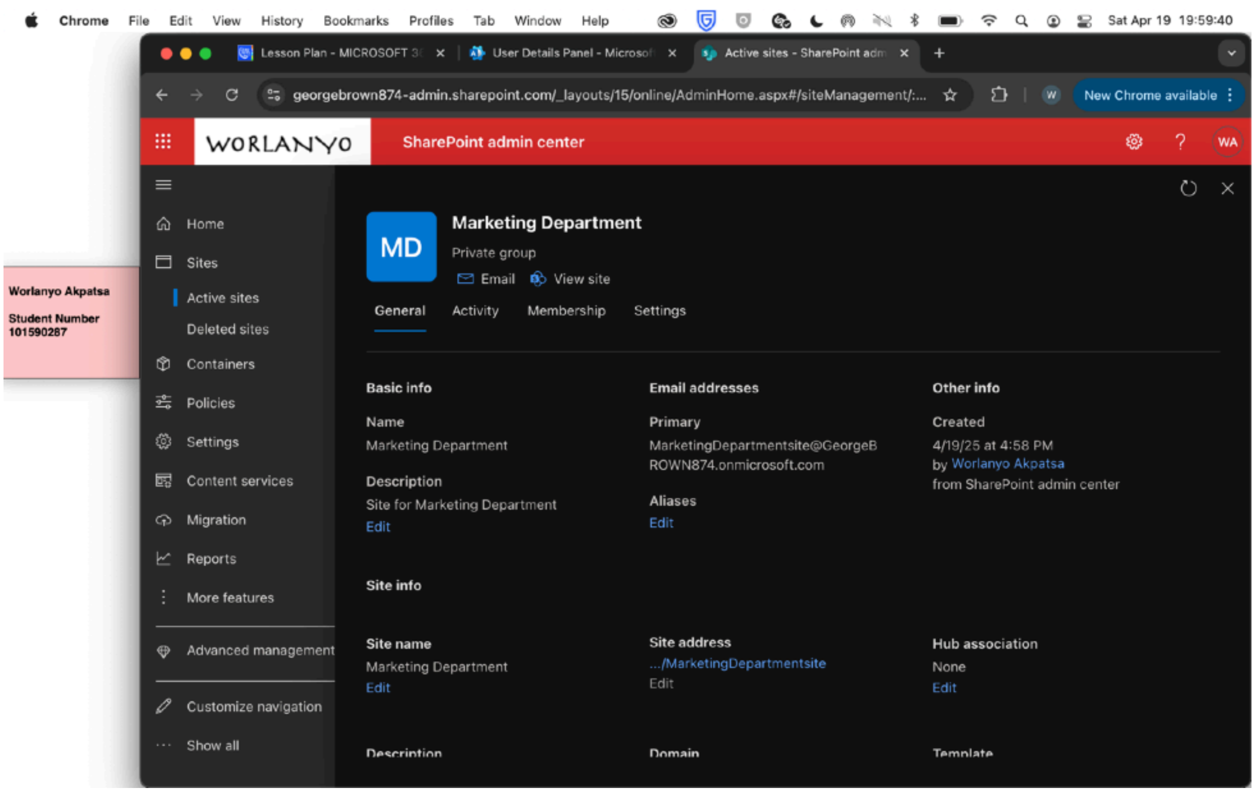


~~~~~~

Student Name: Worlanyo Akpatsa Term: Winter 2025
Student ID: 101590287

~~~~~~

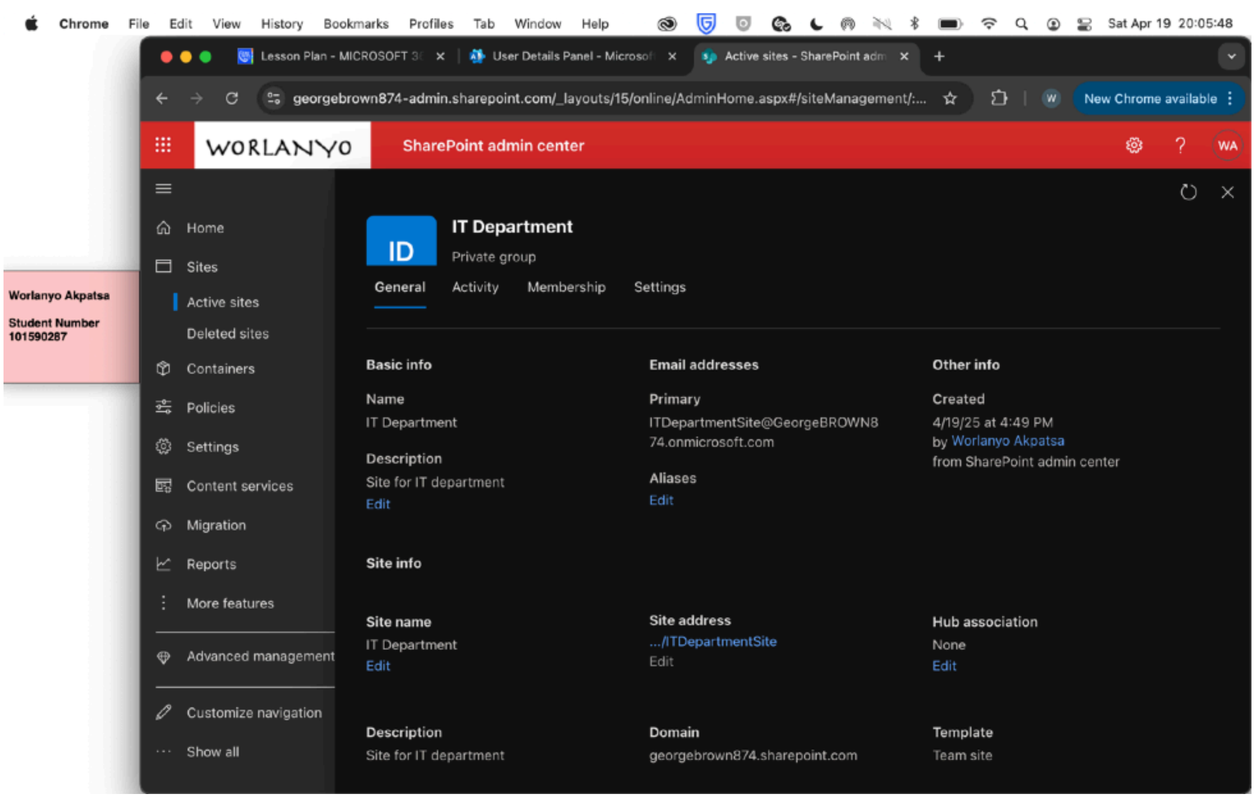
D: Marketing Site Created



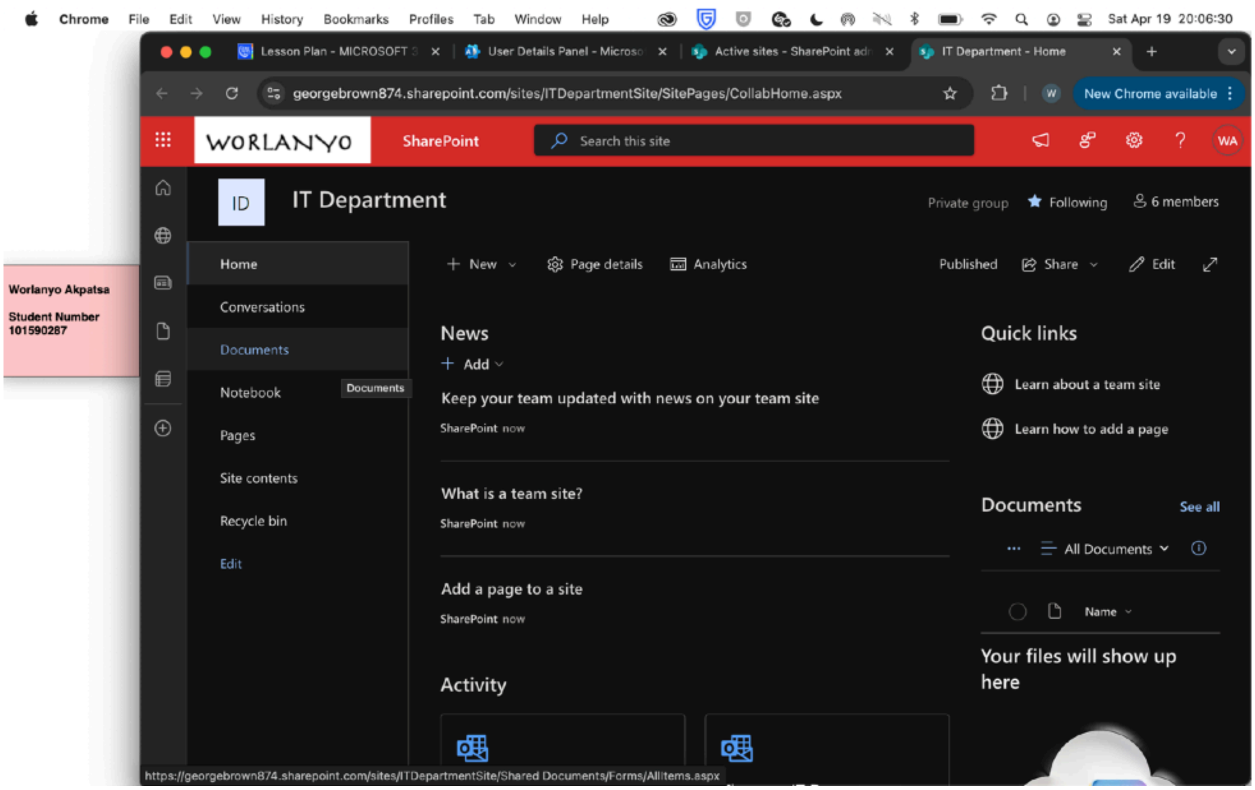
1.2: Configure document libraries and permissions for each site

CONFIGURING DOCUMENT LIBRARIES & PERMISSIONS FOR IT SITE

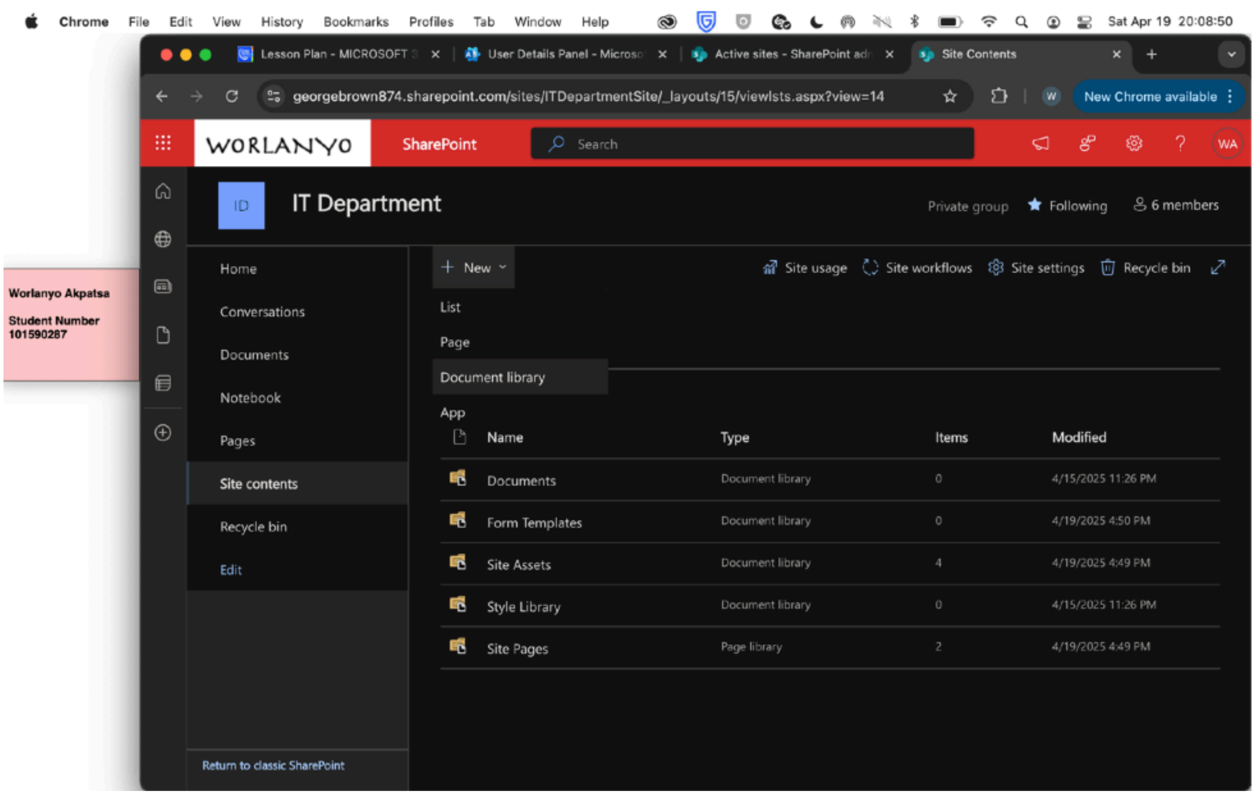
A: Navigate to newly created IT site and click on site link under “site address”



B: Click on Site Contents



C: Click New and select Document Library

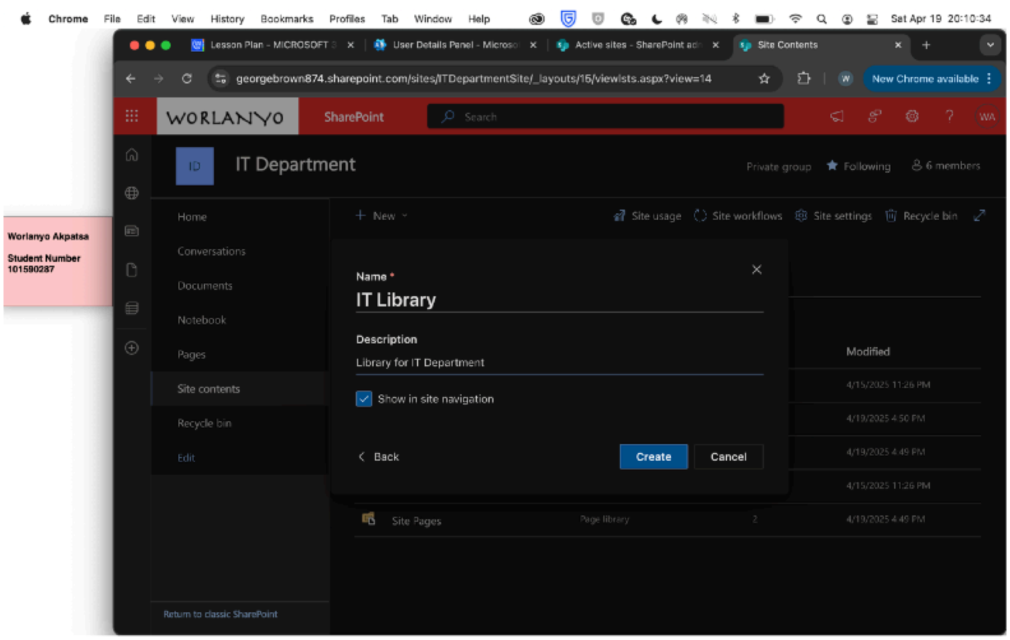


~~~~~~
~~~~

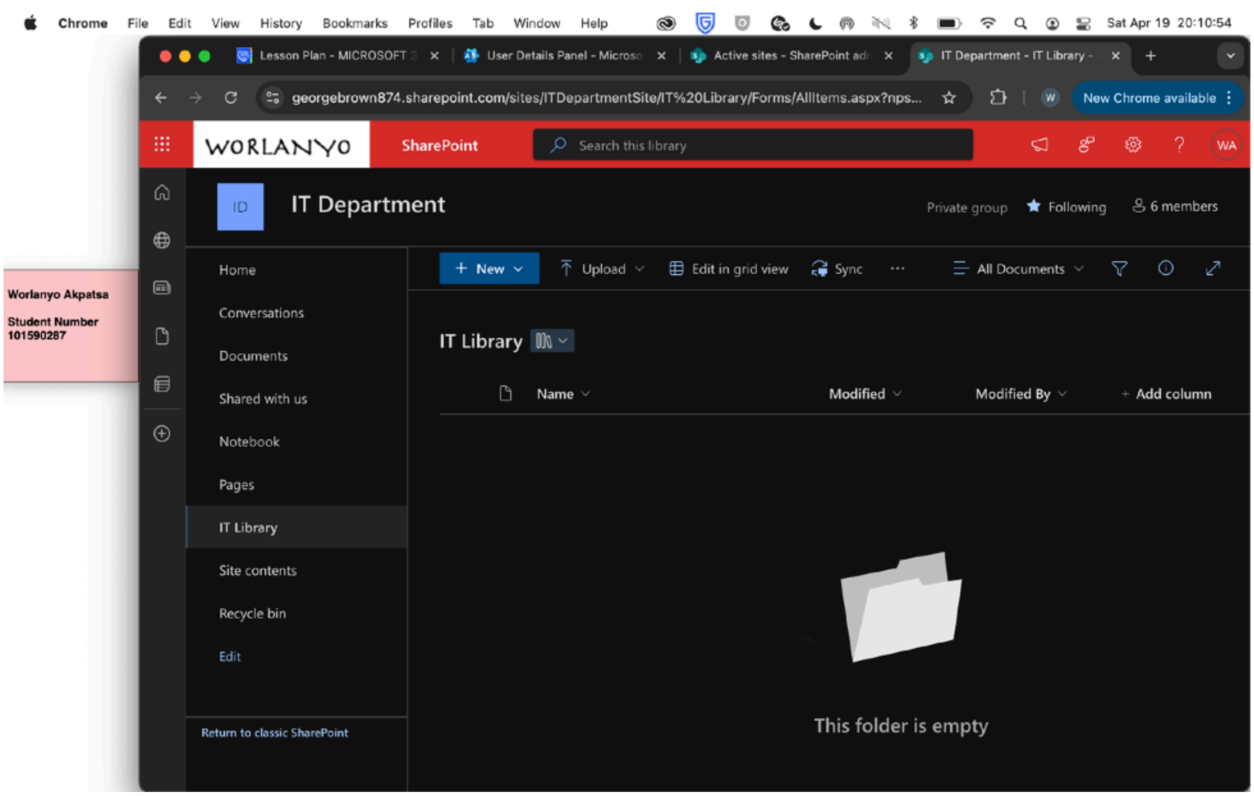
Student Name: Worlanyo Akpatsa | Term: Winter 2025
Student ID: 101590287

~~~~~~
~~~~

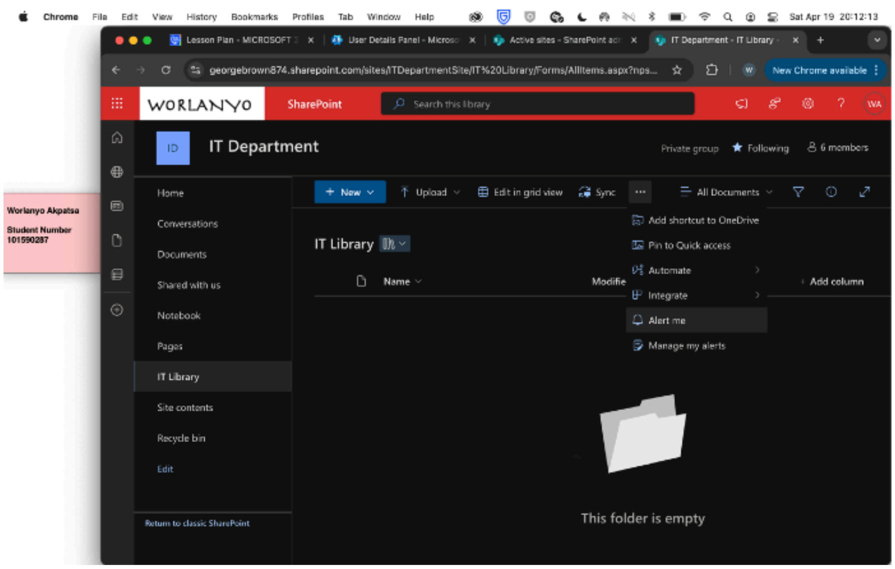
D: Creating Library

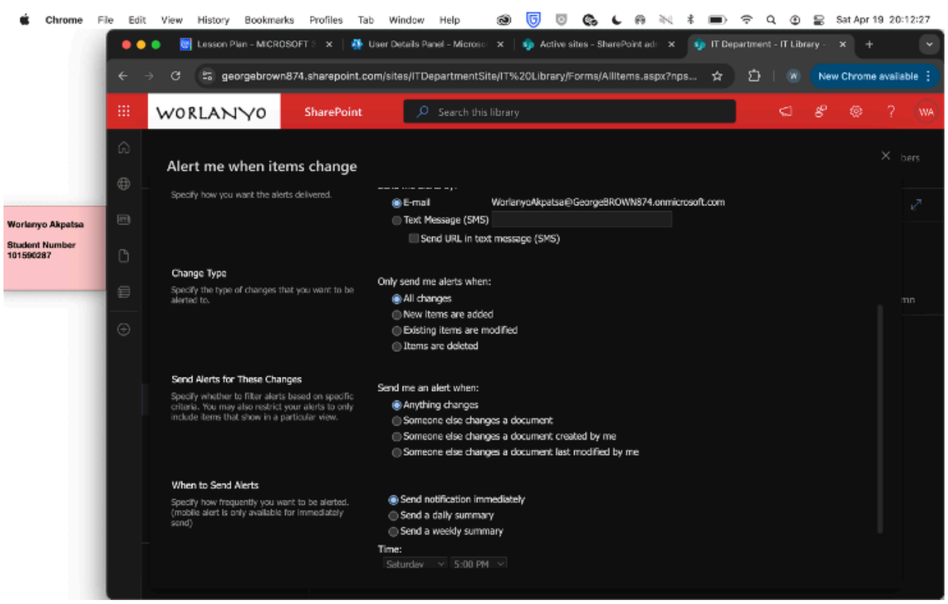


E: Library Created

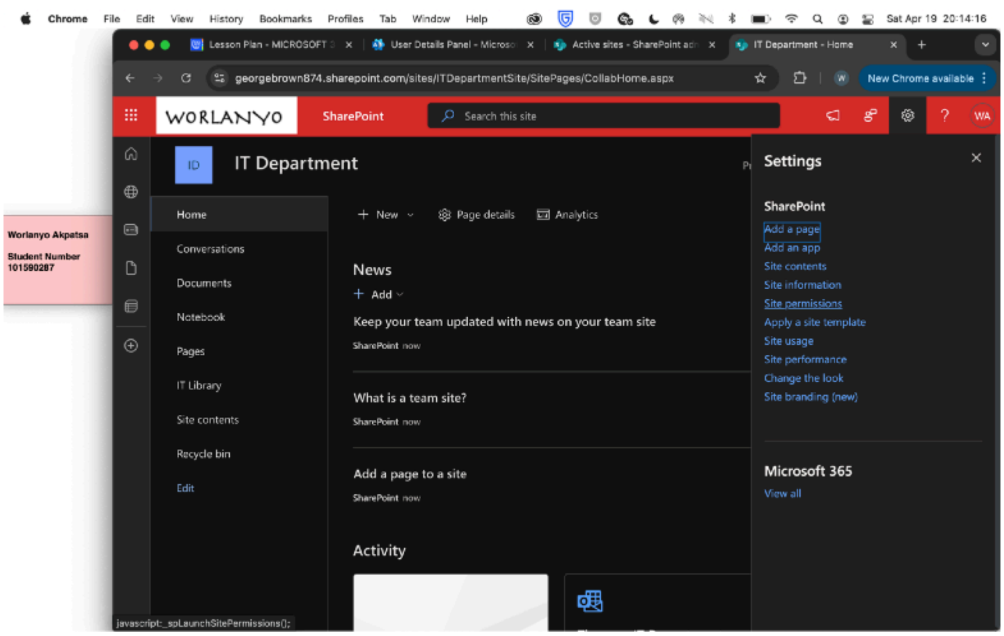


F: Creating Alert for when something changes

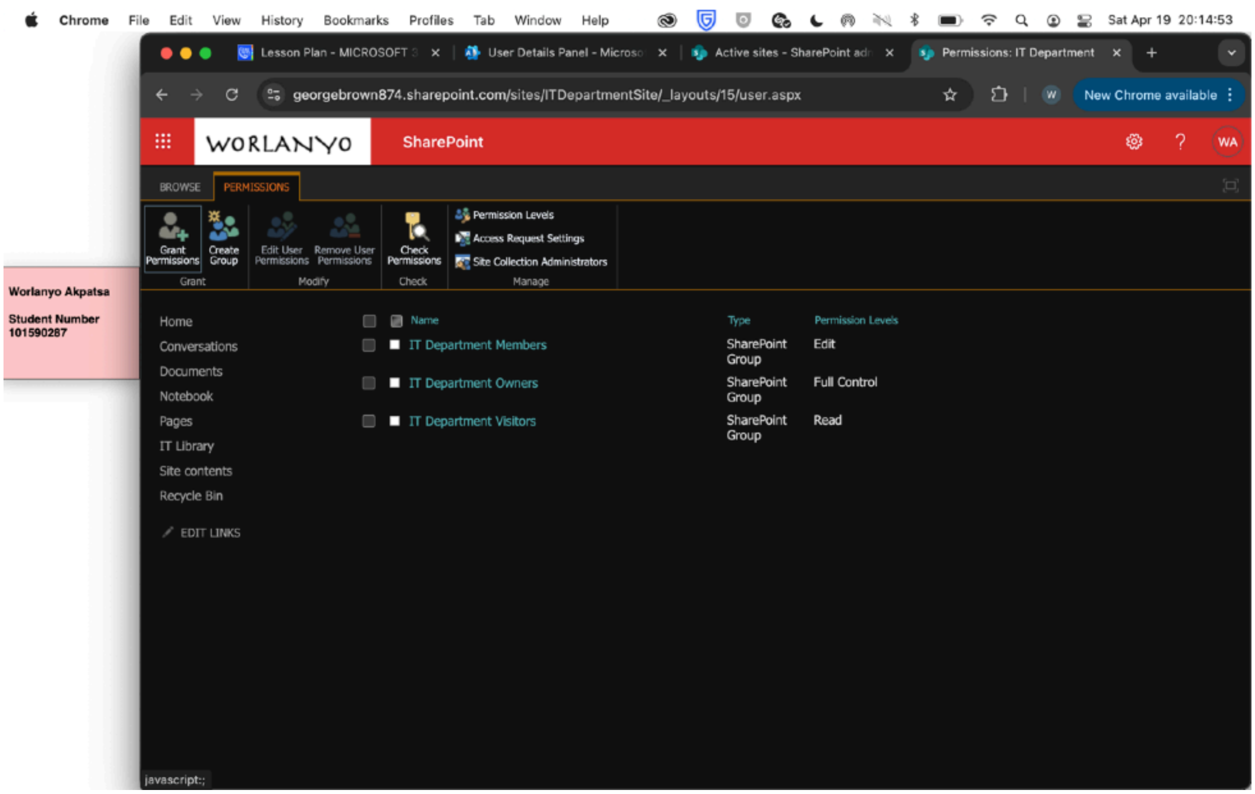




G: Site permissions for IT department. Navigate to settings icon on page and select site permissions->advanced site permissions

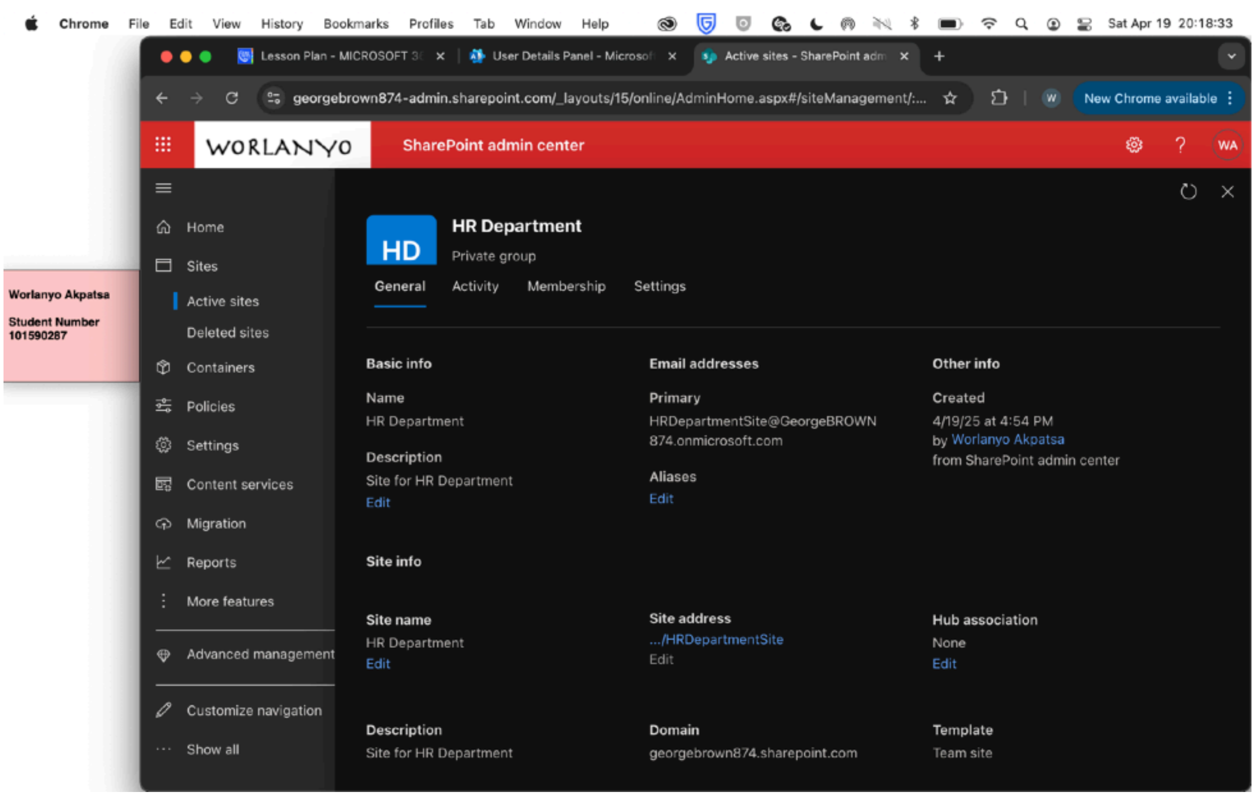


H: Click Grant Permissions to grant permissions



CONFIGURING DOCUMENT LIBRARIES & PERMISSIONS FOR HR SITE

A: Navigate to newly created HR site and click on site link under "site address"

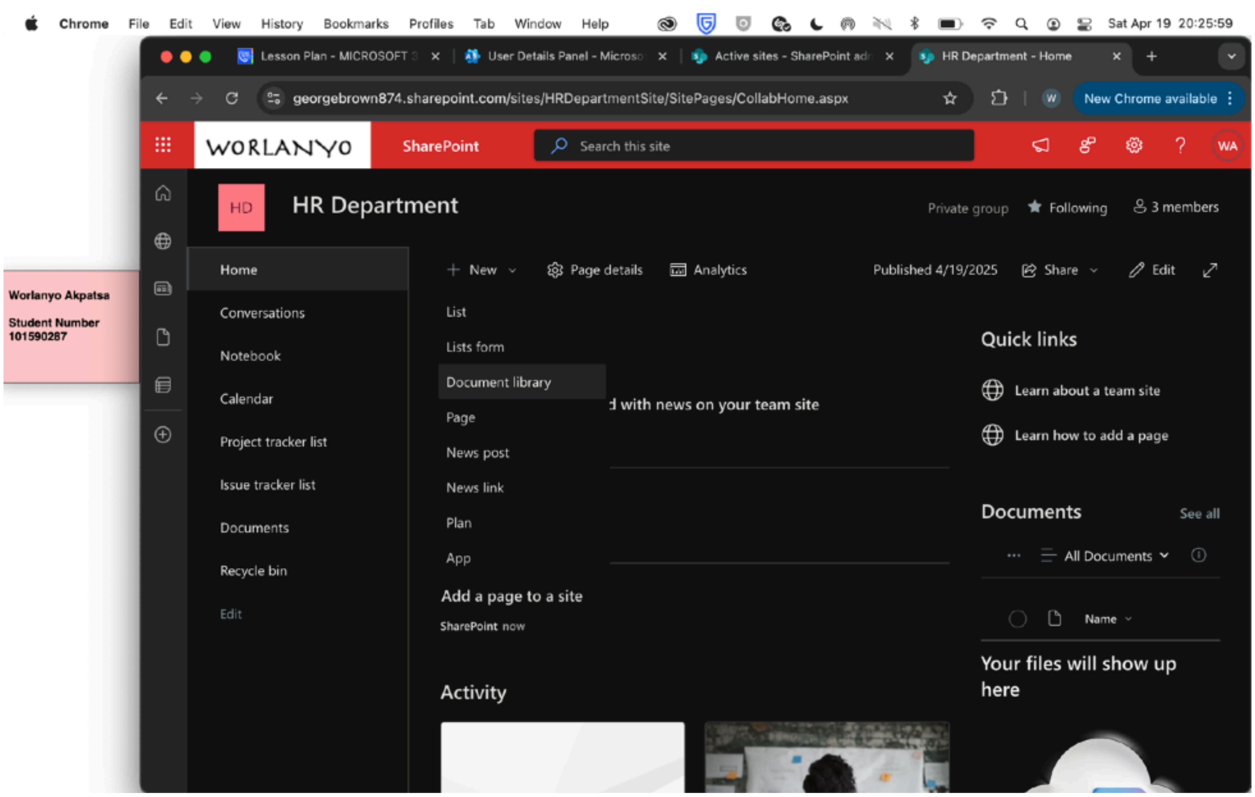


~~~~~~

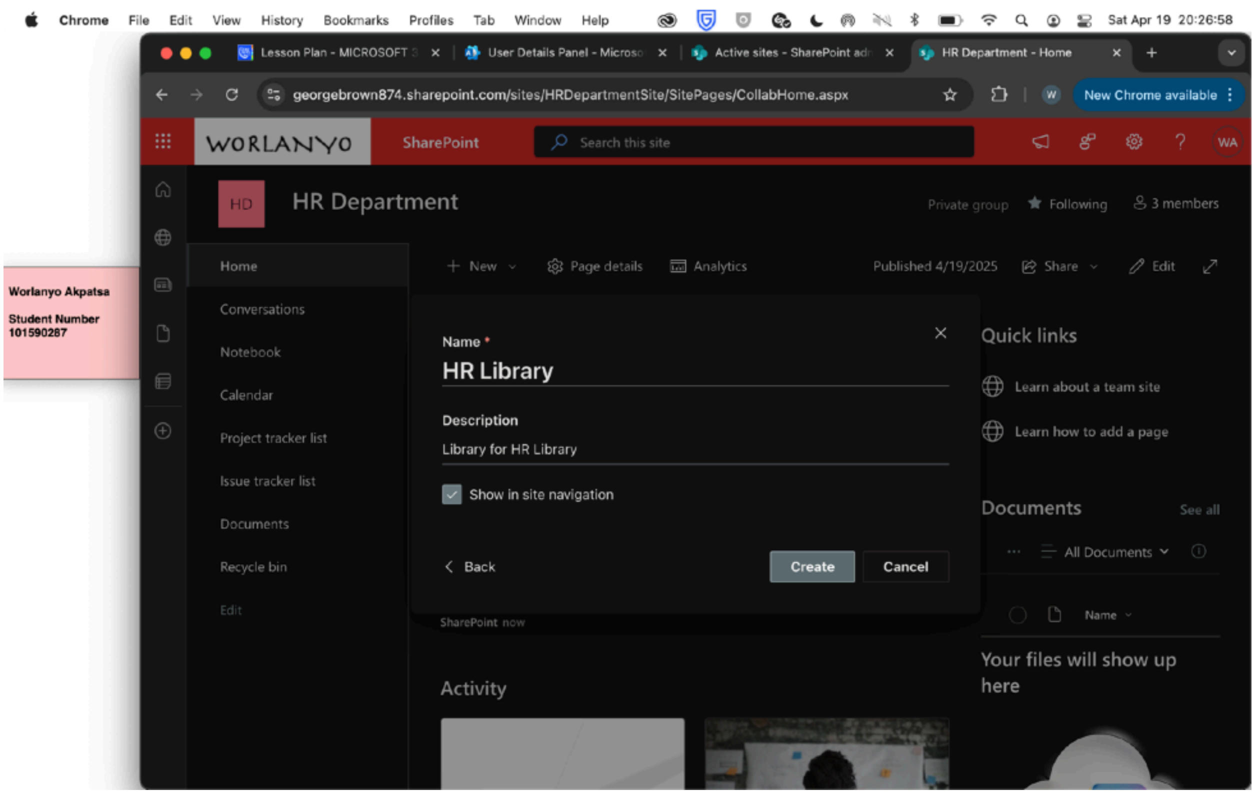
Student Name: Worlanyo Akpatsa Term: Winter 2025
Student ID: 101590287

~~~~~~

B: Click on New and select Document Library



C: Creating Library

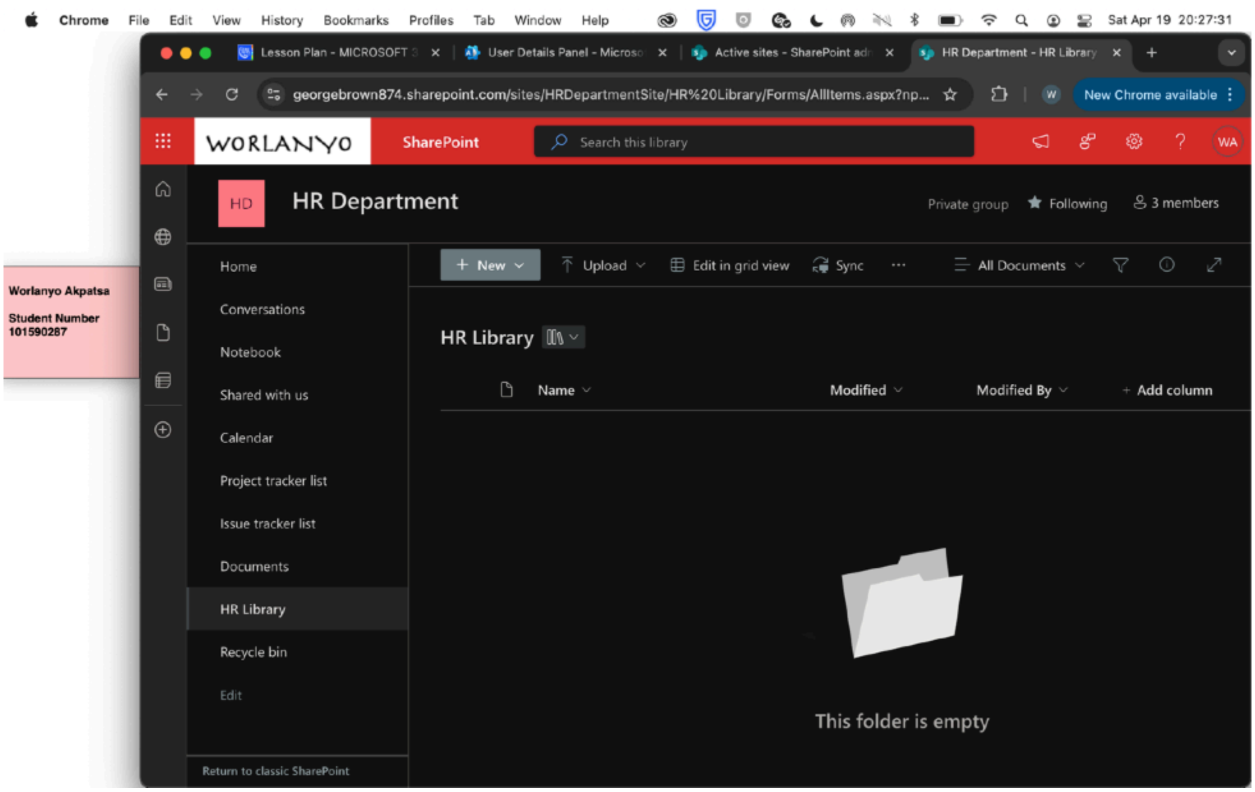


~~~~~~

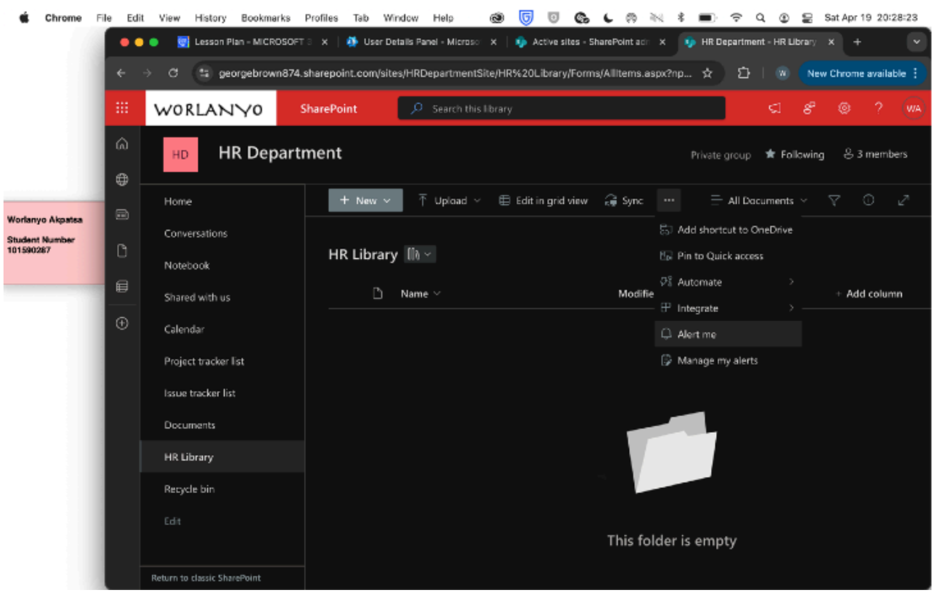
Student Name: Worlanyo Akpatsa Term: Winter 2025
Student ID: 101590287

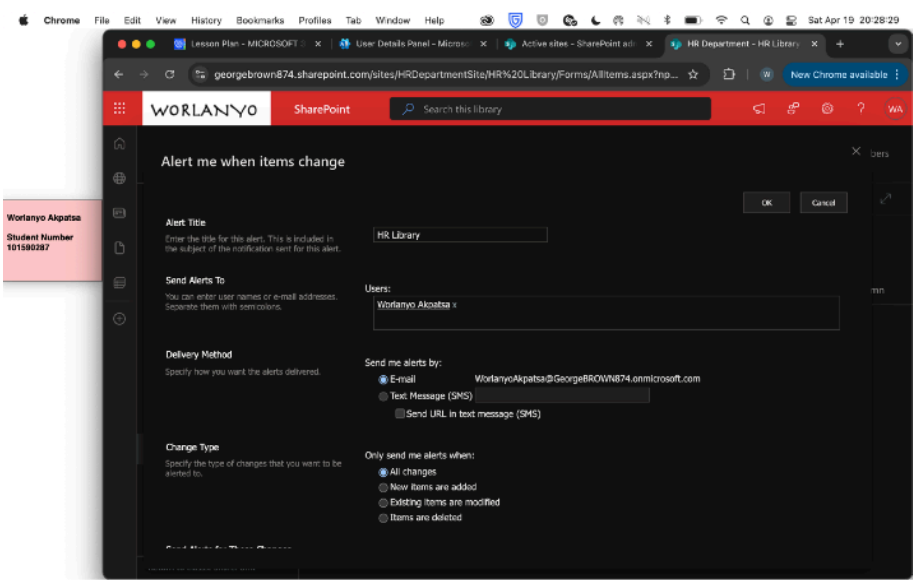
~~~~~~

D: Library Created

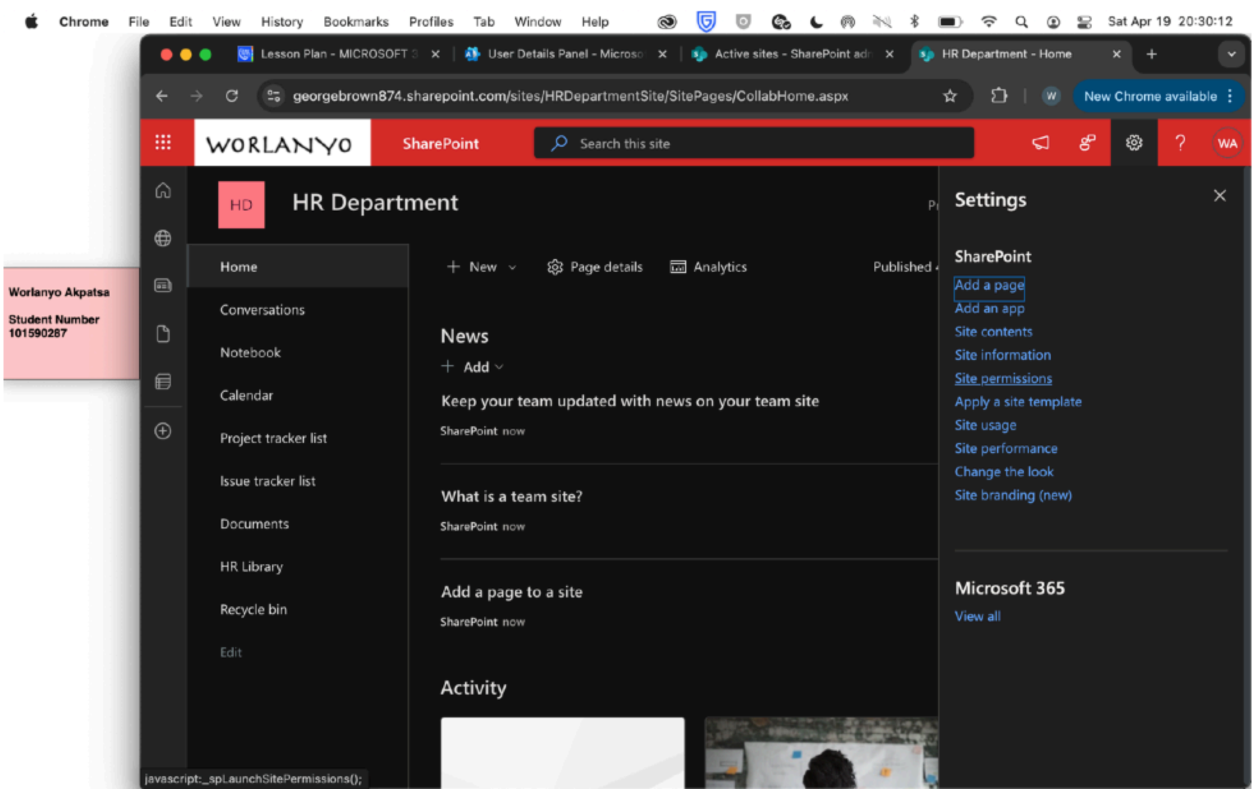


E: Creating Alert for when something changes

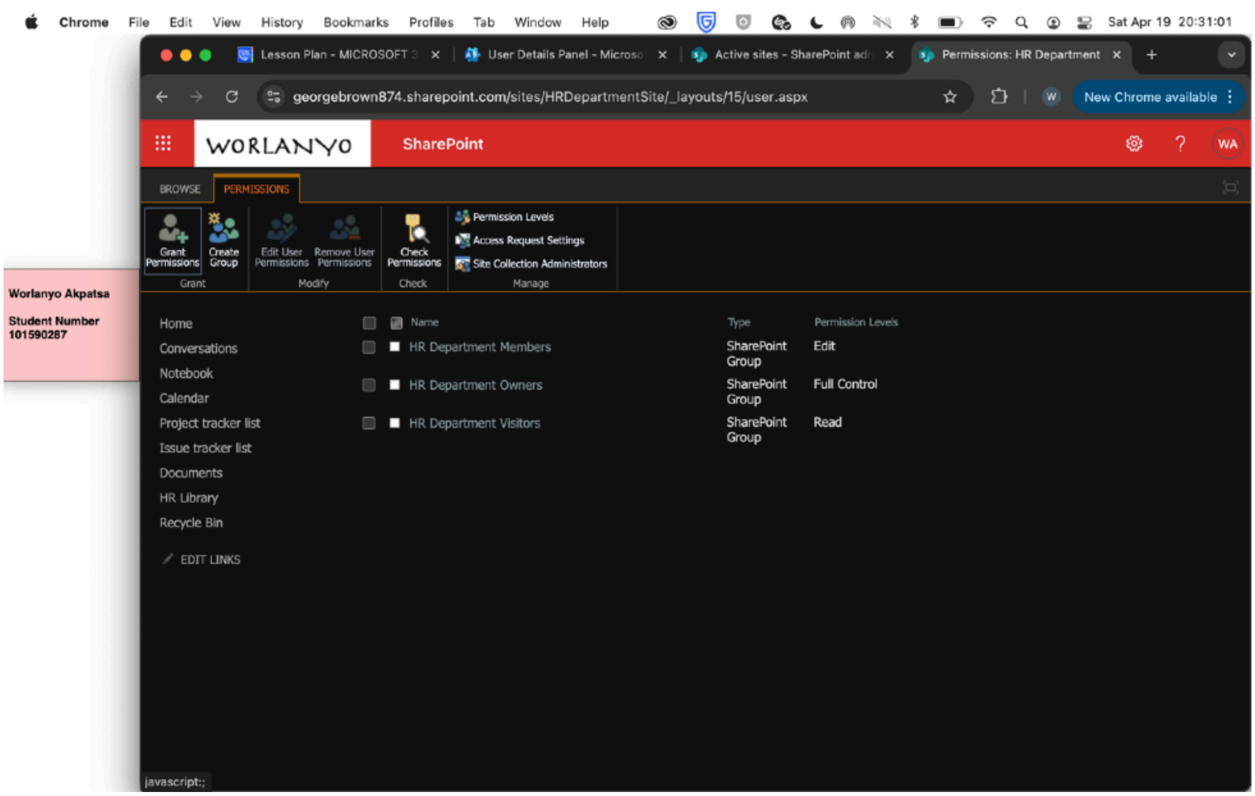




F: Site permissions for HR department. Navigate to settings icon on page and select site permissions->advanced site permissions



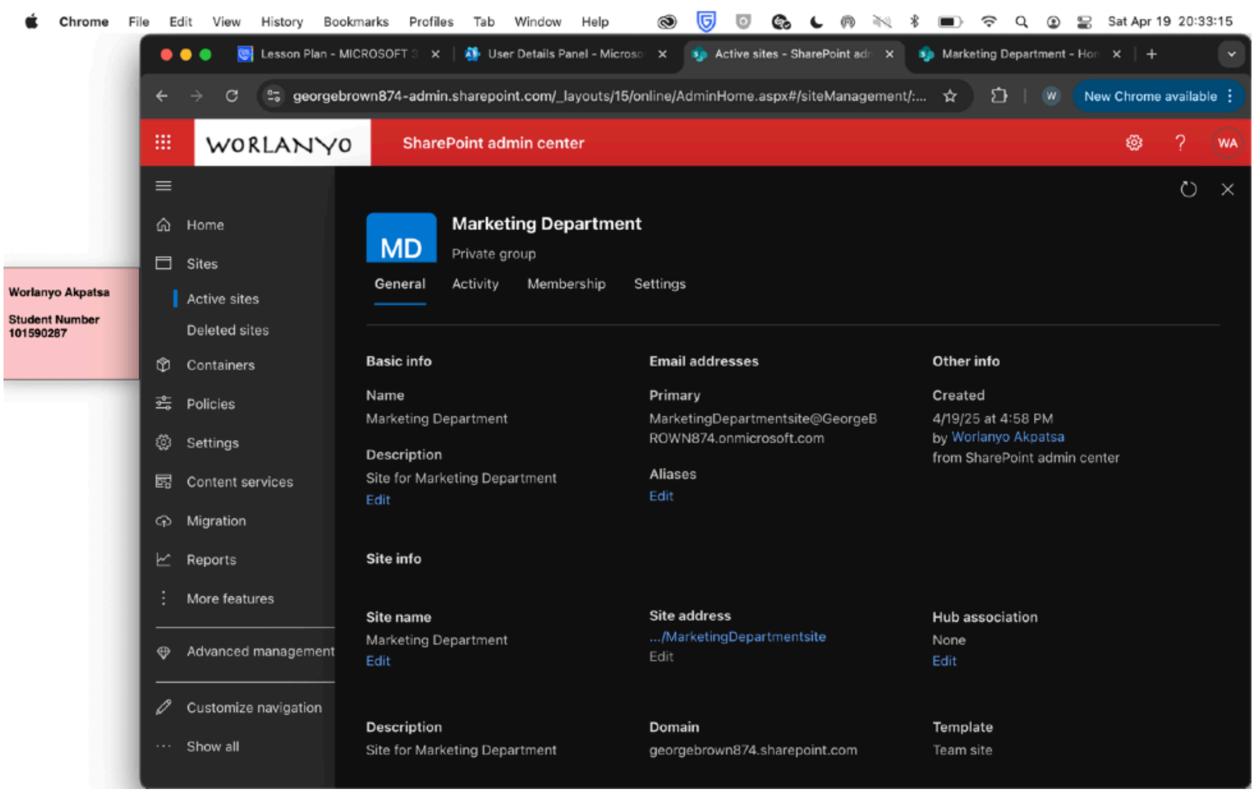
G: Click Grant Permissions to grant permissions



Student Name: Worlanyo Akpatsa
Student ID: 101590287
Term: Winter 2025

CONFIGURING DOCUMENT LIBRARIES & PERMISSIONS FOR MARKETING SITE

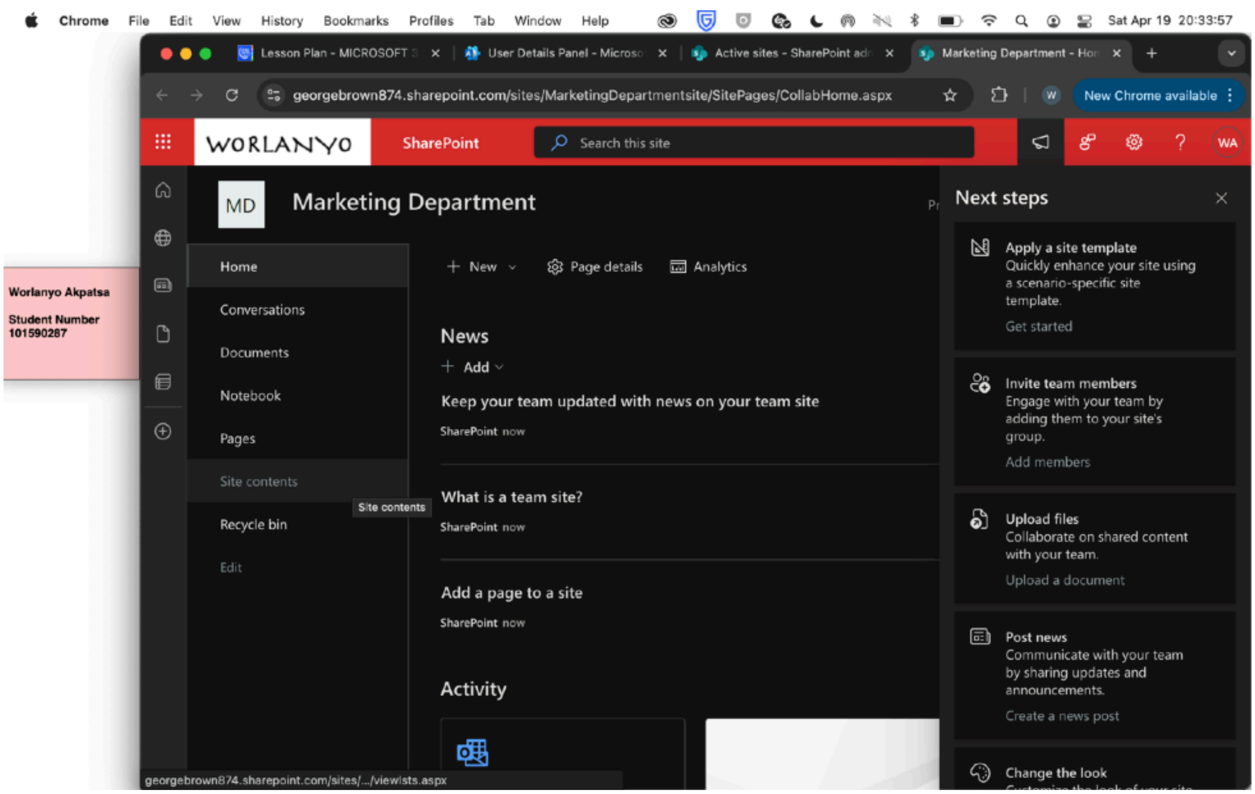
A: Navigate to newly created Marketing site and click on site link under "site address"



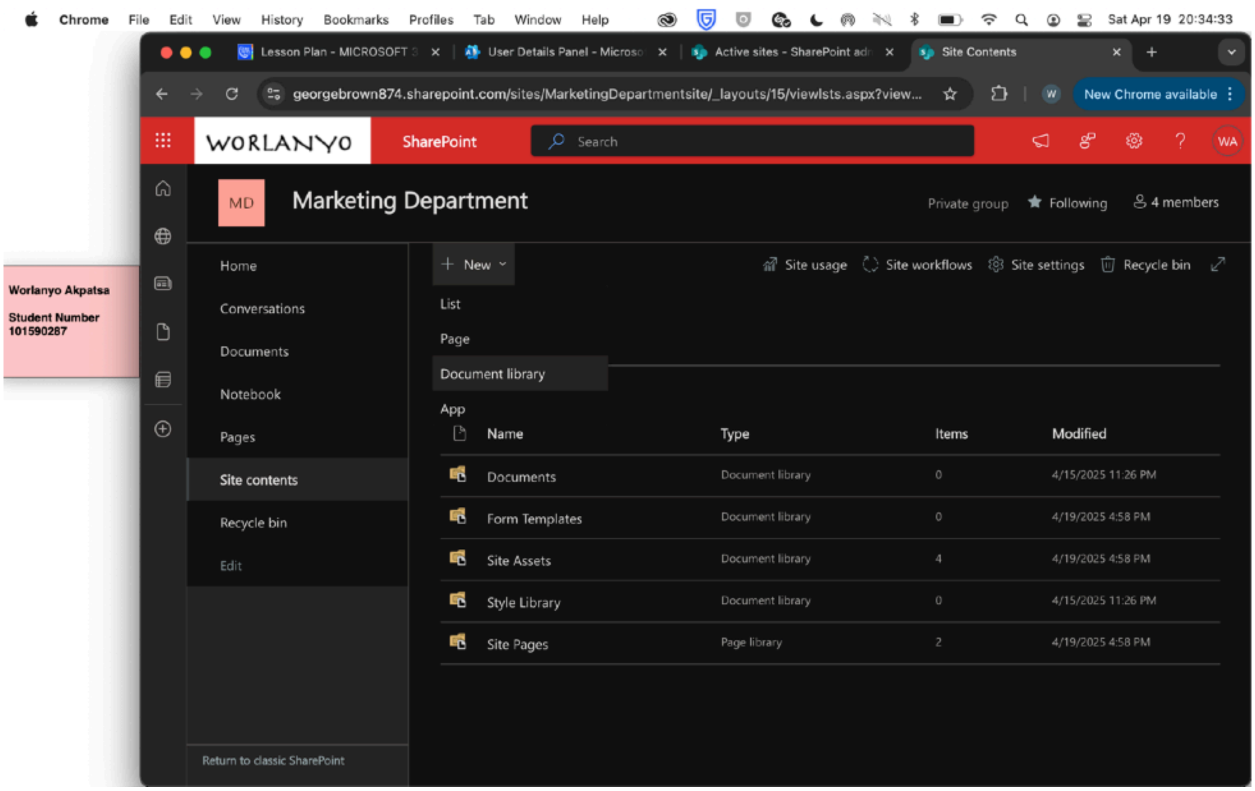
Student Name: Worlanyo Akpatsa | Term: Winter 2025
Student ID: 101590287

~ ~

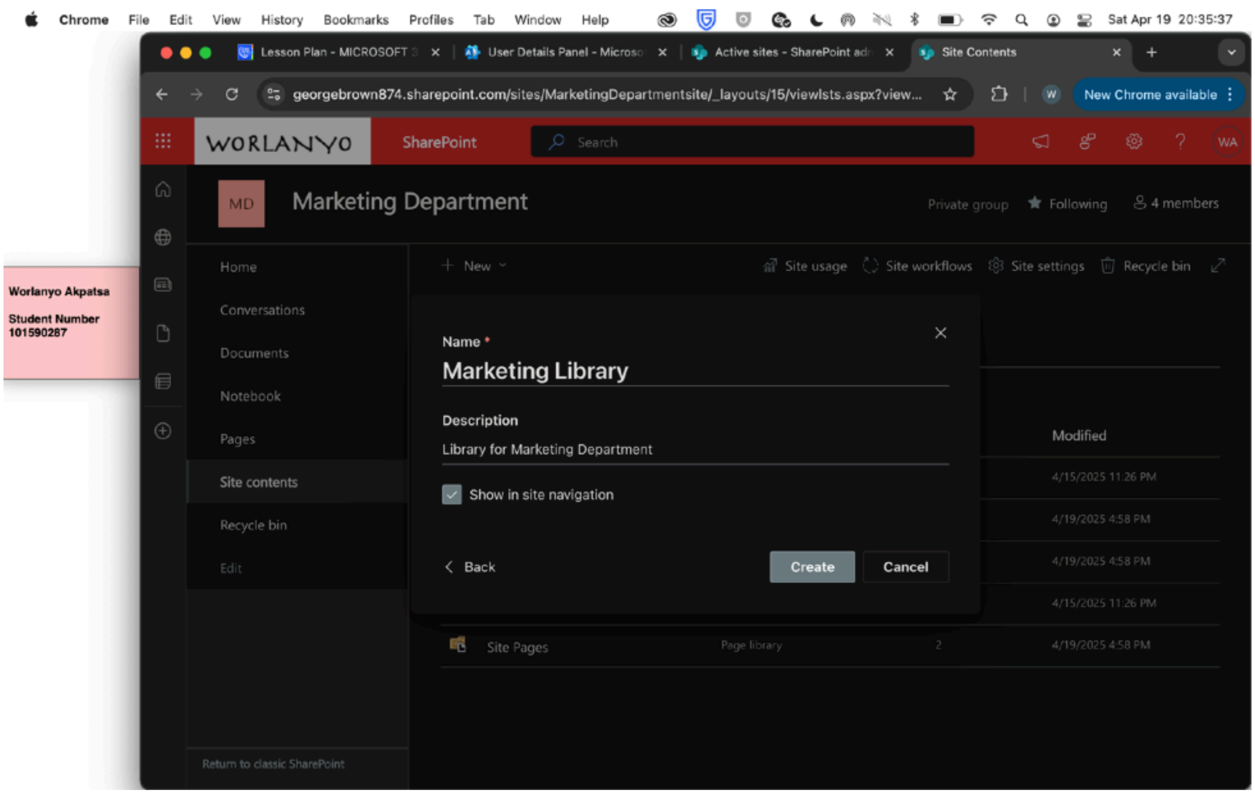
B: Click on Site Contents



C: Click New and select Document Library



D: Creating Library

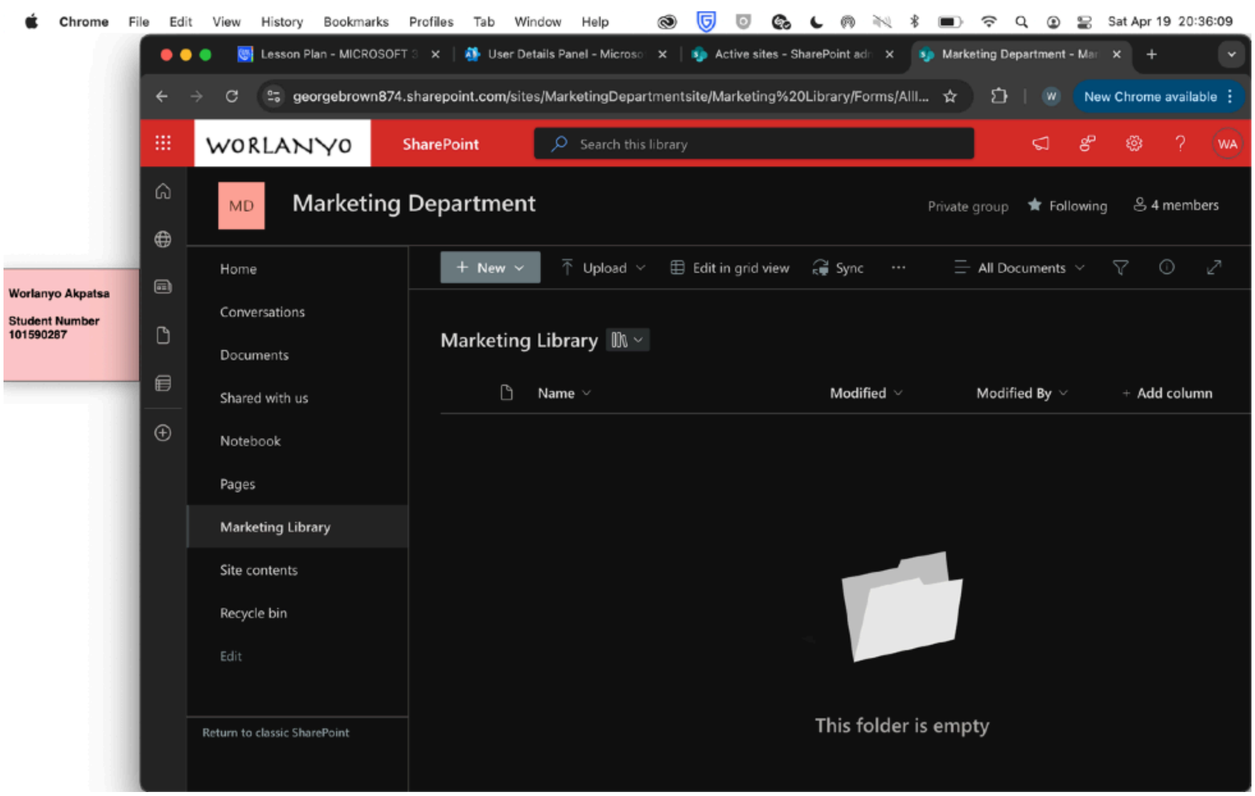


~~~~~~

Student Name: Worlanyo Akpatsa | Term: Winter 2025
Student ID: 101590287

~~~~~~

E: Library Created



~~~~~~

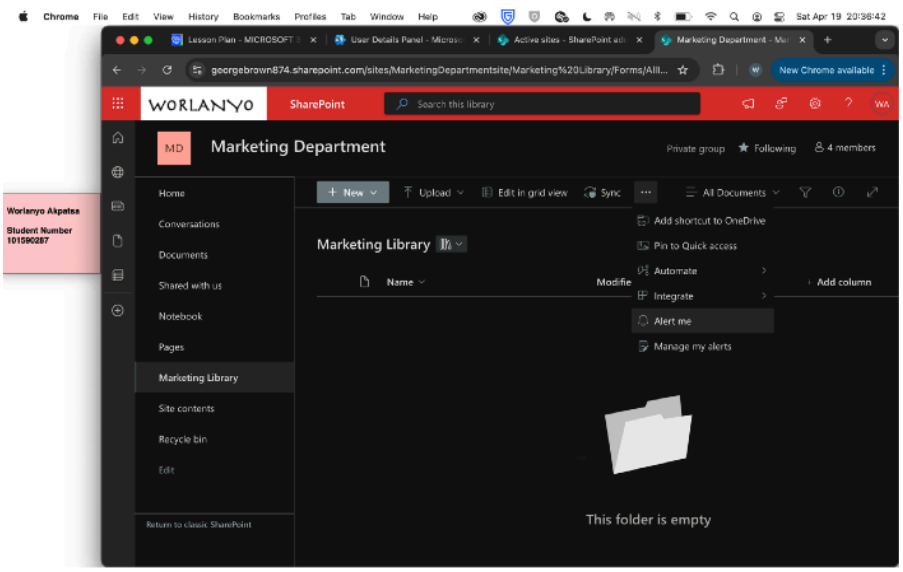
~~~~

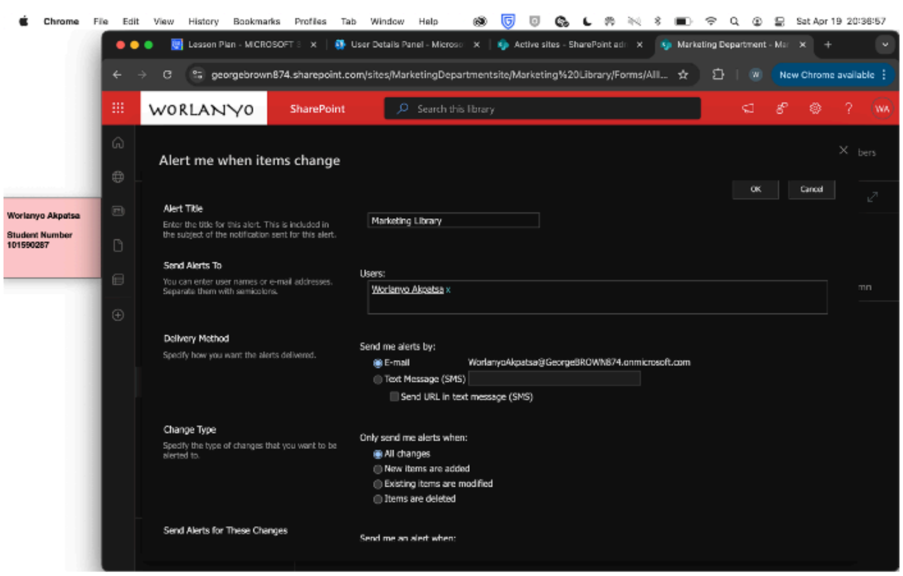
Student Name: Worlanyo Akpatsa Term: Winter 2025
Student ID: 101590287

~~~~~~

~~~~

F: Creating Alert for when something changes





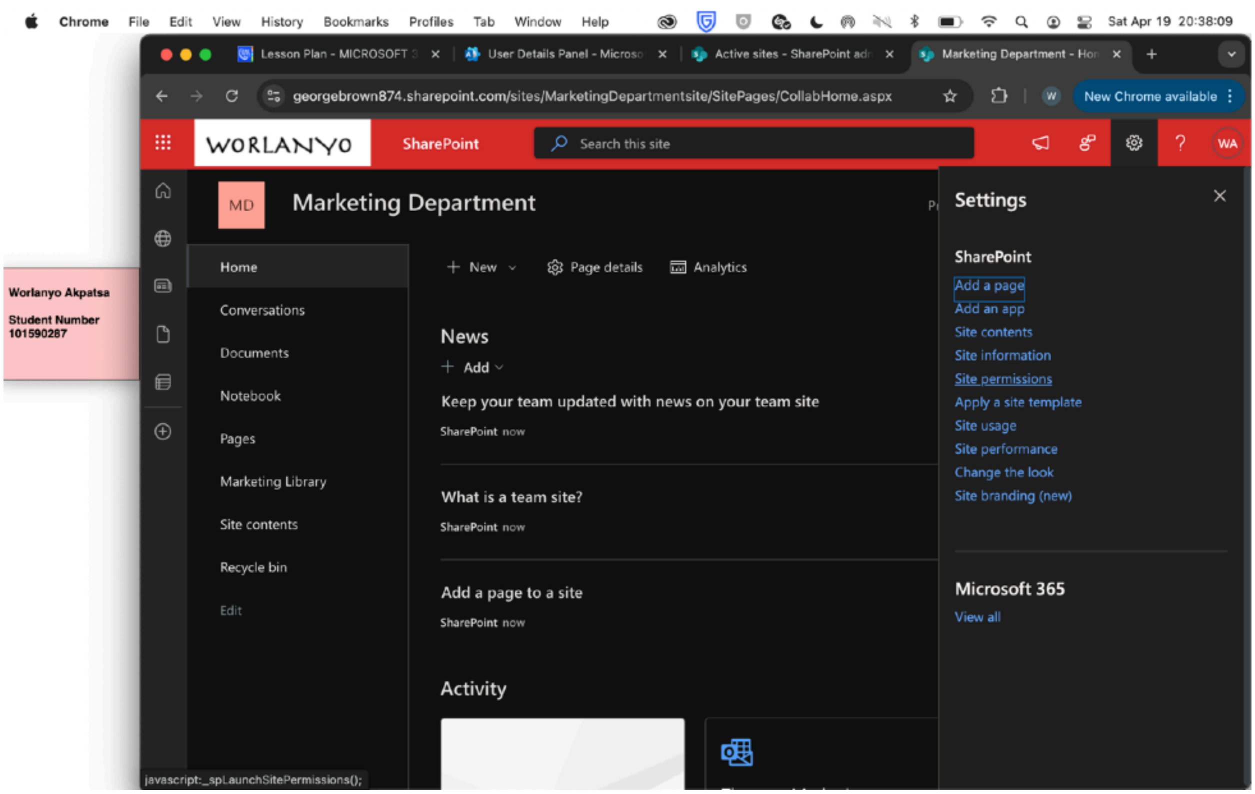
~~~~~~

Student Name: Worlanyo Akpatsa
Student ID: 101590287

Term: Winter 2025

~~~~~~

G: Site permissions for Marketing department. Navigate to settings icon on page and select site permissions->advanced site permissions

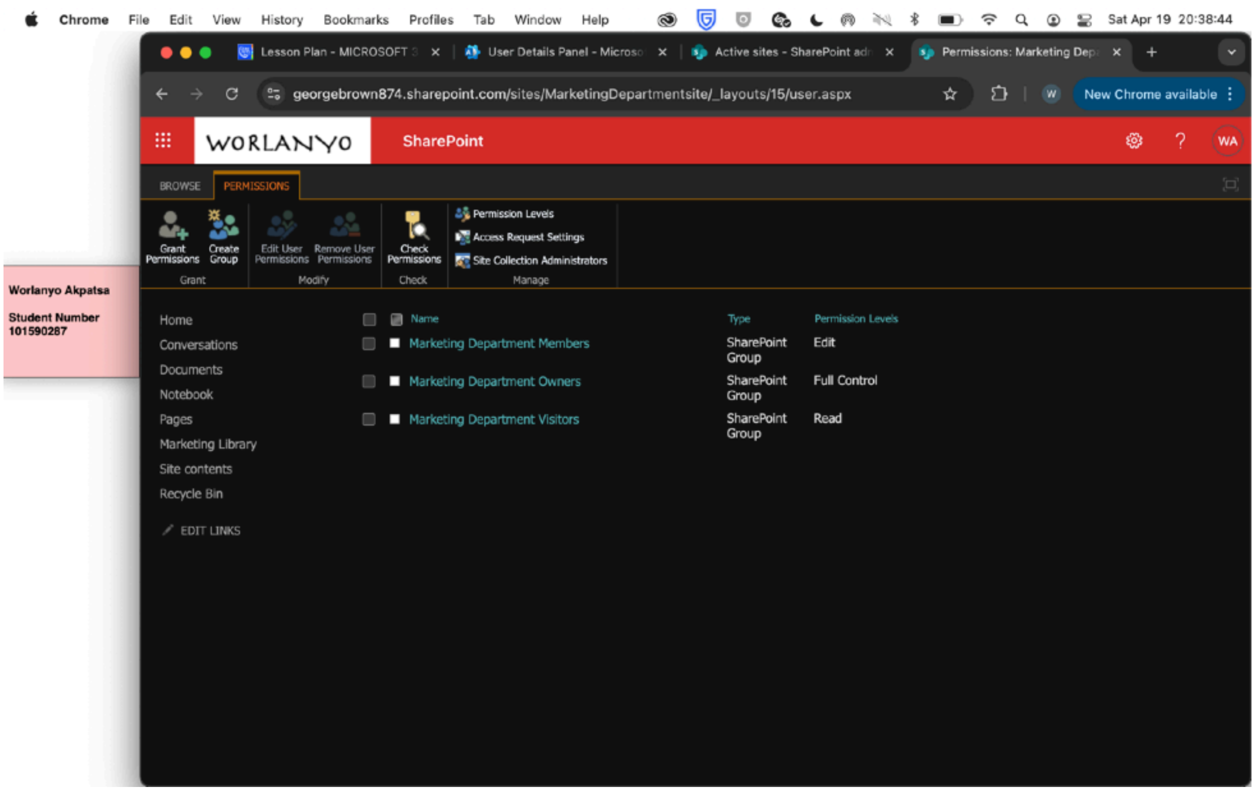


~~~~~~

Student Name: Worlanyo Akpatsa Term: Winter 2025
Student ID: 101590287

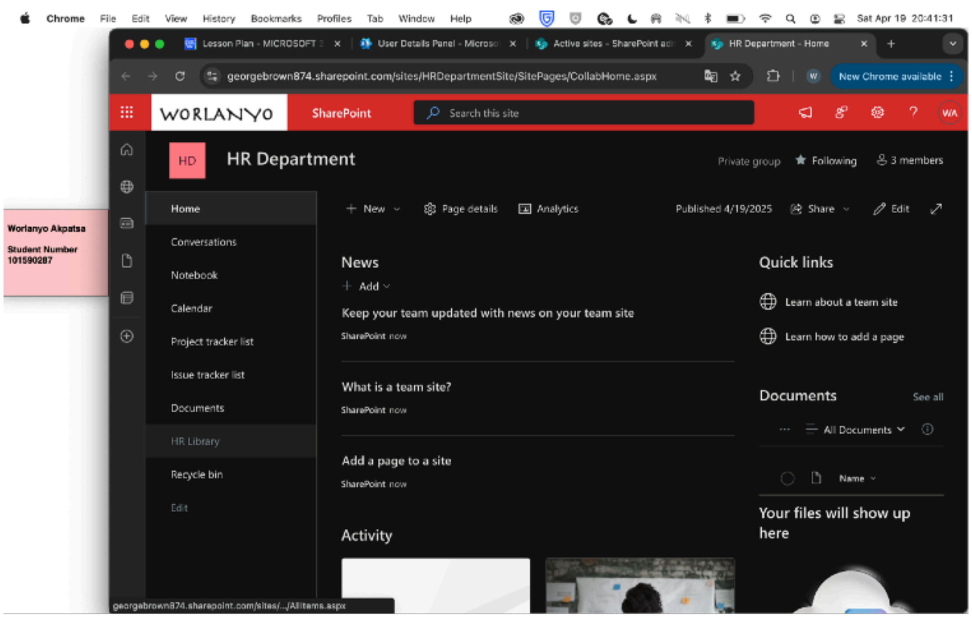
~~~~~~

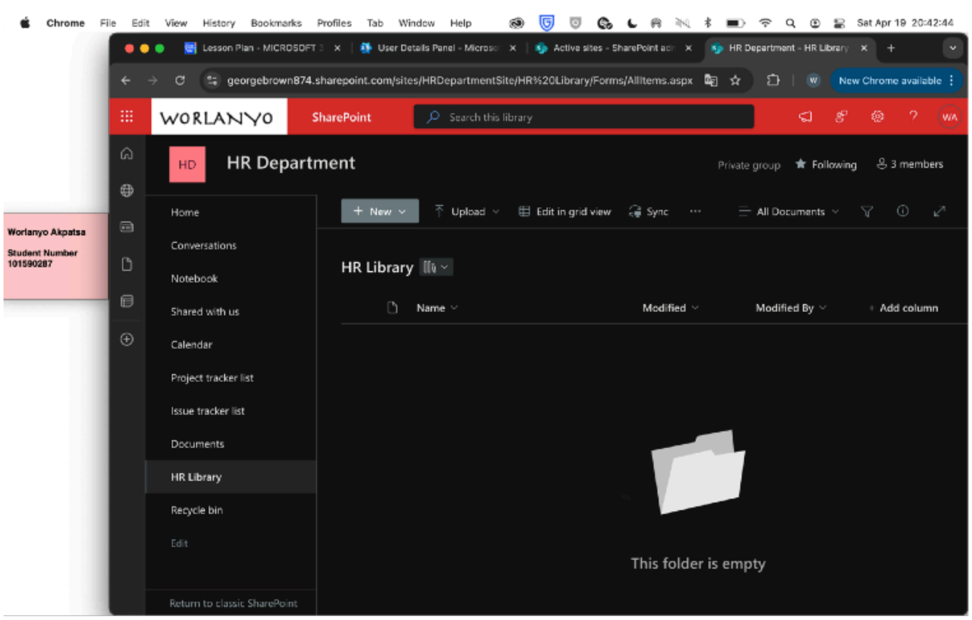
H: Click Grant Permissions to grant permissions



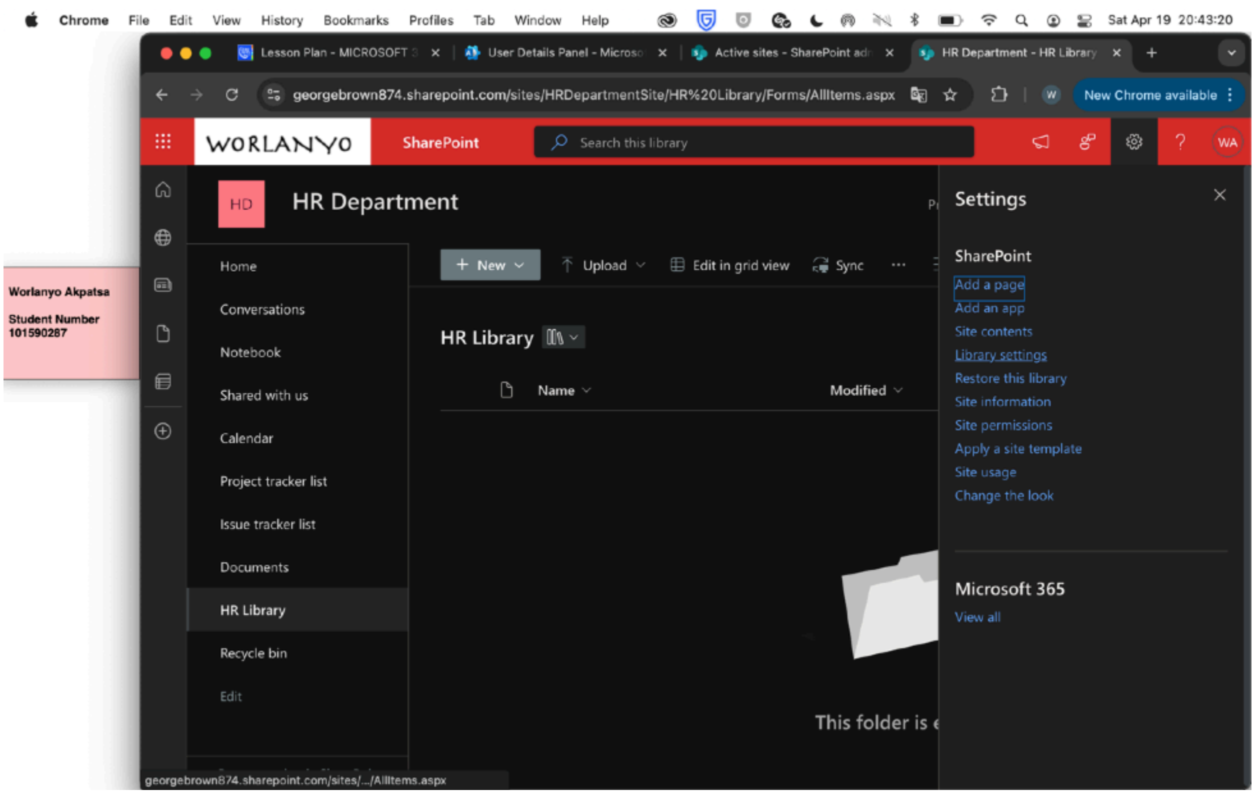
1.3: Enable versioning and content approval for the HR document library

A: Navigate to HR site and open HR library in left pane





B: Select settings icon->library settings->more library settings

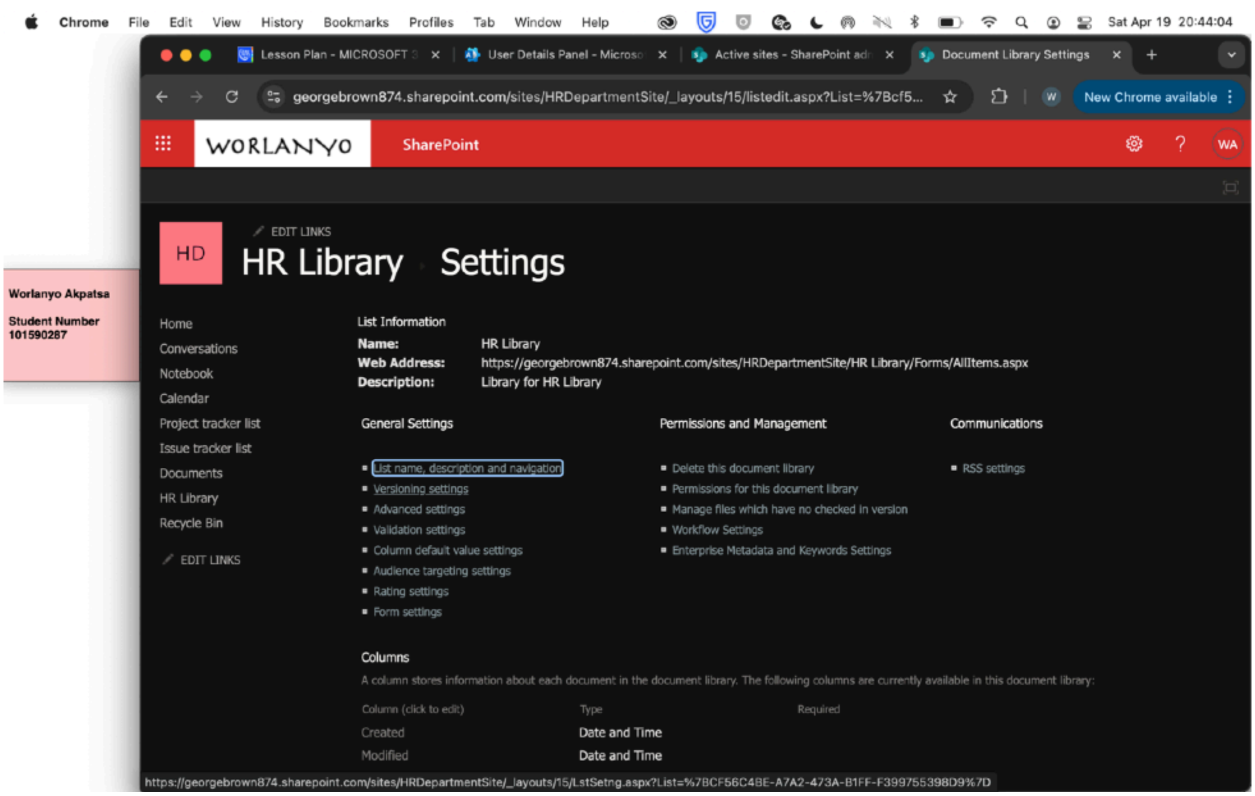


~~~~~~

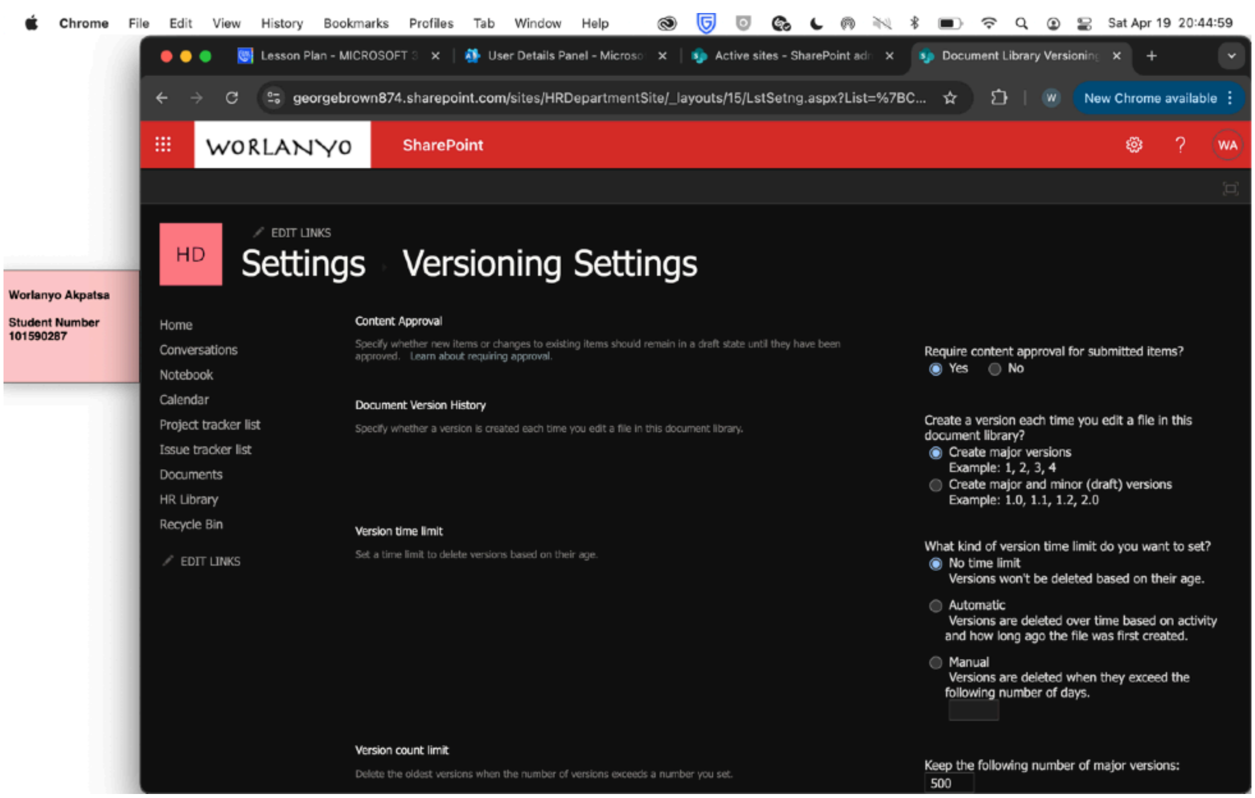
Student Name: Worlanyo Akpatsa Term: Winter 2025
Student ID: 101590287

~~~~~~

C: Choose Versioning Settings



D: Toggling "Yes" on require content approval

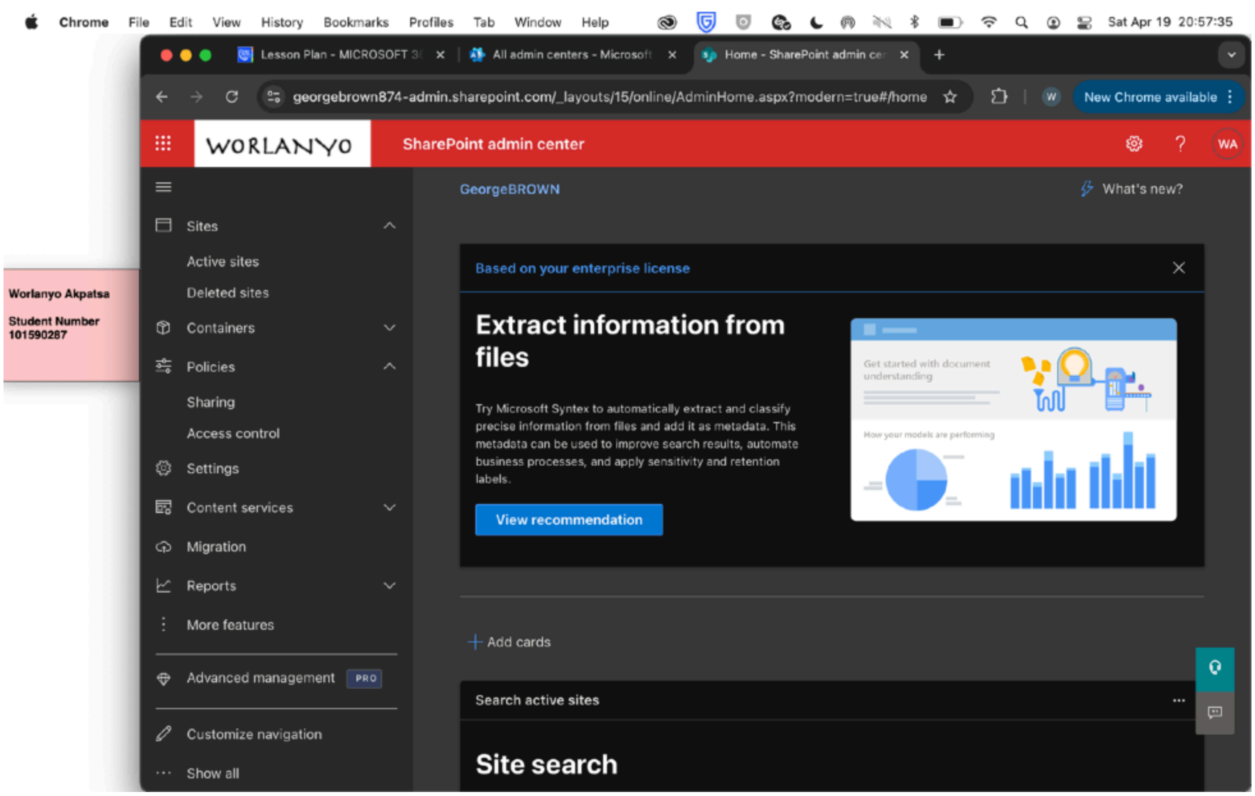


Student Name: Worlanyo Akpatsa Term: Winter 2025
Student ID: 101590287 ~~~~~~ ~~~~

2: Implement OneDrive for Business

2.1: Configure OneDrive settings to restrict external sharing

A: Navigate to Sharepoint Admin Center

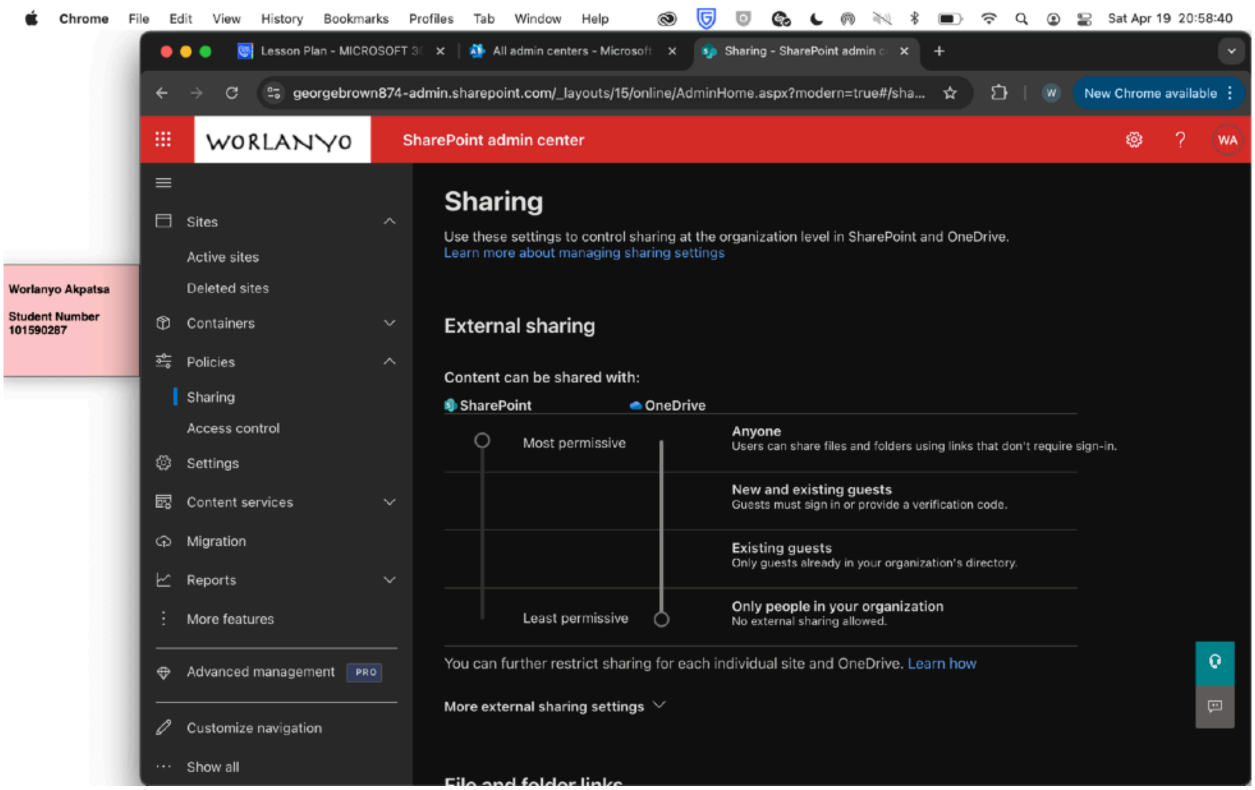


~~~~~~

Student Name: Worlanyo Akpatsa Term: Winter 2025
Student ID: 101590287

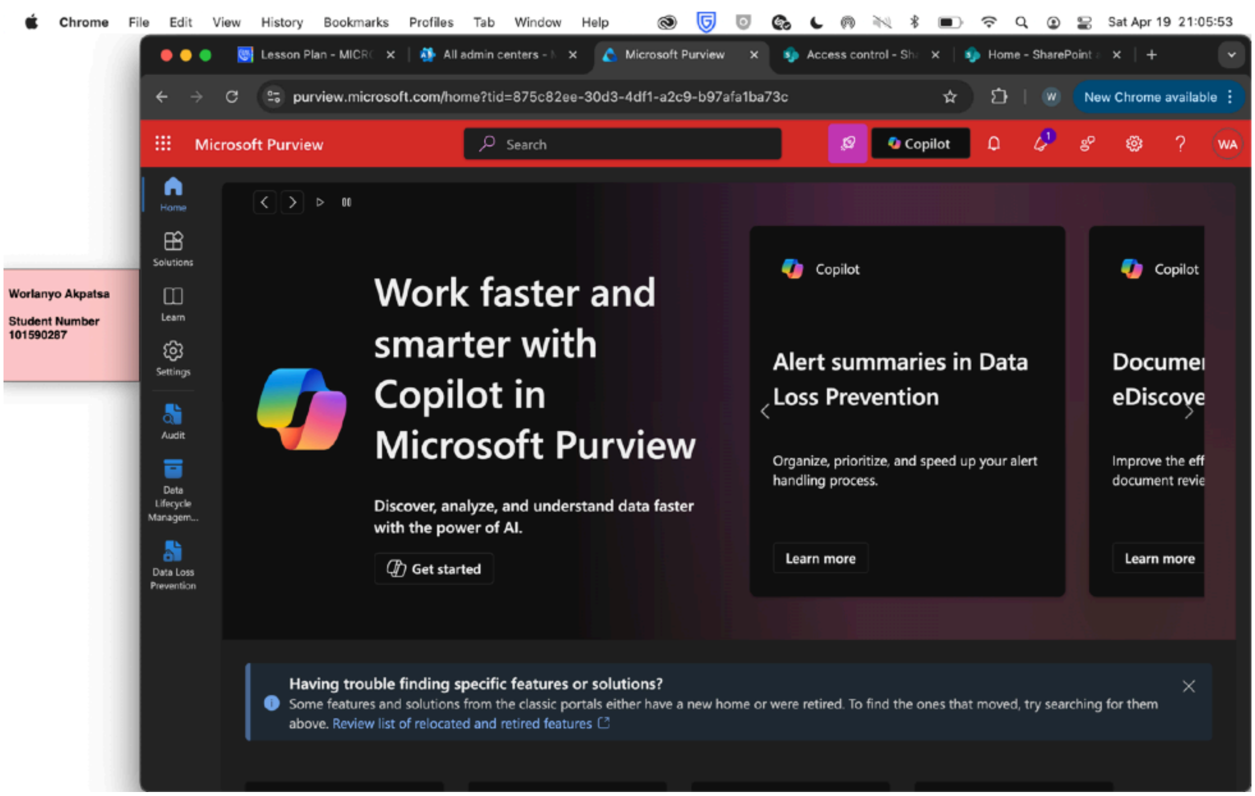
~~~~~~

B: Select policies->sharing in the left pane and drop slider for one drive to the lowest to restrict external sharing

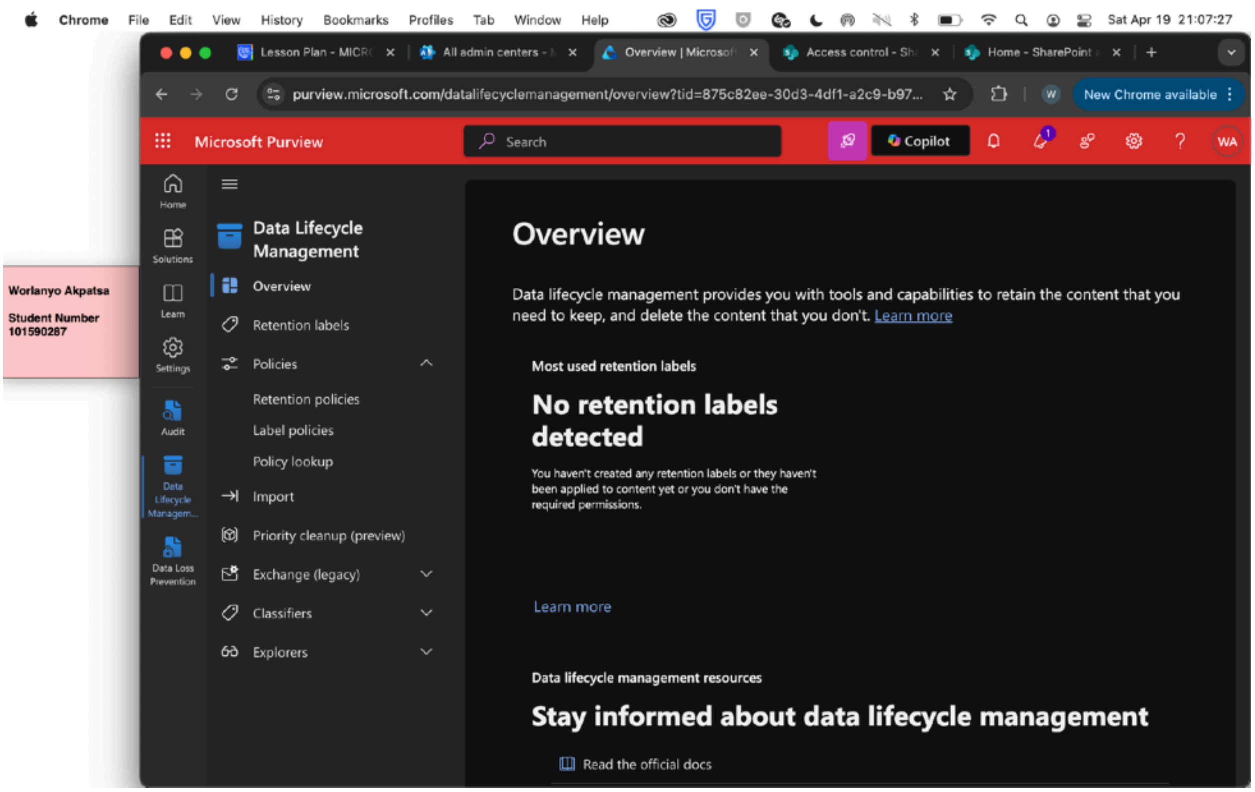


2.2: Enable file retention policies to ensure data is retained for at least five years

A: Navigate to Purview Compliance Center by clicking "compliance" under admin centers in 365 admin center



B: Select Data life cycle Management in the left pane

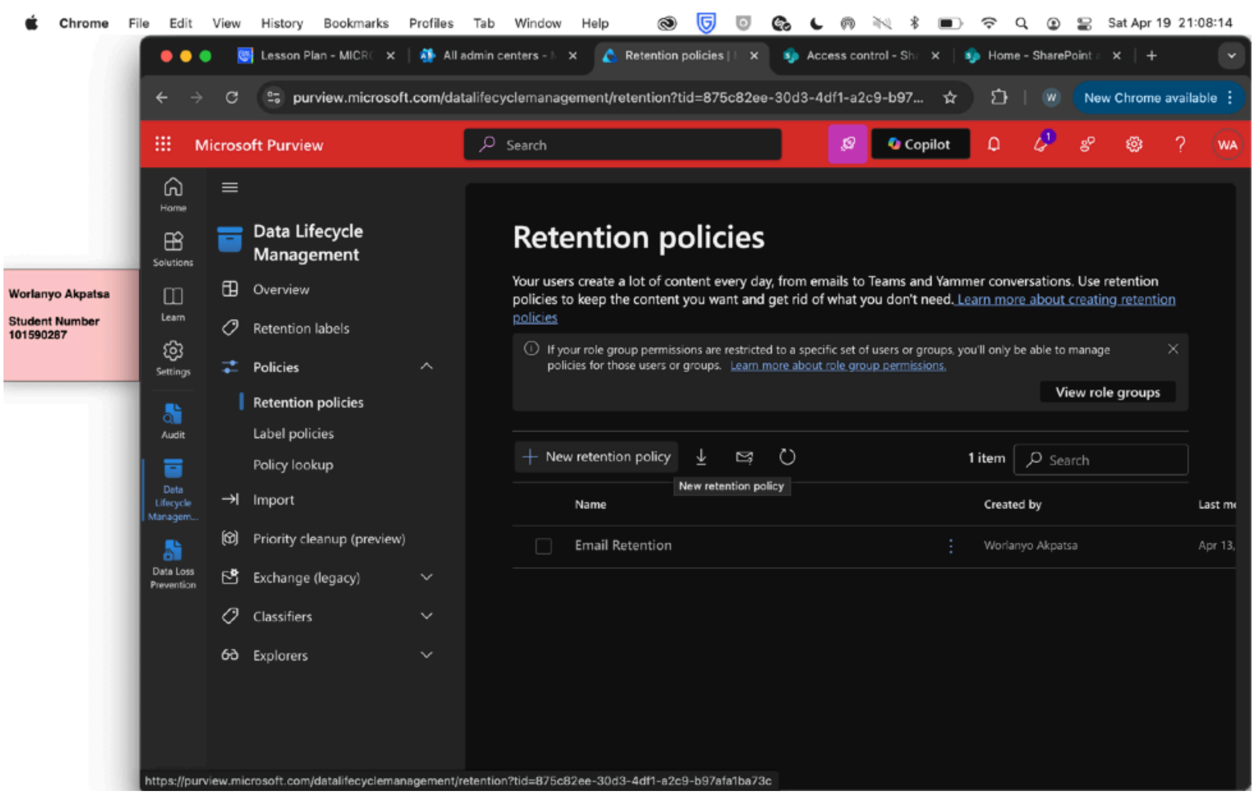


~~~~~~

Student Name: Worlanyo Akpatsa   Term: Winter 2025
Student ID: 101590287

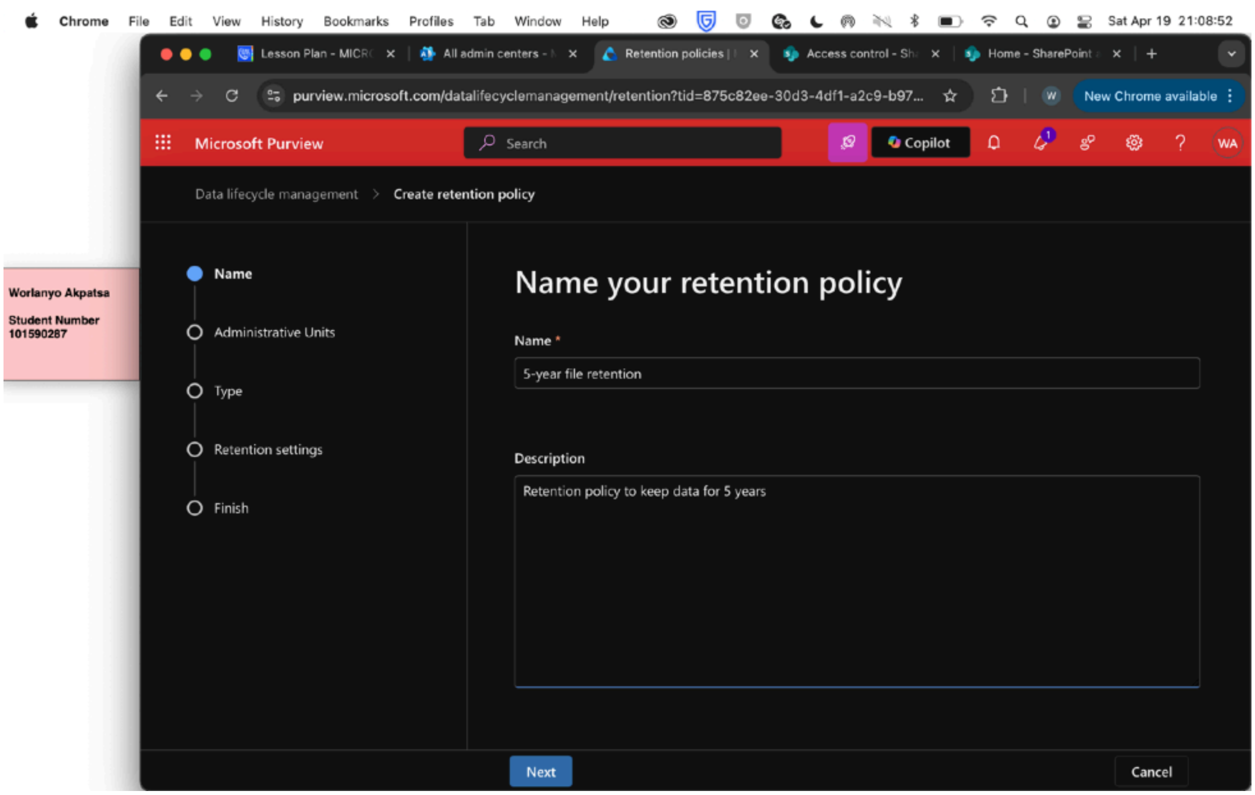
~~~~~~

C: Select Policies->Retention Policies and click new retention policy

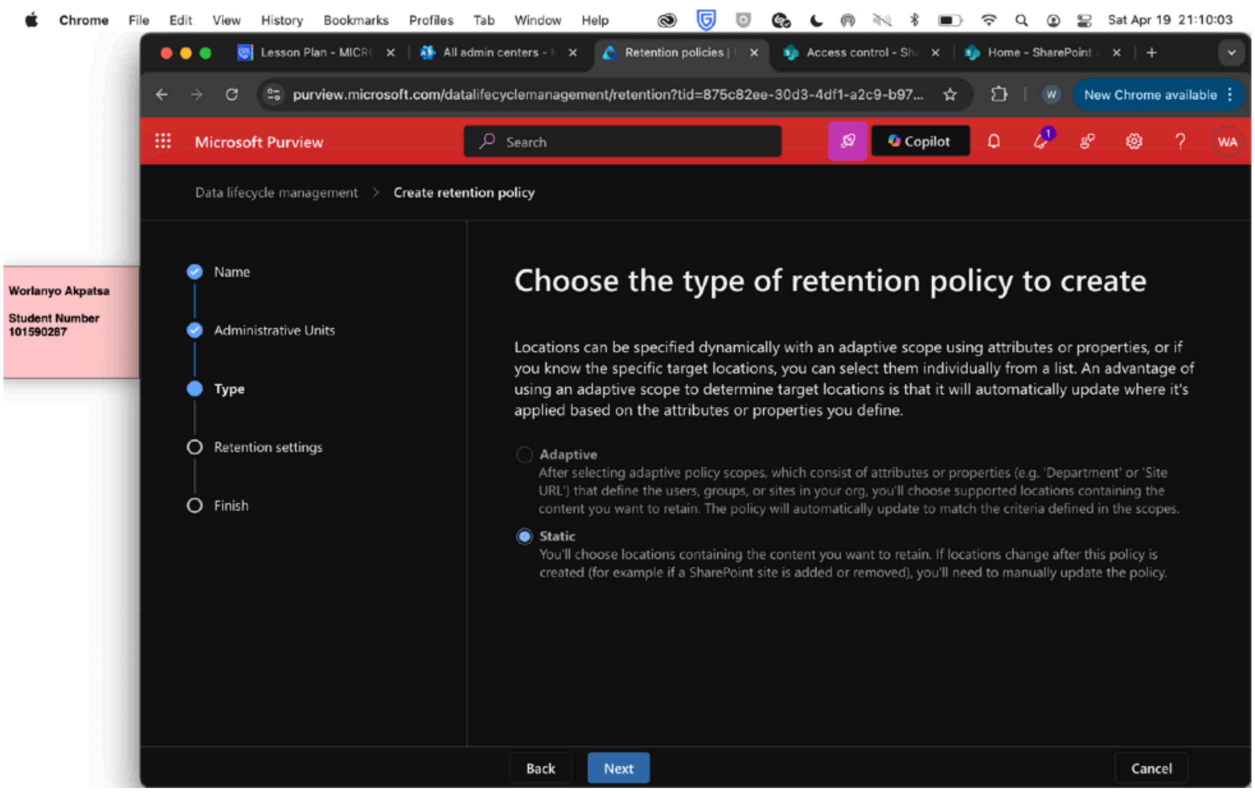


Student Name: Worlanyo Akpatsa Term: Winter 2025
Student ID: 101590287

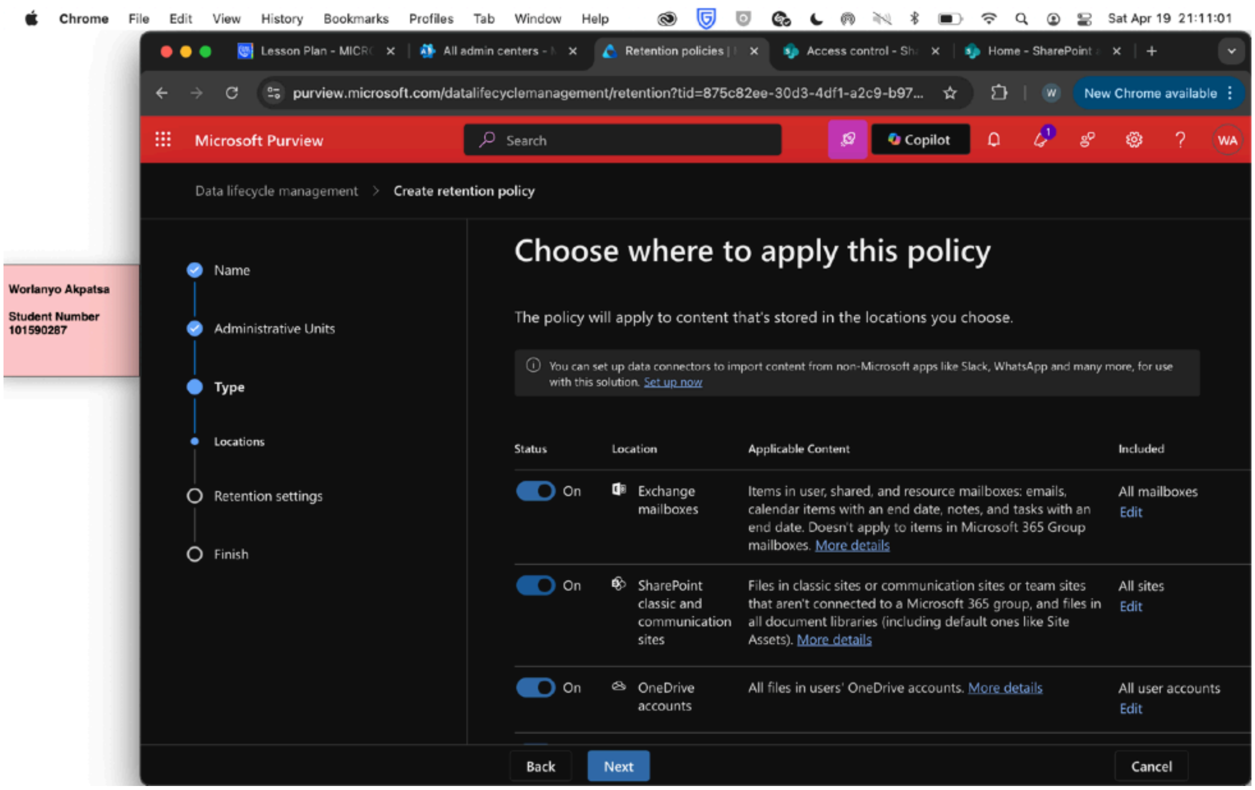
D: Naming policy



E: Type of Policy (Static)



F: Choosing where to apply policy

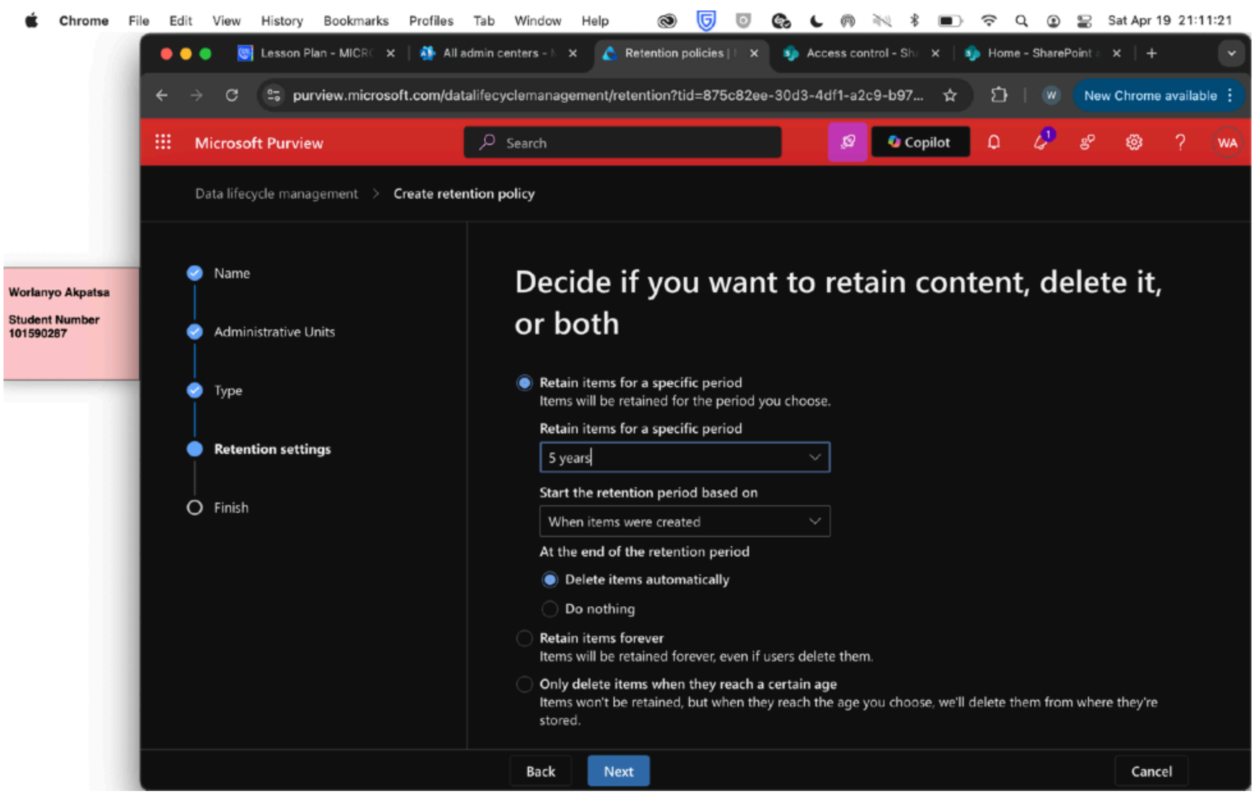


~~~~~~

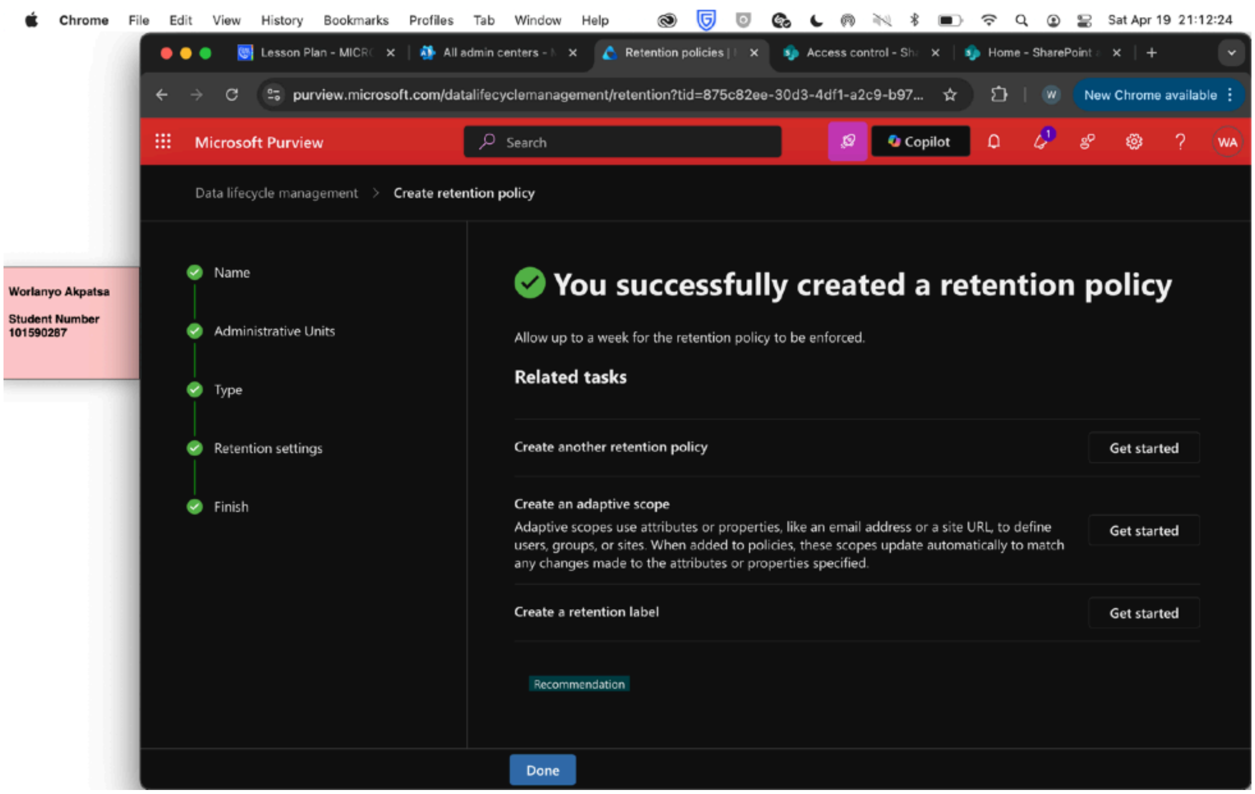
Student Name: Worlanyo Akpatsa Term: Winter 2025
Student ID: 101590287

~~~~~~

G: Choosing retention settings (retention period (5 years))

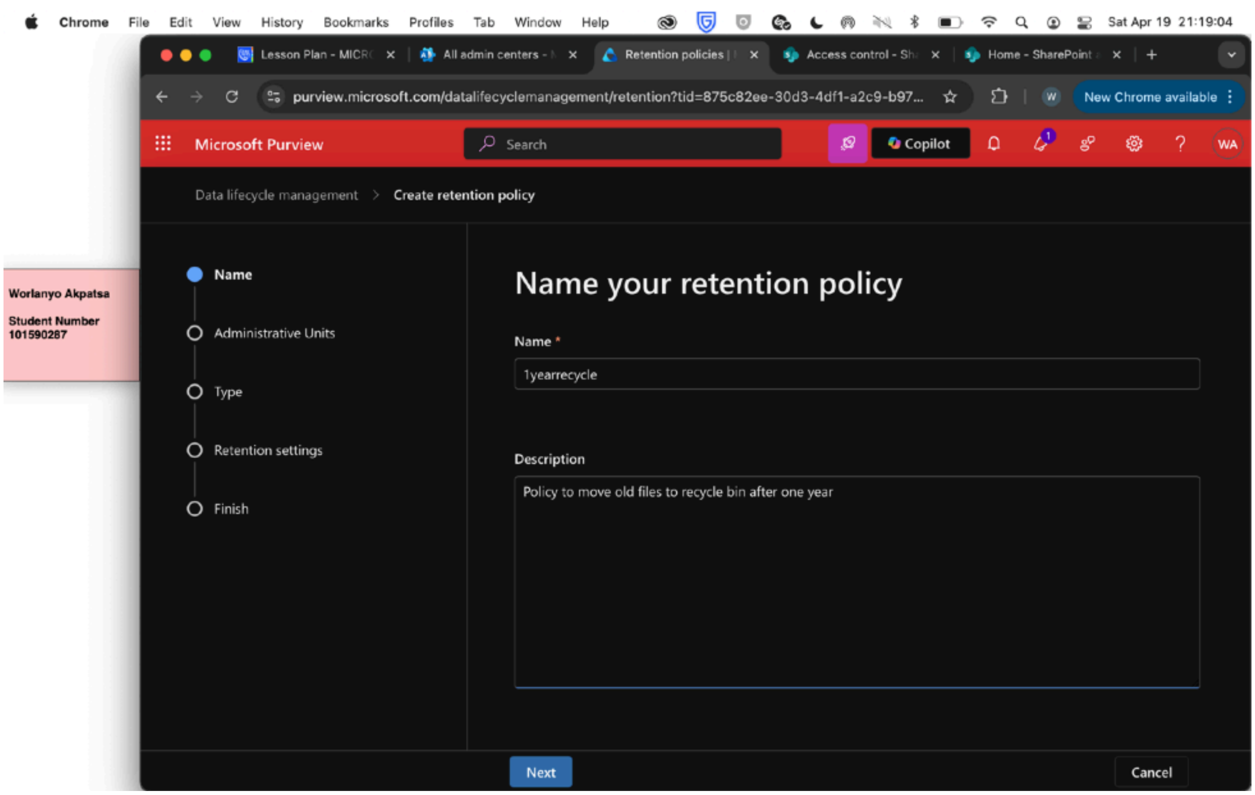


H: Policy Created

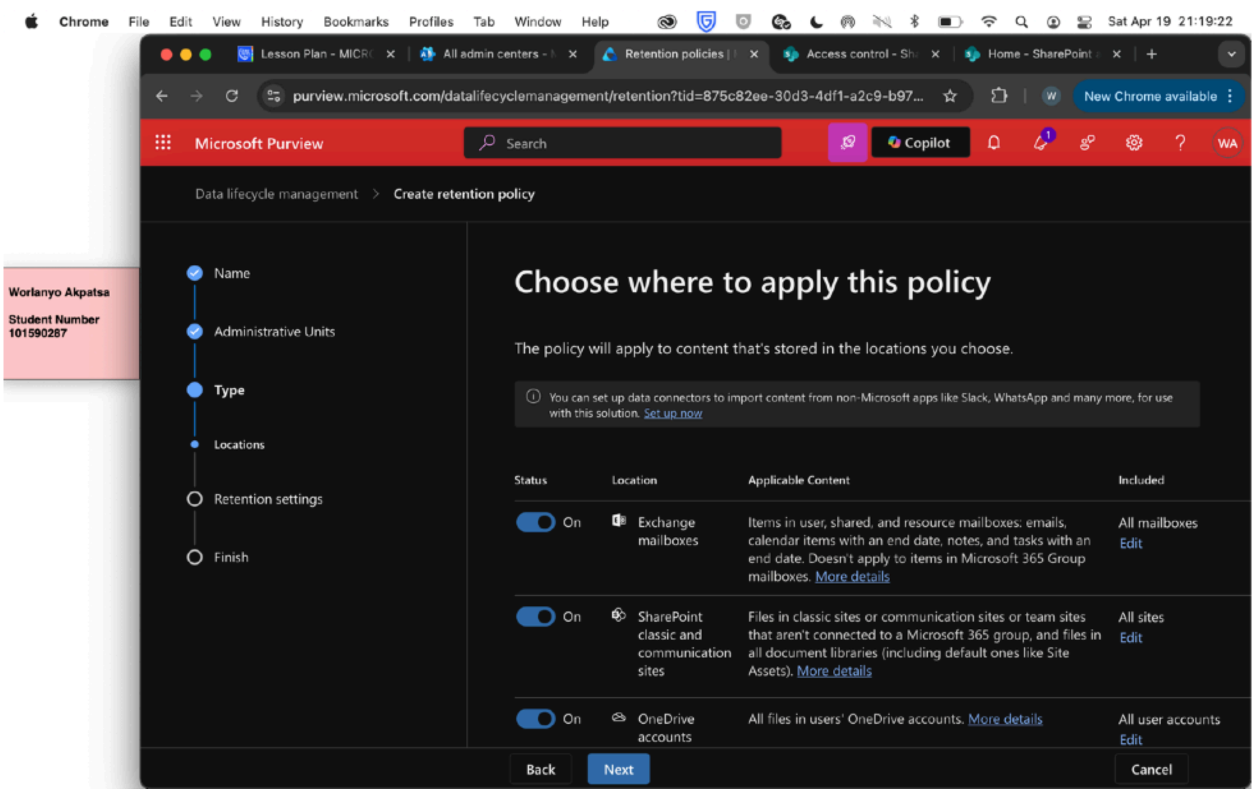


2.2: Set up a policy to automatically move old files to the recycle bin after a year.

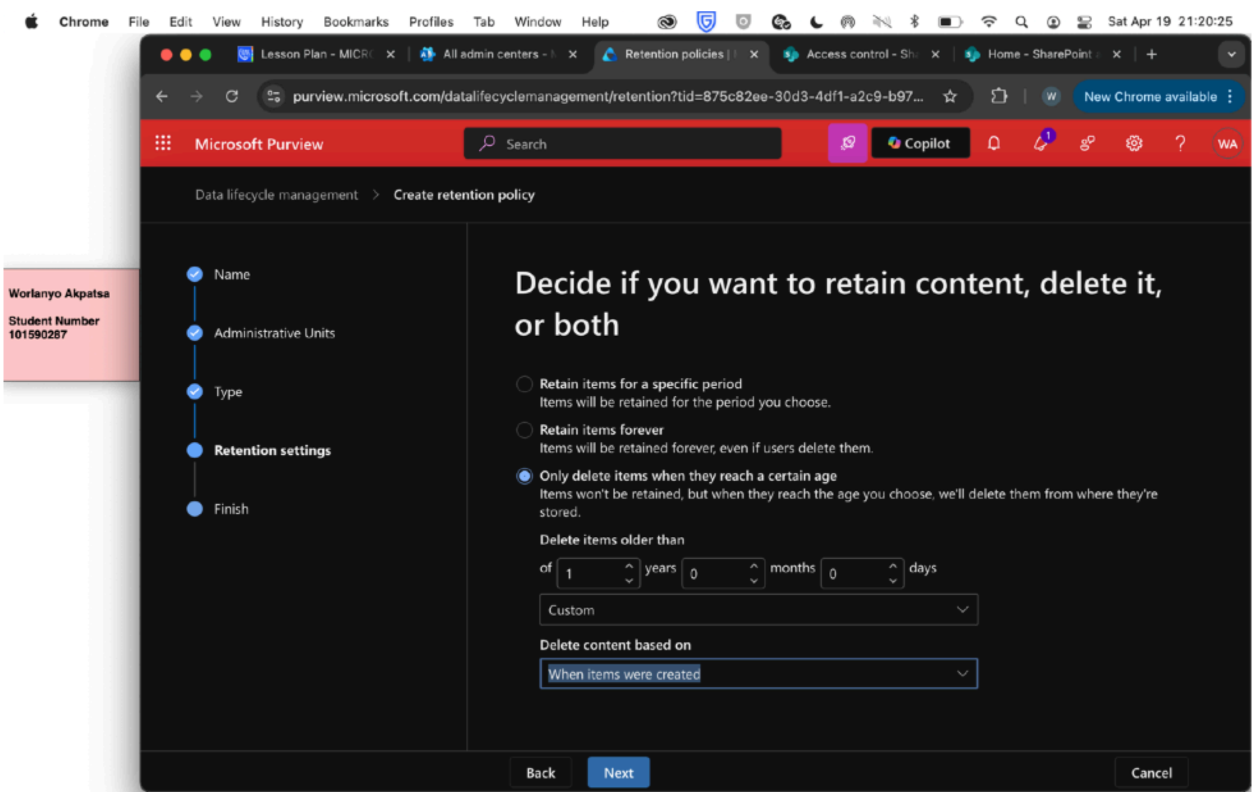
A: Still in Data life cycle Management, create a new retention policy



B: Choosing where to apply policy



C: Retention Settings (deleting files when they reach a year old)

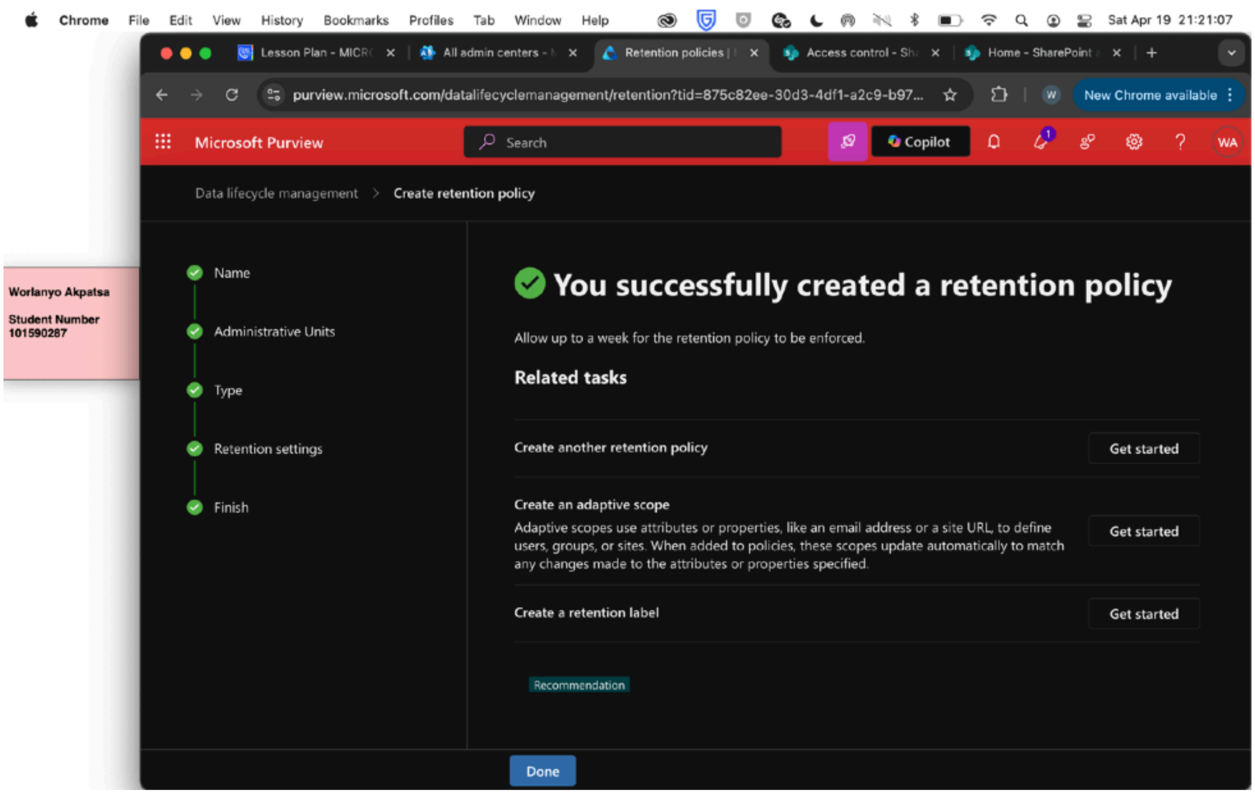


~~~~~~

Student Name: Worlanyo Akpatsa Term: Winter 2025
Student ID: 101590287

~~~~~~

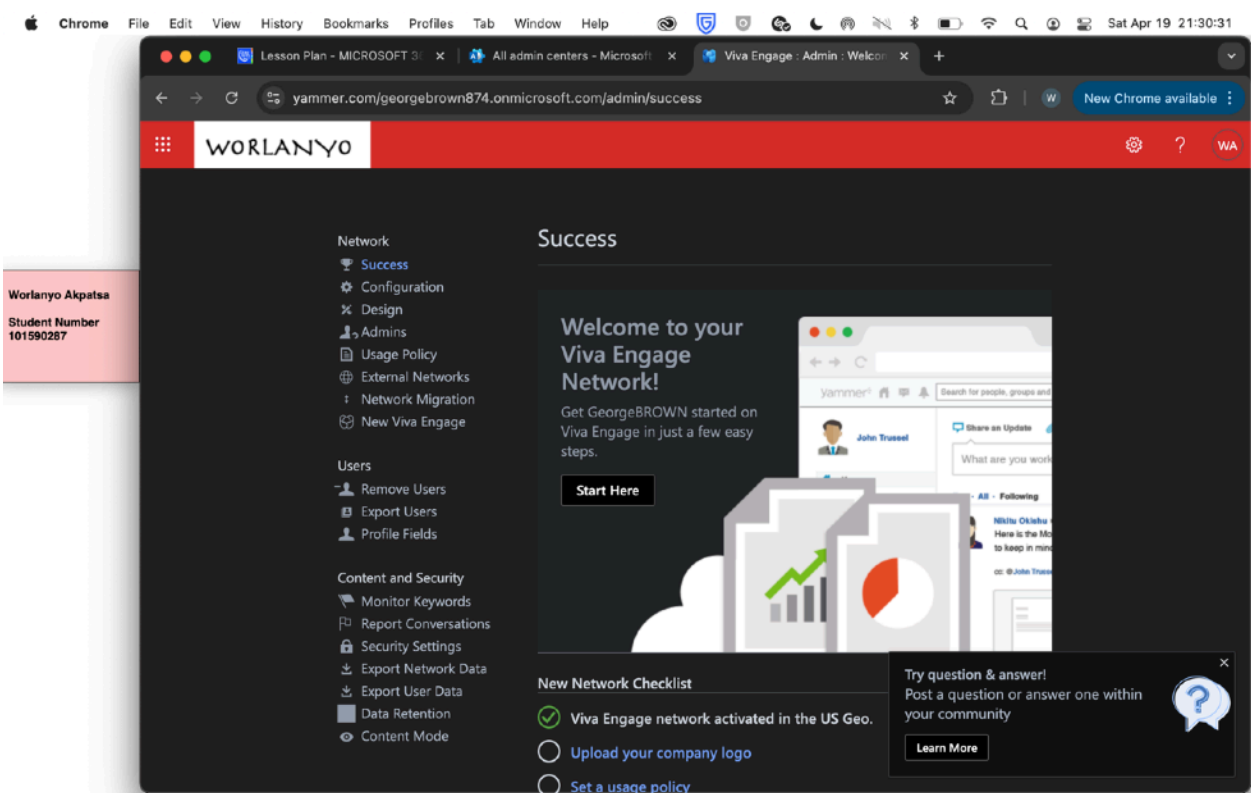
D: Policy Created



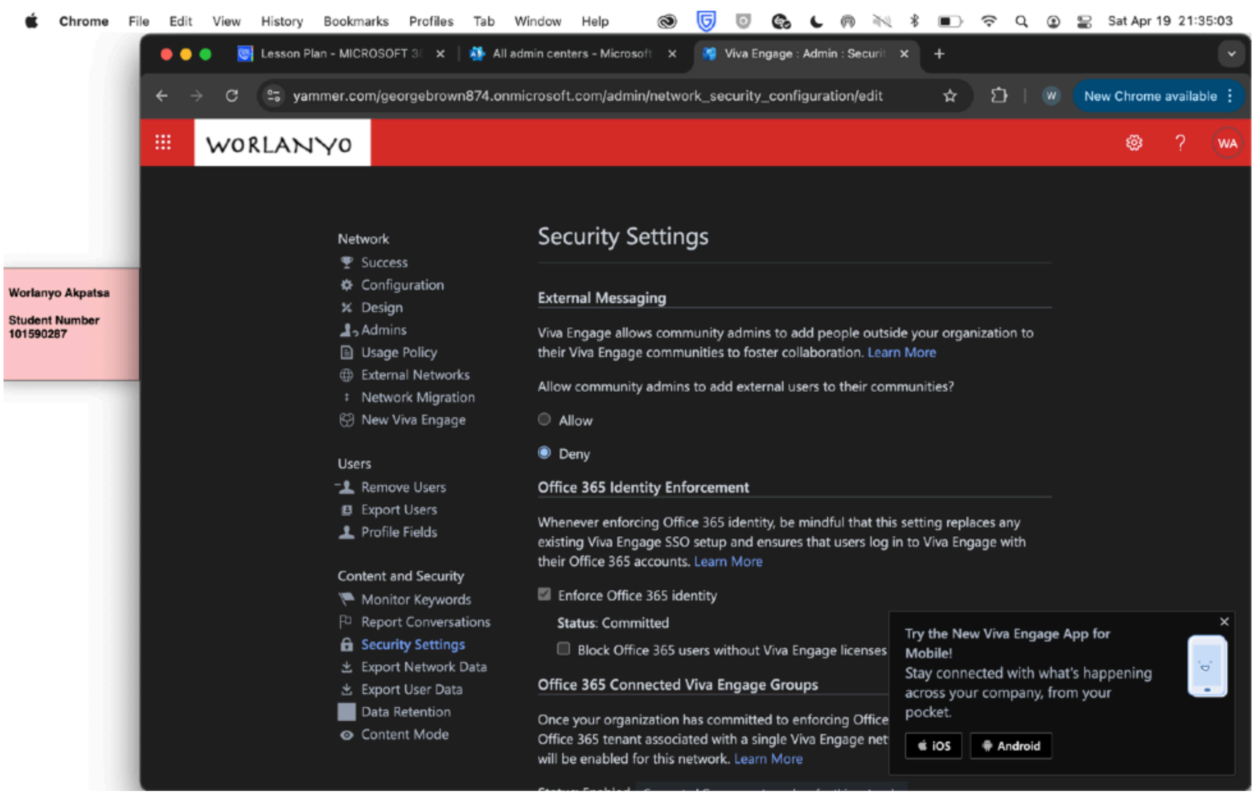
3: Set up Viva Engage for Enterprise Social Networking

3.1: Configure Viva to allow only internal communications

A: Navigate to all admin centers in 365 admin center and search for viva engage. Sign in with global admin credentials



B: In the left pane, select security settings and toggle deny in security settings

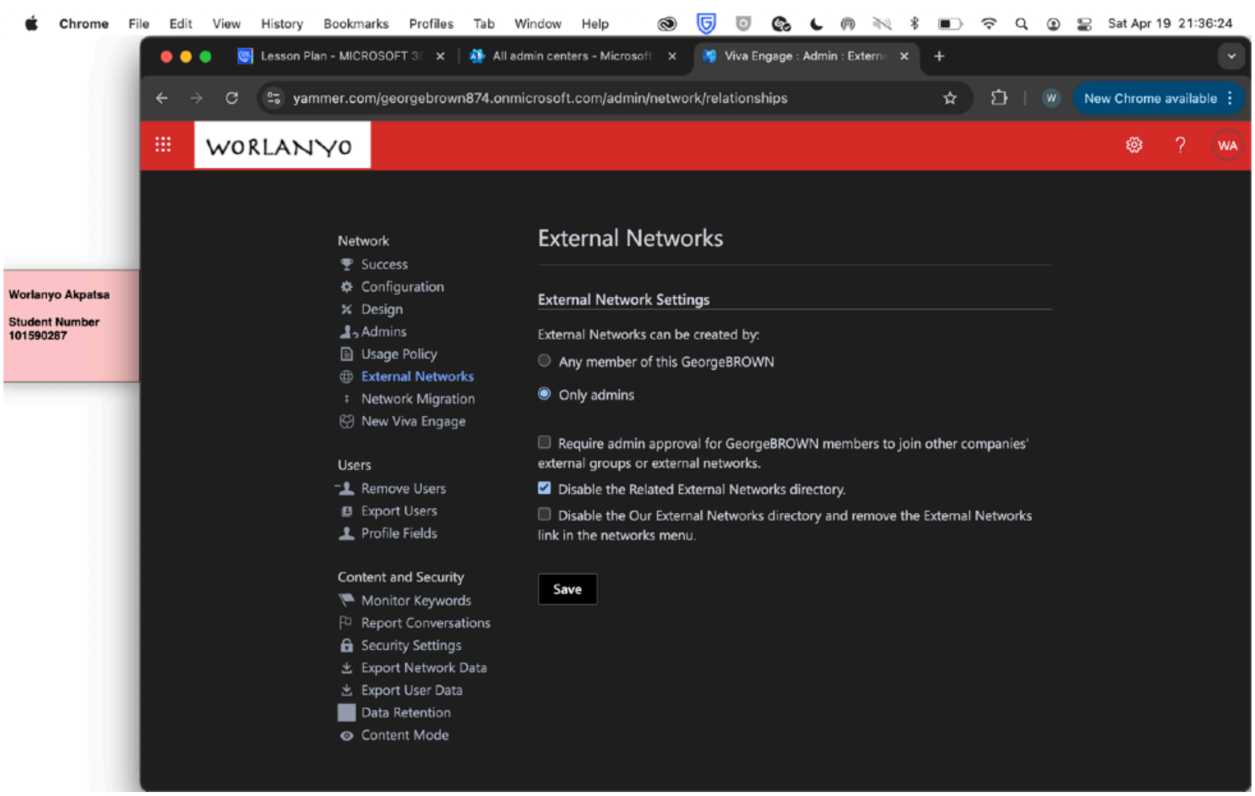


~~~~~~
~~~~

Student Name: Worlanyo Akpatsa Term: Winter 2025
Student ID: 101590287

~~~~~~
~~~~

C: Selecting External Networks and also disabling that



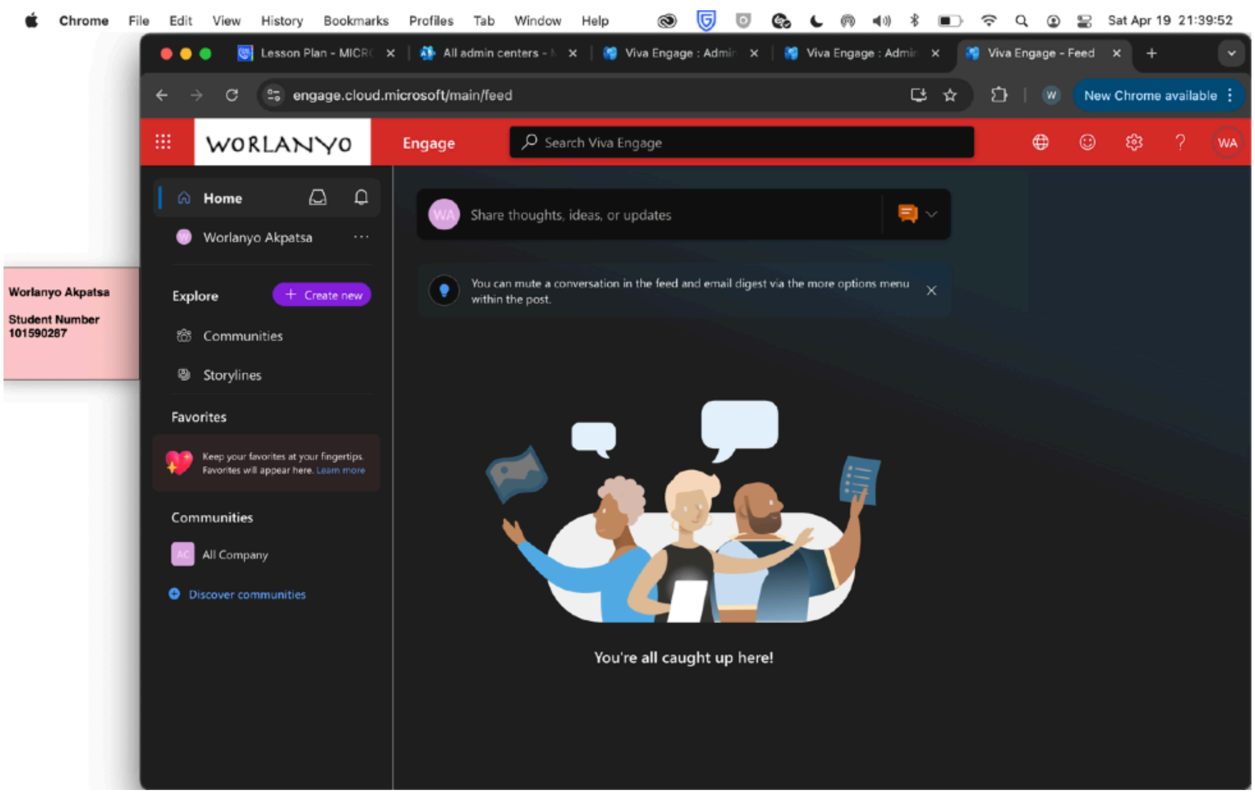
~~~~~~

Student Name: Worlanyo Akpatsa Term: Winter 2025
Student ID: 101590287

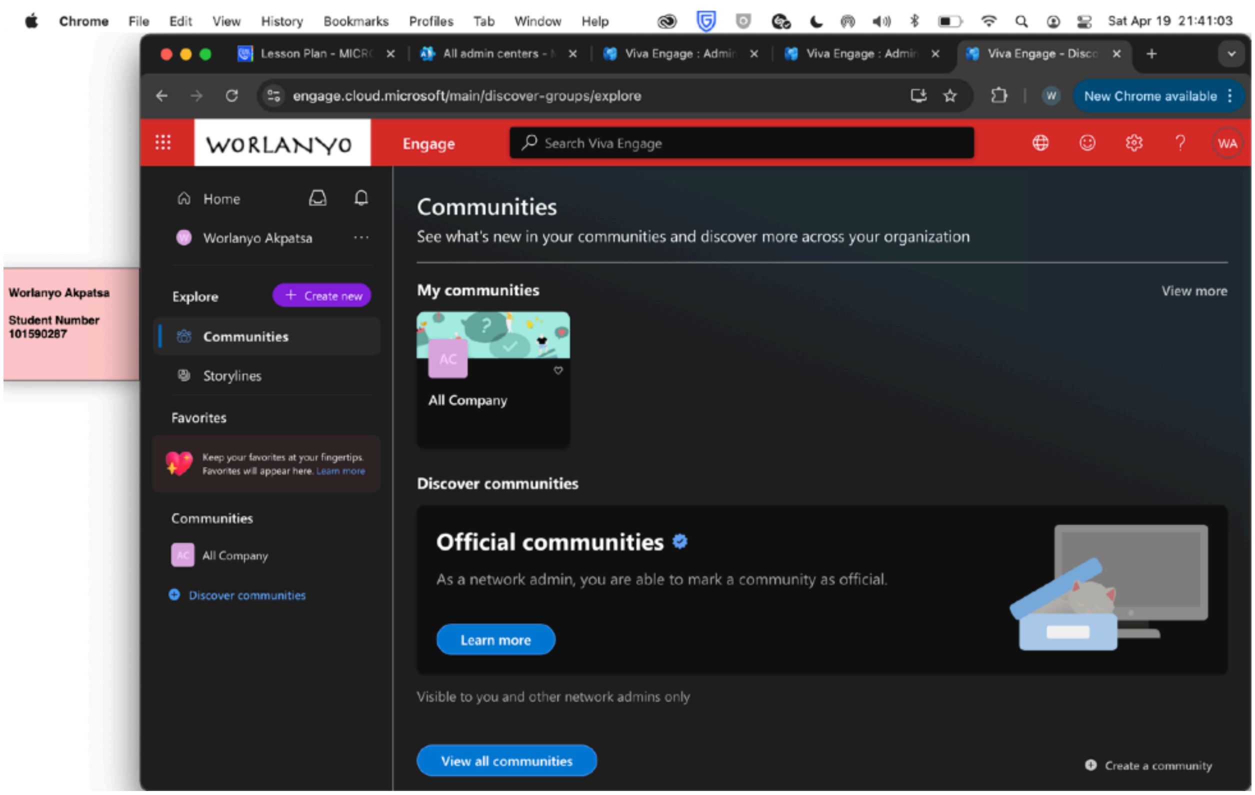
~~~~~~

3.2: Set up groups for company-wide announcements and department specific discussions.

A: Navigate to engage.cloud.microsoft and select coommunities in the left pane



B: Choose All Company as official company group for company-wide announcements



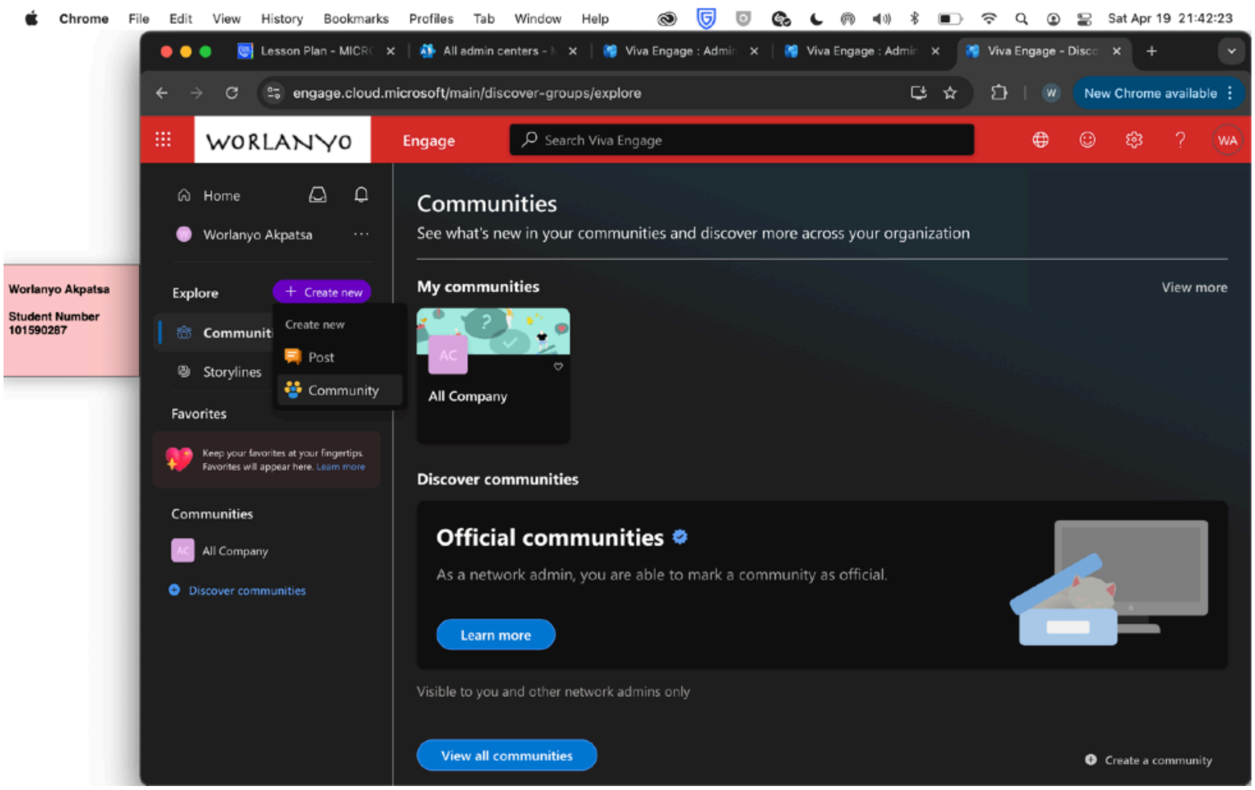
~~~~~~

Student Name: Worlanyo Akpatsa Term: Winter 2025
Student ID: 101590287

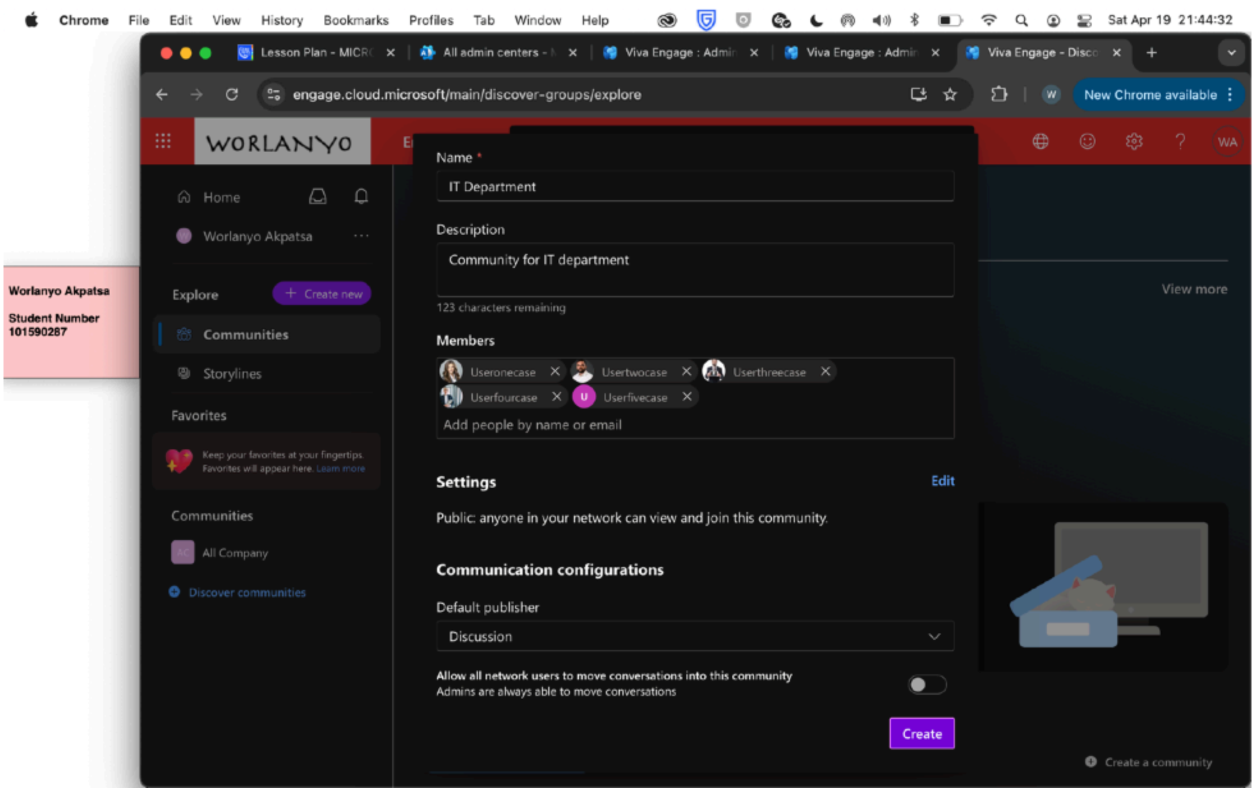
~~~~~~

Creating IT Community

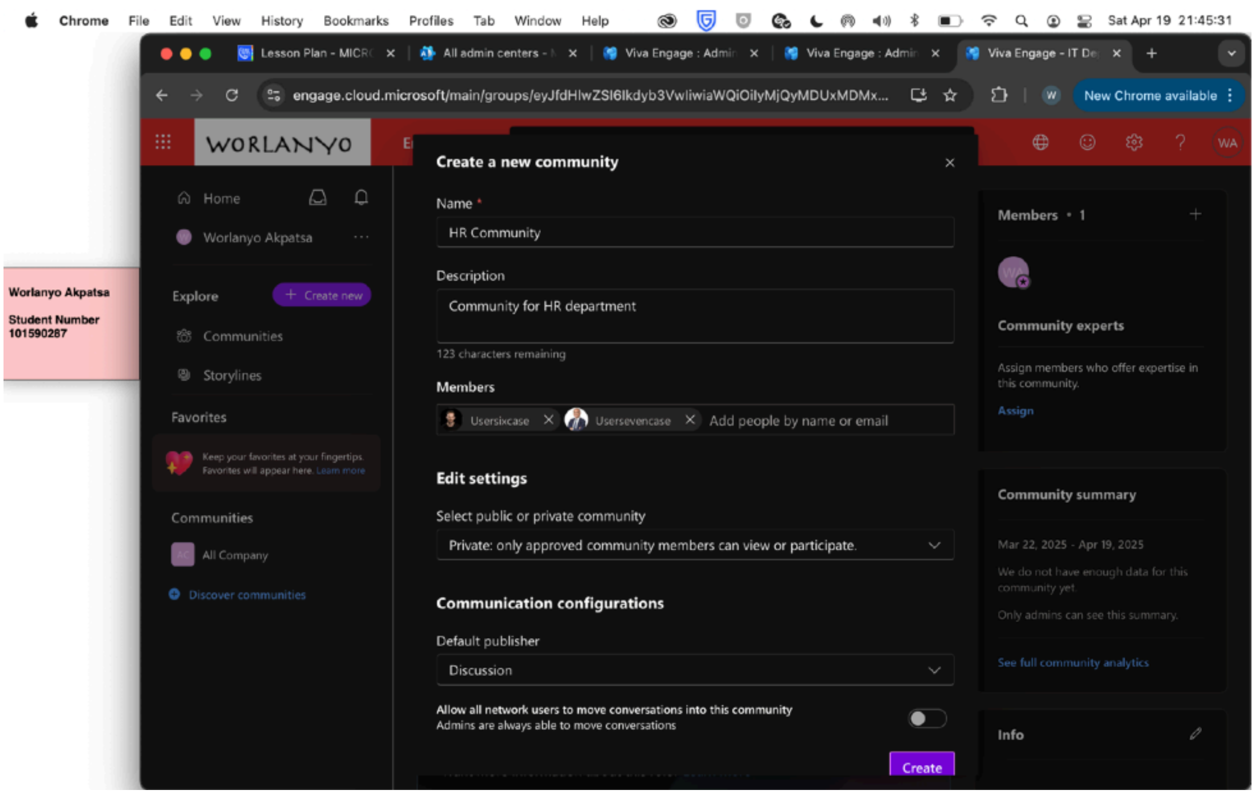
A: Choose create new->community in the left pane



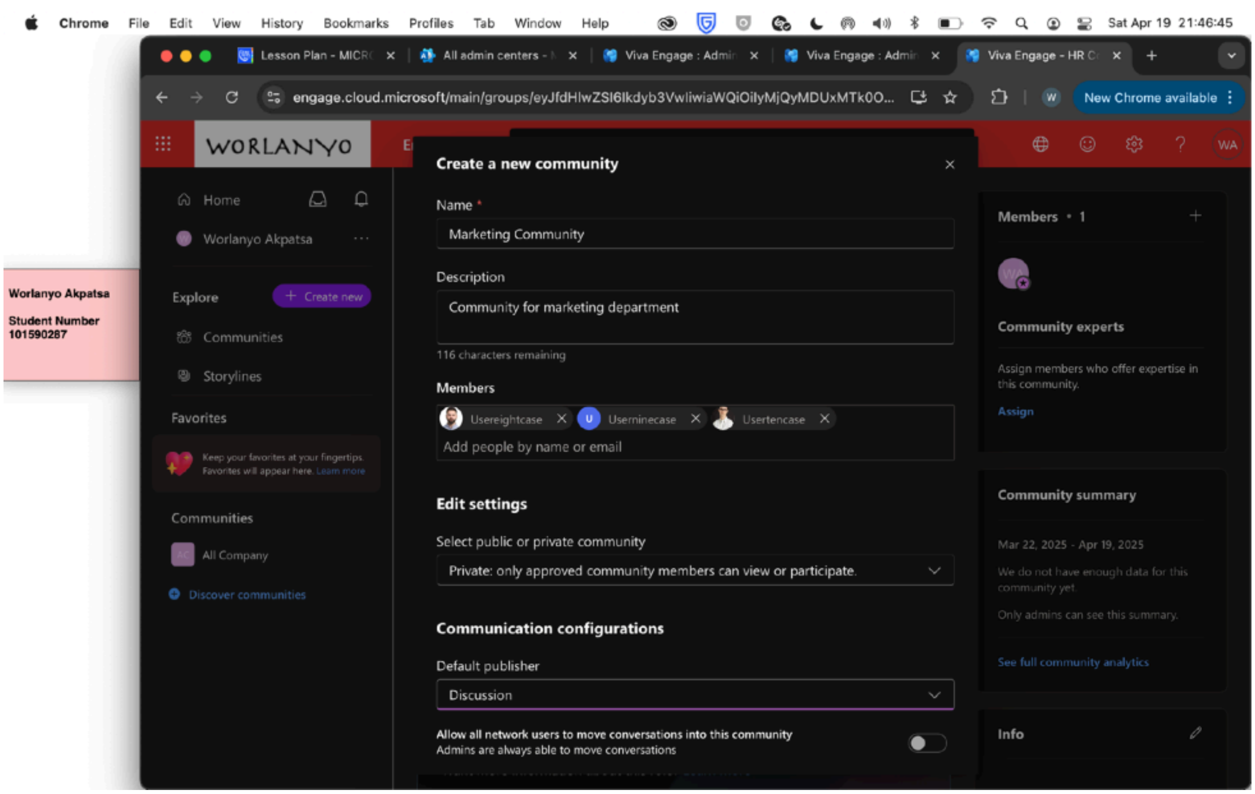
B: Confirming Name and adding members per csv file



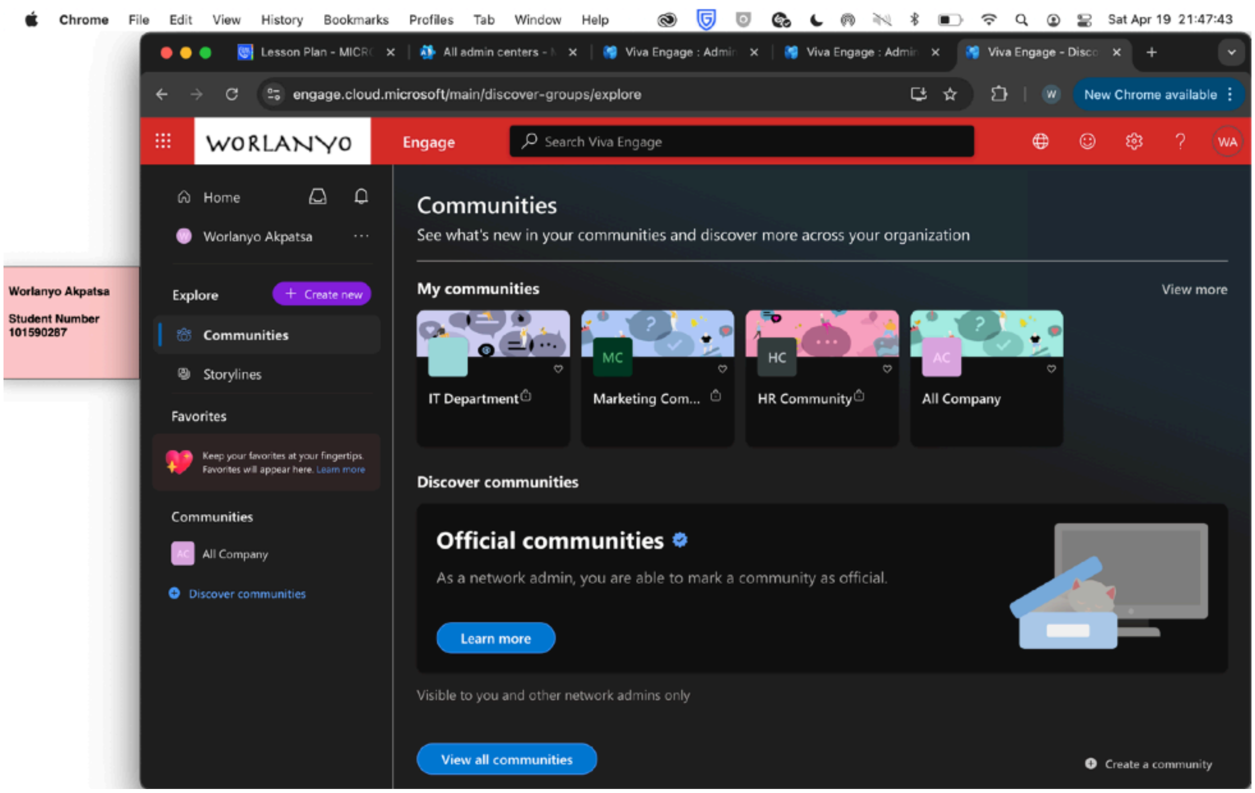
C: Creating HR Community and adding members per csv file



D: Creating Marketing Community



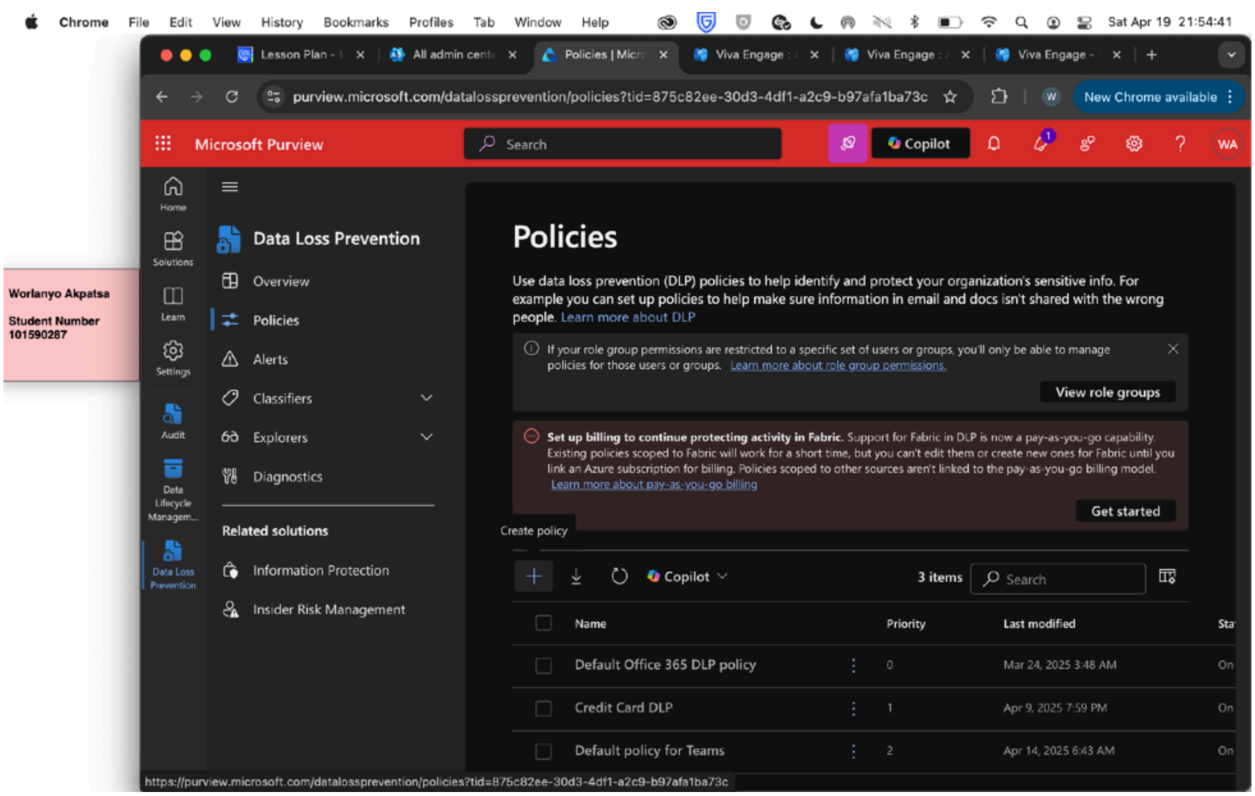
E: All communities created



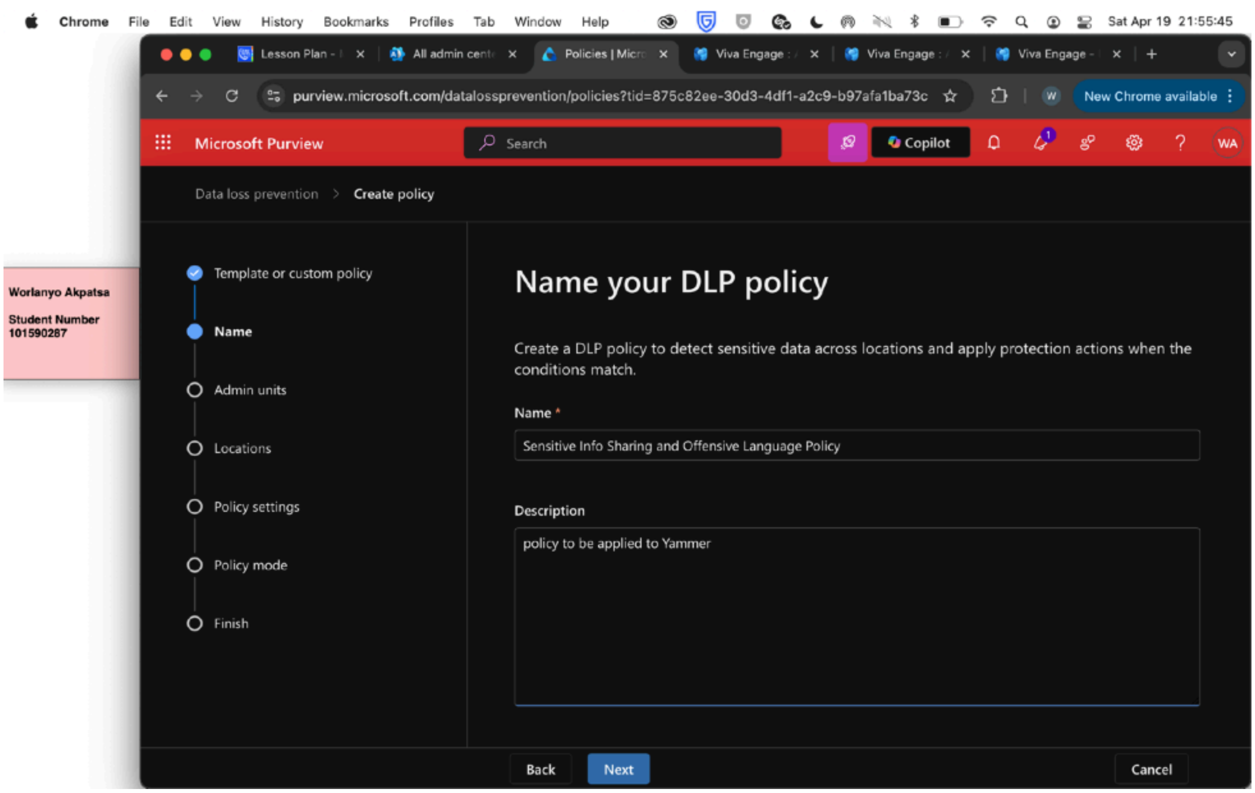
3.3: Ensure Compliance with the company's social media policy

I plan to do this by creating a policy in Microsoft purview to detect sensitive info sharing

A: Navigate to data loss prevention->policies in Microsoft Purview and click create a policy



B: Name and describe policy

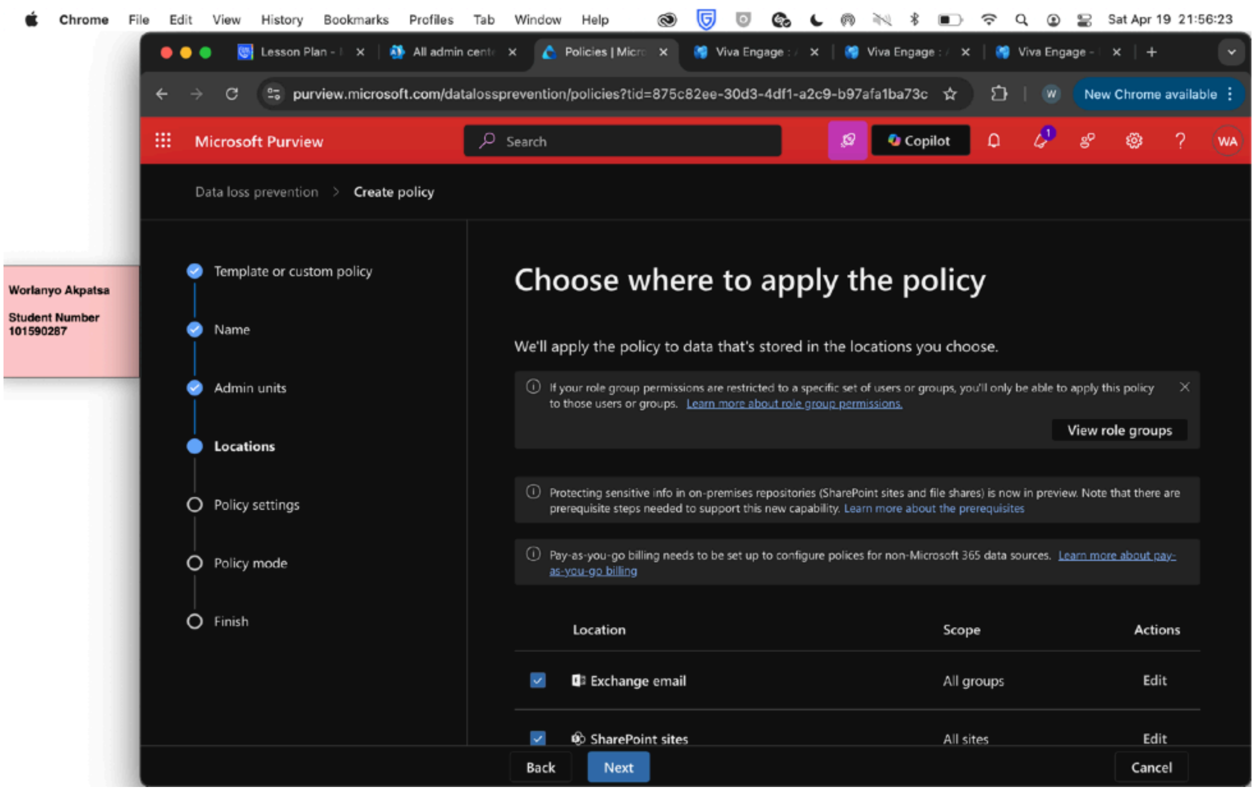


~~~~~~

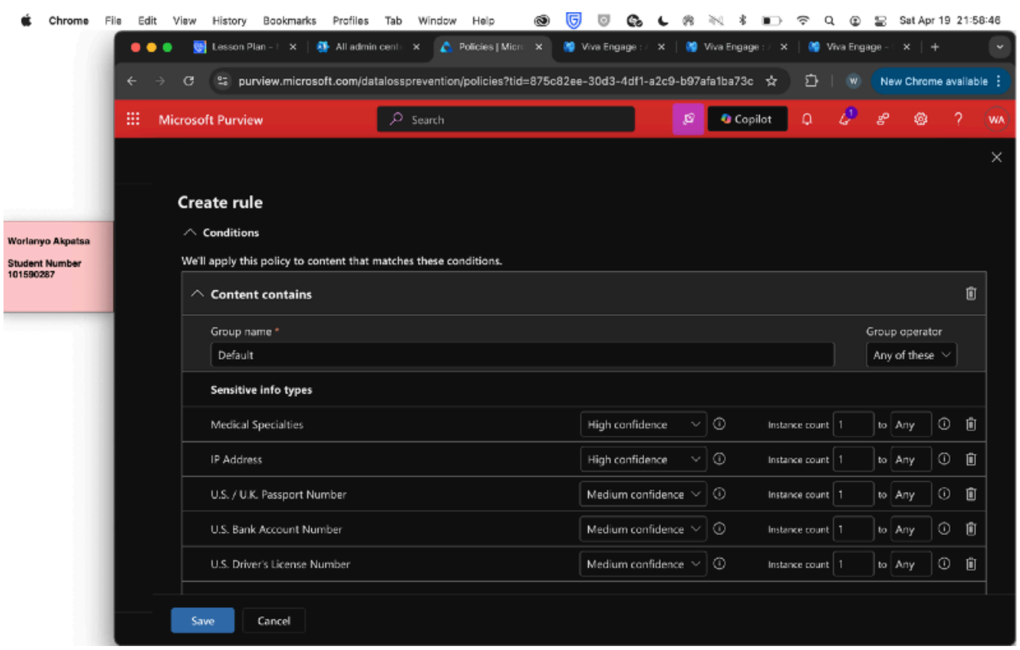
Student Name: Worlanyo Akpatsa | Term: Winter 2025
Student ID: 101590287

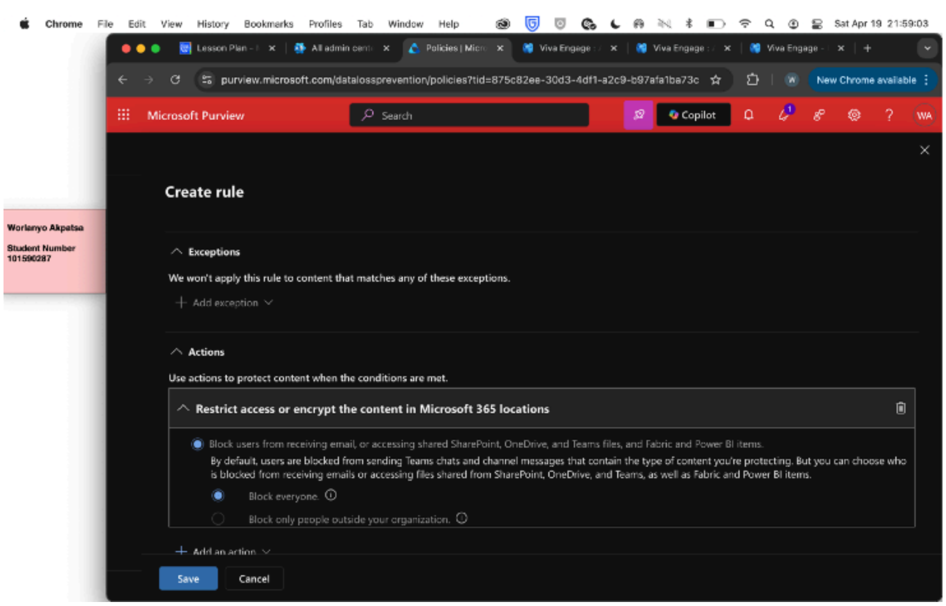
~~~~~~

C: Applying policy to all locations including Yammer



D: Creating rule condition and responding action



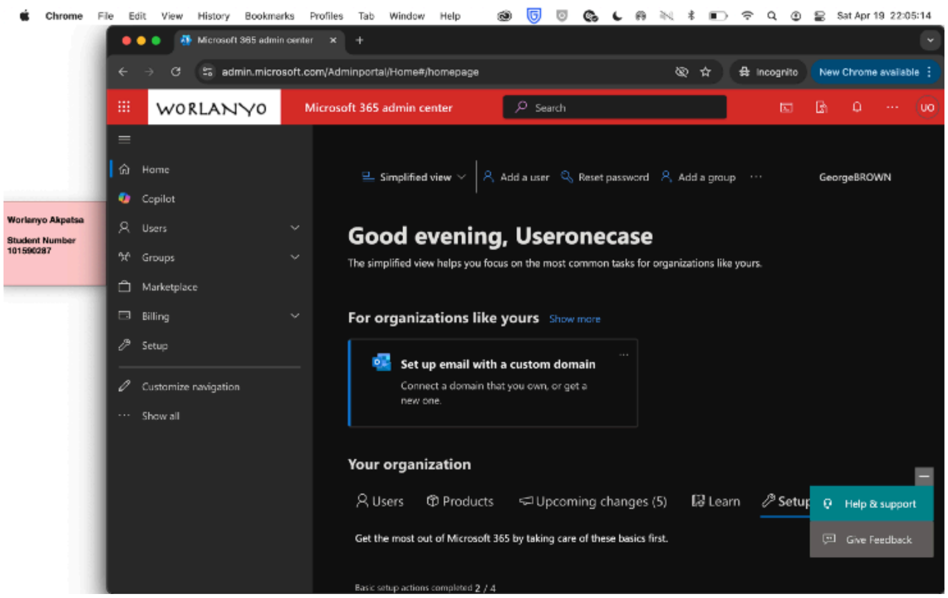


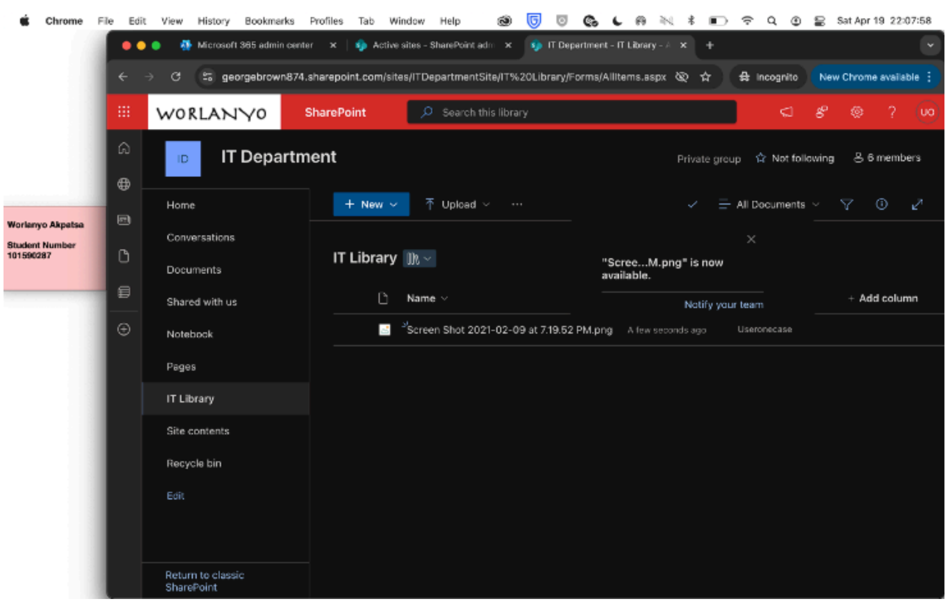
~~~~~~

Student Name: Worlanyo Akpatsa　　　　Term: Winter 2025
Student ID: 101590287

~~~~~~

THIS IS A CREATED USERS ACCOUNT IN ADMIN CENTER, VIVA ENGAGE AND OTHER SERVICES LIKE SHAREPOINT



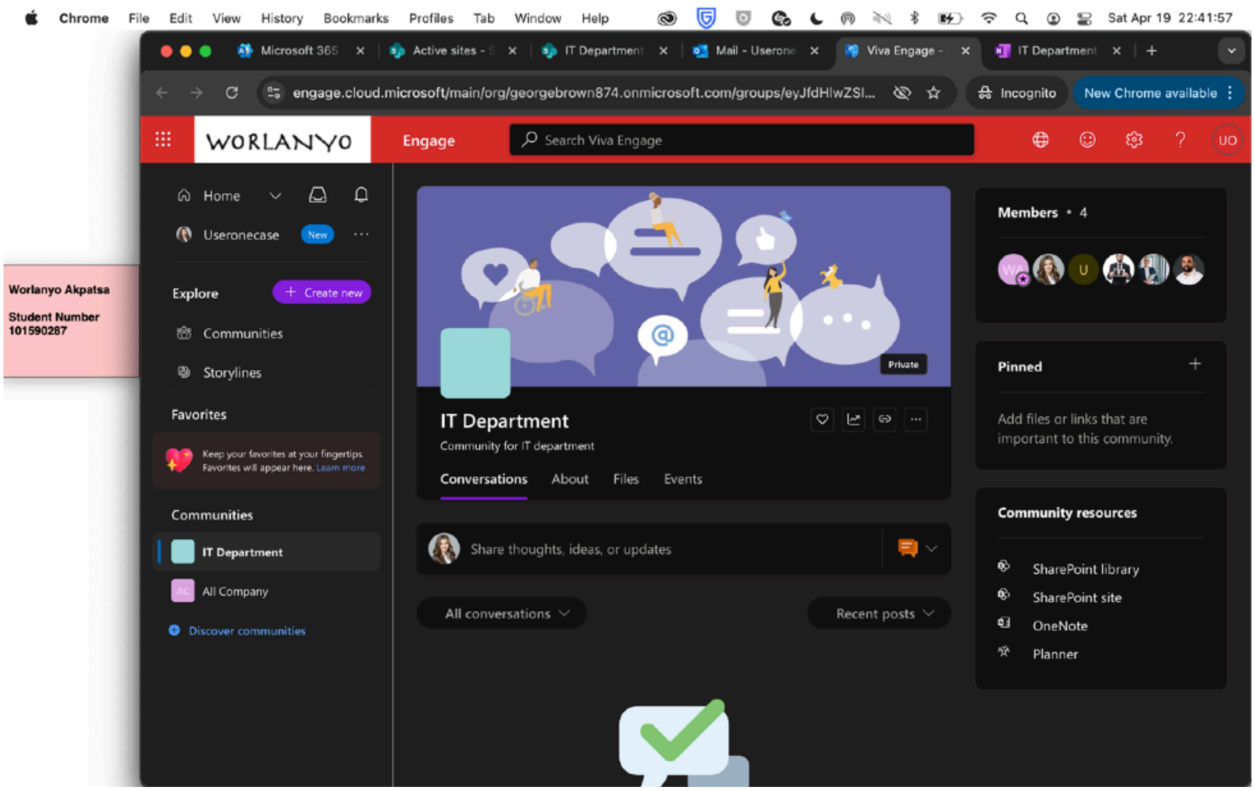


~~~~~~

Student Name: Worlanyo Akpatsa
Student ID: 101590287

Term: Winter 2025

~~~~~~



Task 3 Summary:

If I am being completely honest, task 3 was the most tiring activity to do in this assignment. Nonetheless, this teaches mental toughness and helps me get more accustomed to doing a heavy load of work.

To start, I had to create 3 different sites for the 3 different departments of the company. To do this, I navigated to the Sharepoint admin center and selected sites->active sites in the left pane. I then selected to choose a team site and chose my template. After this, I named my site (depending on the department I was creating it for) and then added the members as per my csv file that i used to create the ten users.

Next job on the list was to configure document libraries and permissions for each site. To configure document libraries, I had to visit the site address to display the sites. On the homepage, I clicked new and selected document library to add a new document library. Just like the sites, I named the libraries after the respective departments.

Just to do some further configuration, I decided to create an alert for when something happens in the document library for all the 3 created document libraries. To do this, I had to click on the three dots in the top corner and select alert me.

Next thing to configure was site permissions. While on the site homepage, I clicked the settings icon in the top right corner and selected site permissions->advanced site permissions m. Here, I am able to configure site permissions for the various users.

Last thing I had to do regarding the document libraries was to enable versioning and content approval which was straightforward. While in the library, select the settings icon and click library settings->more library settings. This opens up a window where I selected versioning settings and toggled yes on require content approval.

The next major job for task 3 was to implement Onedrive for Business which I have done quite a few times so it was smooth. Here, you need to use SharePoint Admin Center as it has incorporated Onedrive settings. On the left pane in Sharepoint Admin Center, I selected policies->sharing and in this window, dragged down the slider for OneDrive sharing to the lowest which means no external sharing allowed.

After this, I navigated to The Purview Compliance center to create a retention policy to ensure data is retained for at least five years. Creating policies in the compliance center is something I have done several times so at this point, it was easy navigation.

I had to click Data Life Cycle Management in the left pane and then select policies->retention policies. I then decided to create a new retention policy to ensure my data is retained for at least five years. I named my policy and chose where to apply it (everywhere) and then had to choose my retention settings. I chose to retain items for 5 years as per the instructions given. I concluded and created my policy.

Next thing I had to do was create a policy to automatically move old files to the recycle bin after a year. Lucky for me, I did not have to leave data life cycle management to do this. I simply chose to create a new retention policy. After naming it and choosing locations to apply, I had to choose retention settings. This time, I chose to "only delete files when they reach a certain age" and put the period of one year for the age. I concluded and created my new policy.

The last part of this task is something I had not really gotten used to at first so I was glad to do it; Viva Engage.

First thing I had to do was configure Viva to allow only internal communication. I navigated to my 365 admin center, and searched for viva engage in all admin centers. I clicked it when it showed up and was taken to Viva engage where I had to resign in with my global admin credentials.

In the left pane in Viva, I selected security settings and toggled deny for external messaging. This for sure only encourages internal communication in the company.

Next, I had to set up groups for company-wide announcements and department specific discussions. This was a new one for me and I enjoyed it very much. I navigated to engage.cloud.microsoft and selected communities in the left pane.

Luckily for me, there was already a community called All company. I chose this as my official company group for company-wide announcements/discussions.

Now I had to get groups for specific departments. I selected create new and chose communities. I then named the communities respectively to the departments and added users as per my csv file. I made these communities private so only members of the specific departments could access them.

Lastly, I had to ensure compliance with the companies social media policy. To do this, I decided it would be best to create a Data Loss Prevention policy to block sharing of sensitive info types on the Yammer platform.

I went back into Compliance center, selected Data Loss Prevention on the left pane and then policies and created a new policy to block sensitive info types. I applied it to all users and chose everywhere in 365 as the location for the policy to be applied. Hence, users in communities when sharing information will have their content blocked if it contains sensitive information.

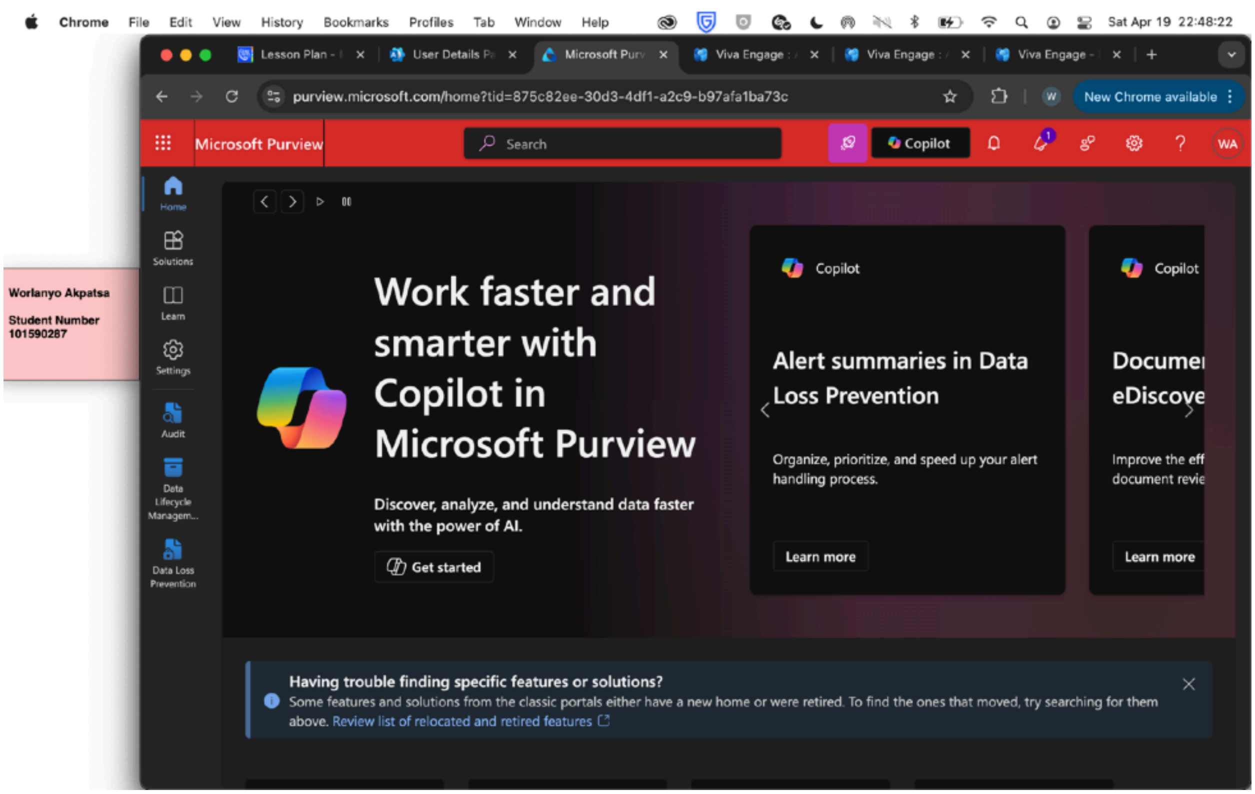
Even though this was quite long and tedious, I felt fulfilled after completing it.

TASK 4: MONITORING AND REPORTING

1: Configure Audit Logs

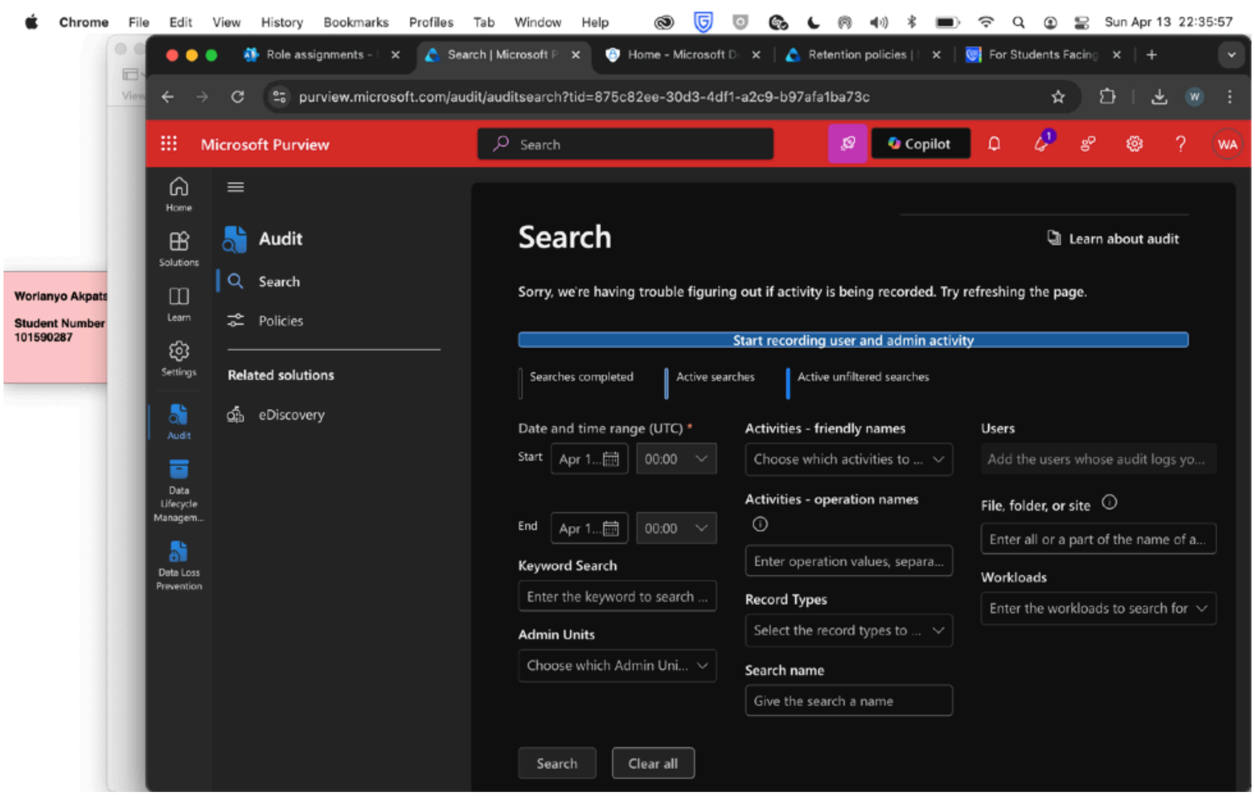
1.1: Enable and configure audit logging in 365 Compliance Center

A: Navigate to Compliance center homepage by selecting compliance under admin centers in 365 admin center



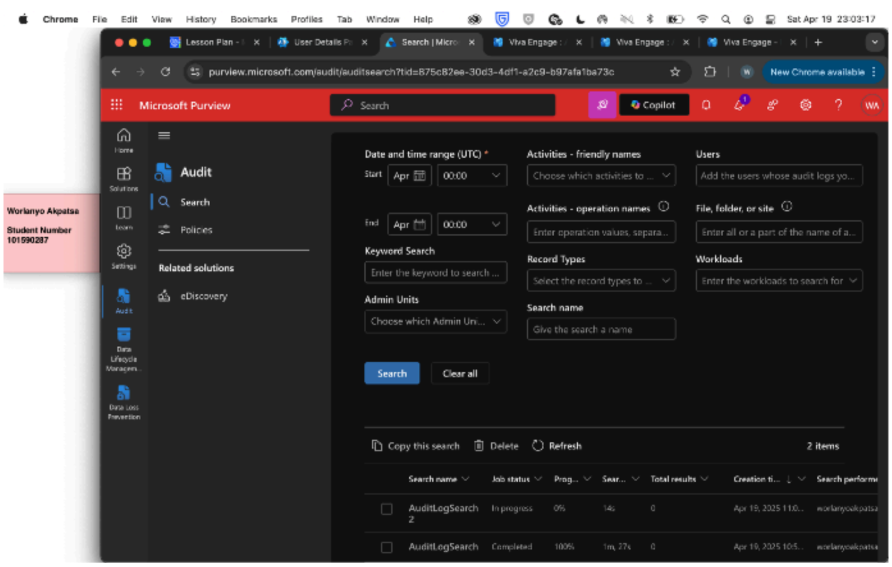
Student Name: Worlanyo Akpatsa Term: Winter 2025
Student ID: 101590287

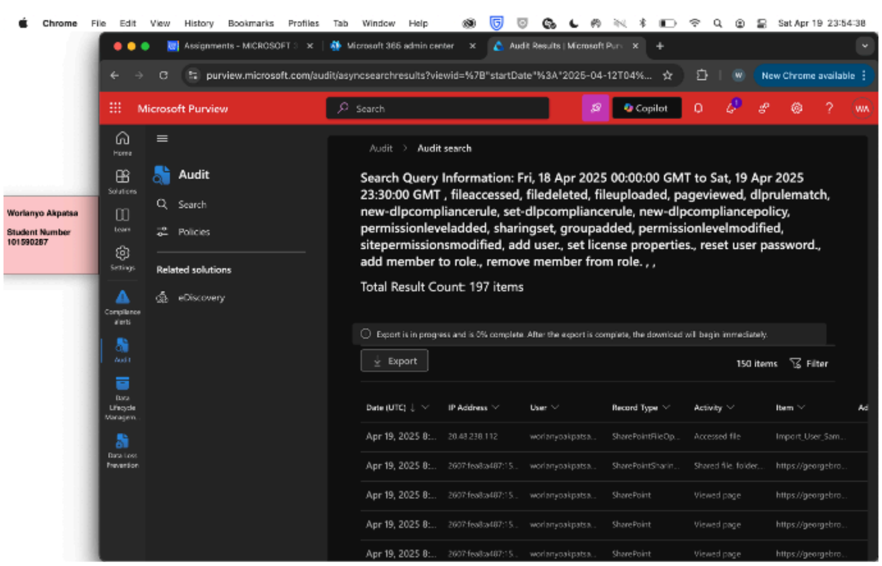
B: Select Audit in the left pane and enable auditing by clicking 'start recording user and admin activity"



1.2: Create a custom audit log search to track user activities related to at least one activity in Sharepoint such as updating site content

A: Select Audit->search and add custom activities and other preferences





~~~~~~

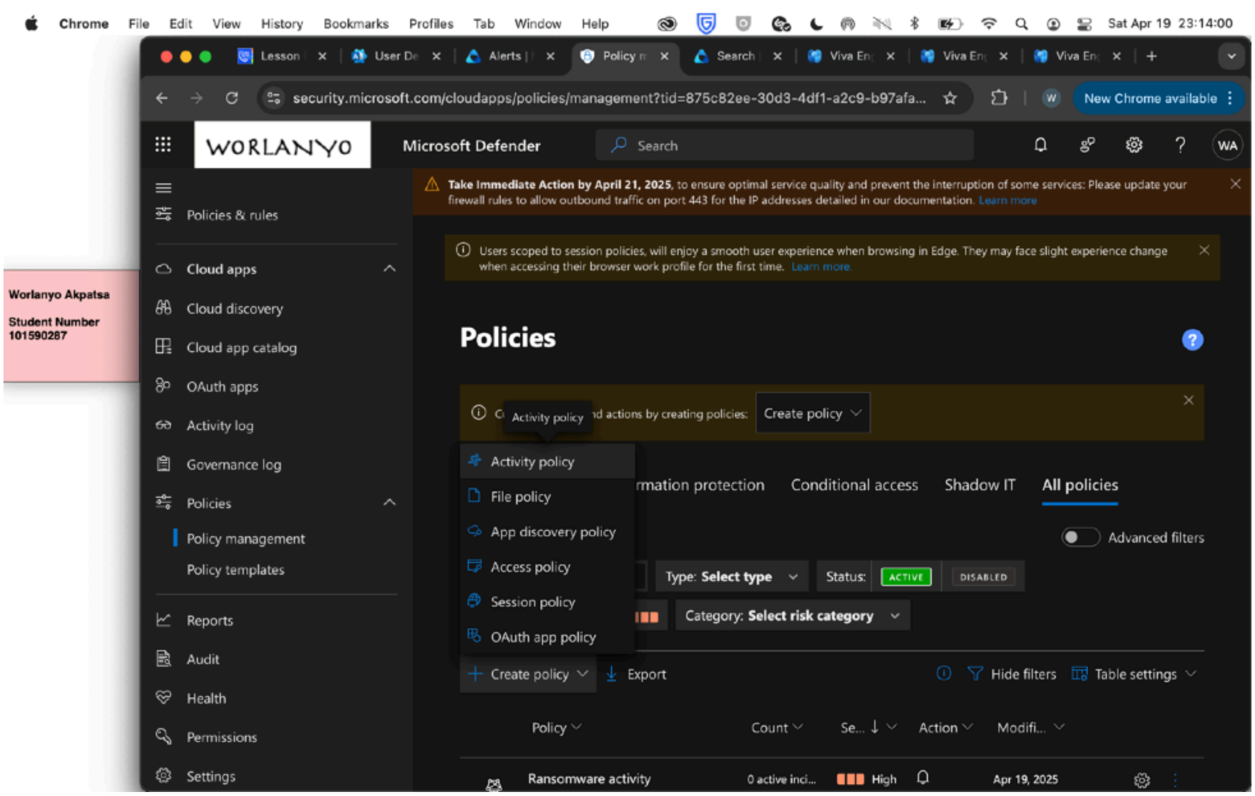
Student Name: Worlanyo Akpatsa Term: Winter 2025
Student ID: 101590287

~~~~~~

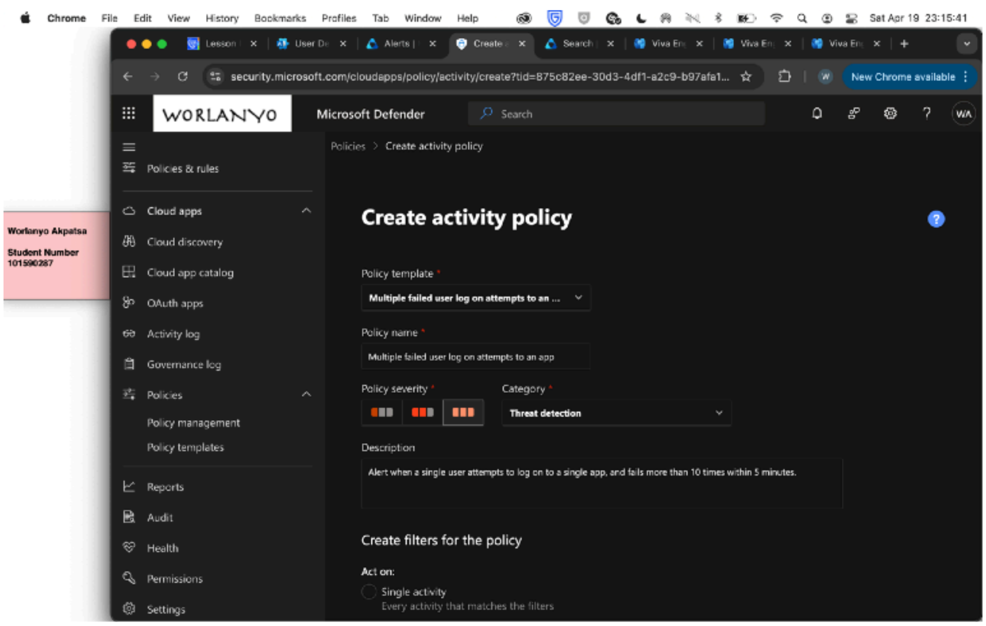
2: Set up Alerts

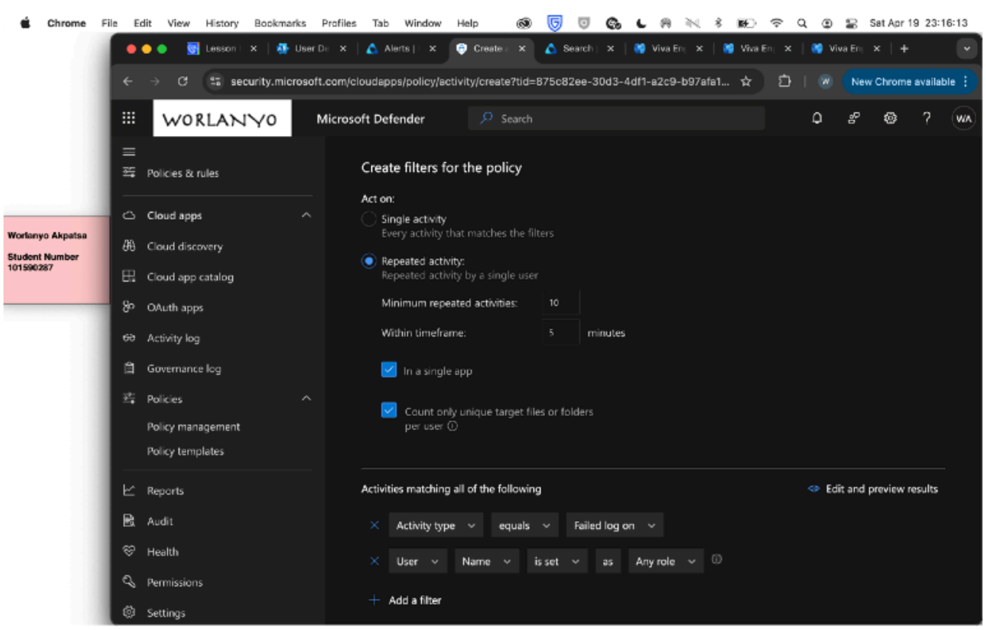
2.1: Configure alert policies to notify admins of suspicious activities

A: Navigate to Microsoft Defender, go to policies->policy management and create an activity alert



B: Select template (multiple failed user log in attempts) and configure further settings



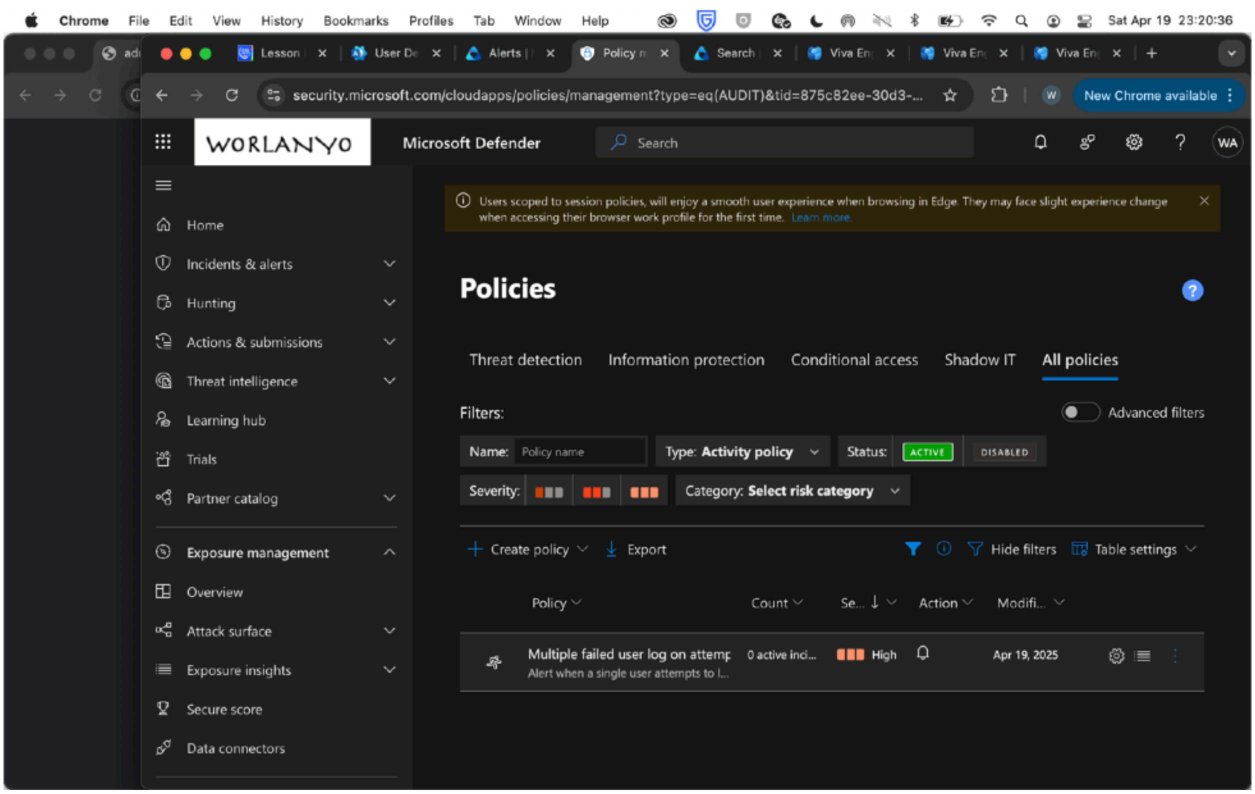


~ ~

Student Name: Worlanyo Akpatsa Term: Winter 2025
Student ID: 101590287

~~~~~~

Policy Created

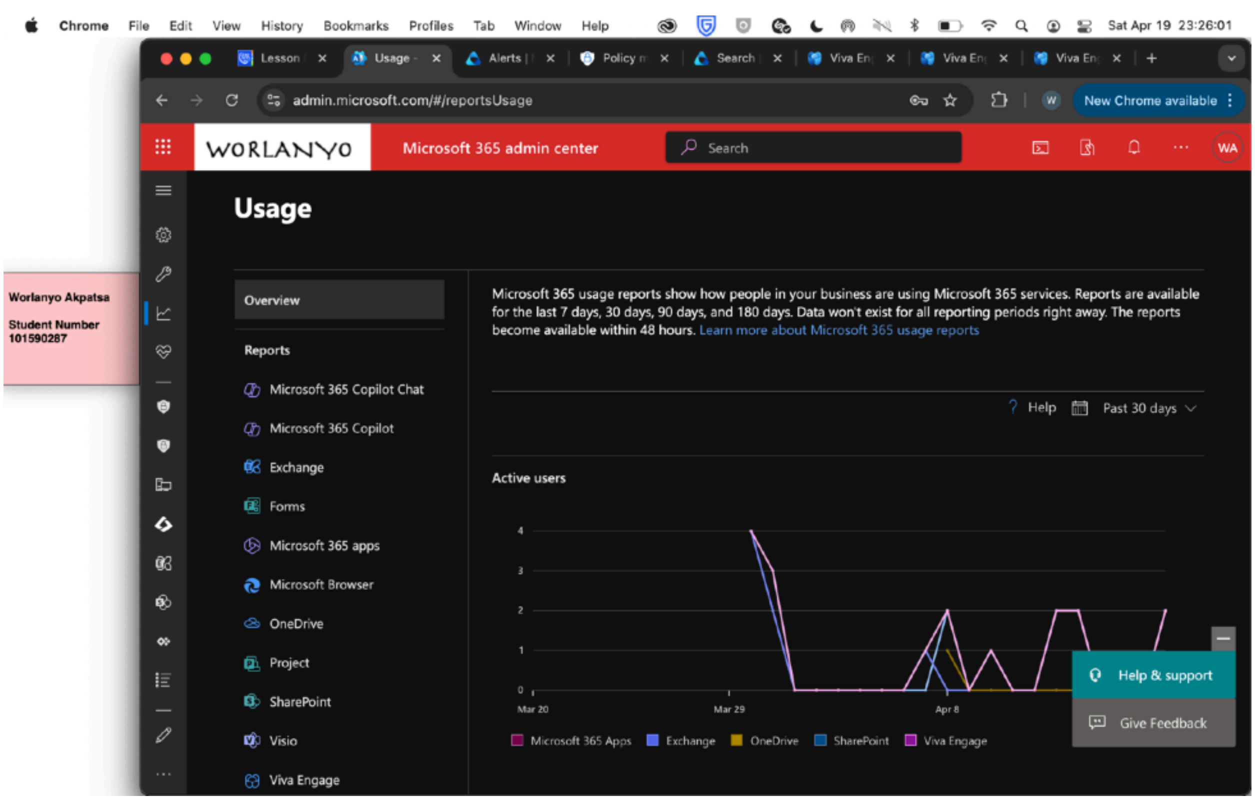

~~~~~~

Student Name: Worlanyo Akpatsa Term: Winter 2025
Student ID: 101590287

3: Generate User Reports

3.1: Use the 365 Admin Center to generate reports on user activity

A: Navigate to 365 Admin Center and choose reports->usage in the left pane



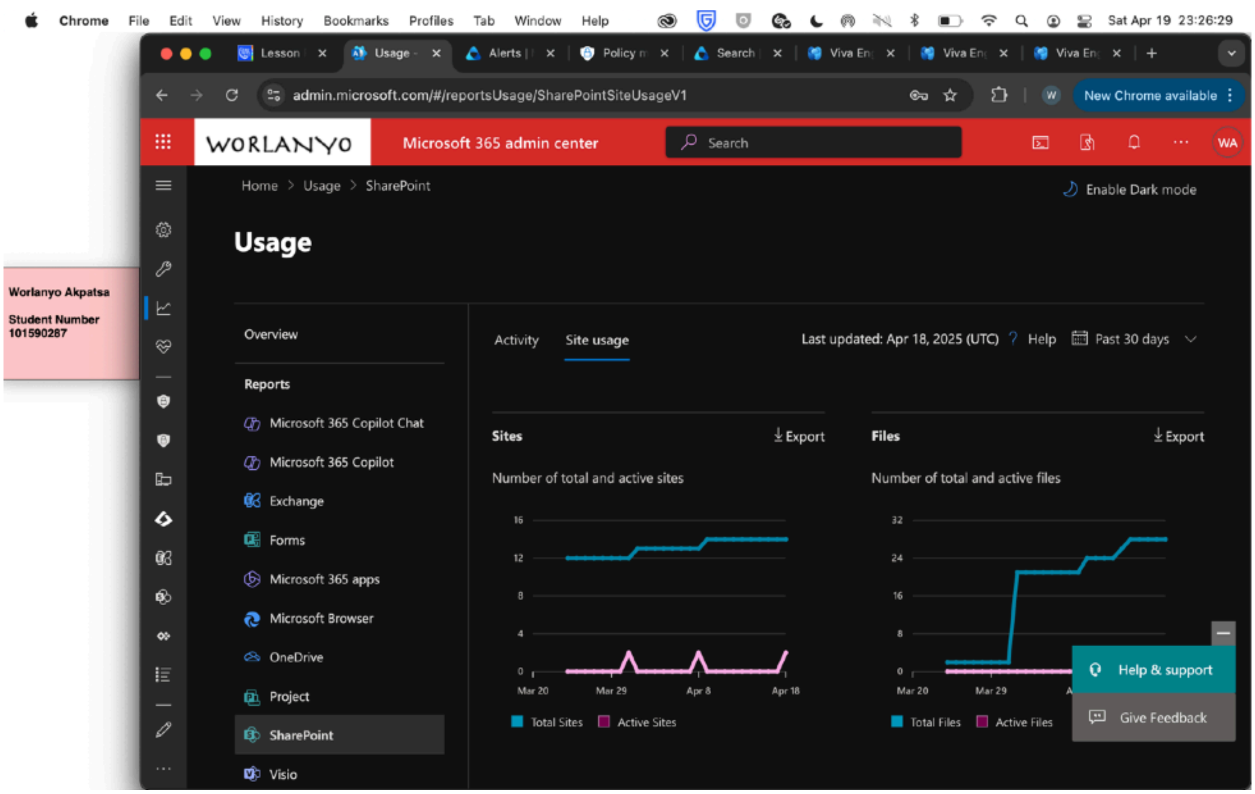
~~~~~~

Student Name: Worlanyo Akpatsa
Student ID: 101590287

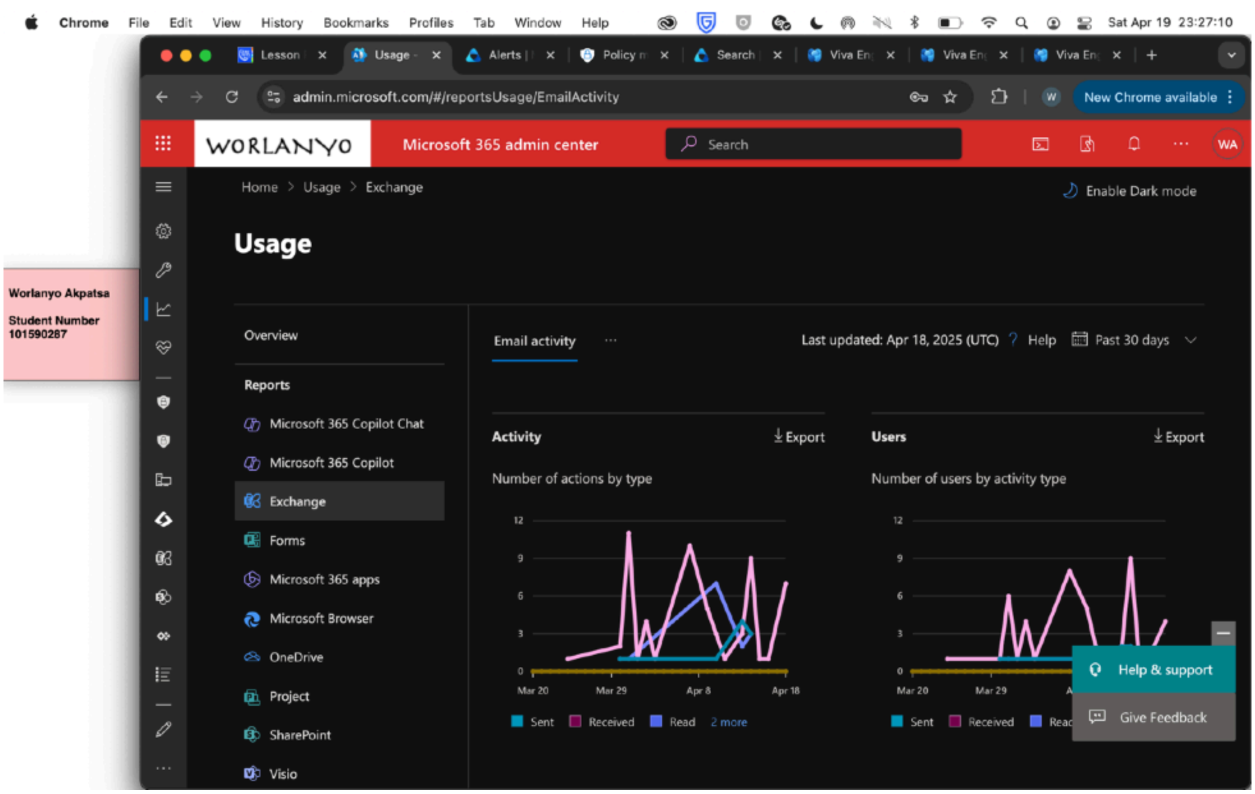
Term: Winter 2025

~~~~~~

B: SharePoint Site Usage



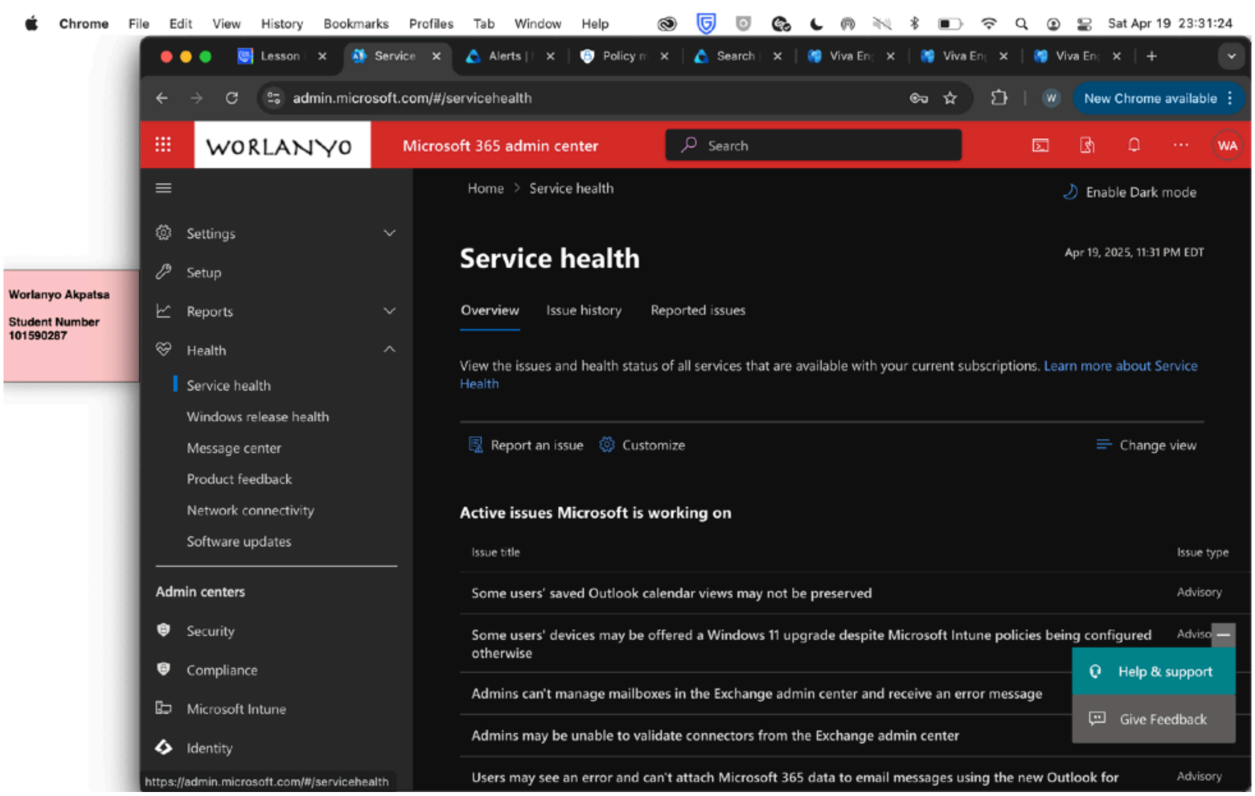
C: Email Usage



4: Implement and Monitor Service Health

4.1: Set up service health alerts to notify admins of any issues with Microsoft 365 services

A: Navigate to 365 Admin Center and select health->service health in the left pane

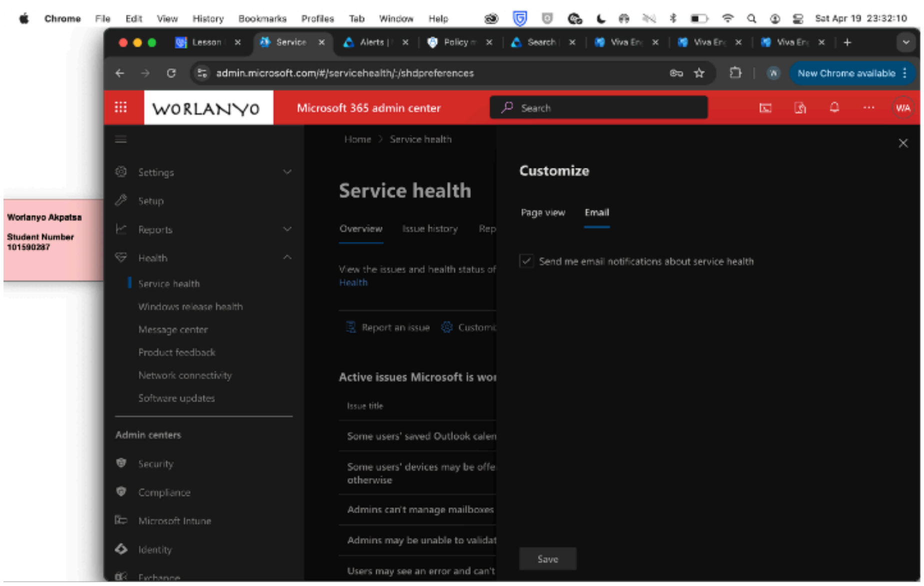


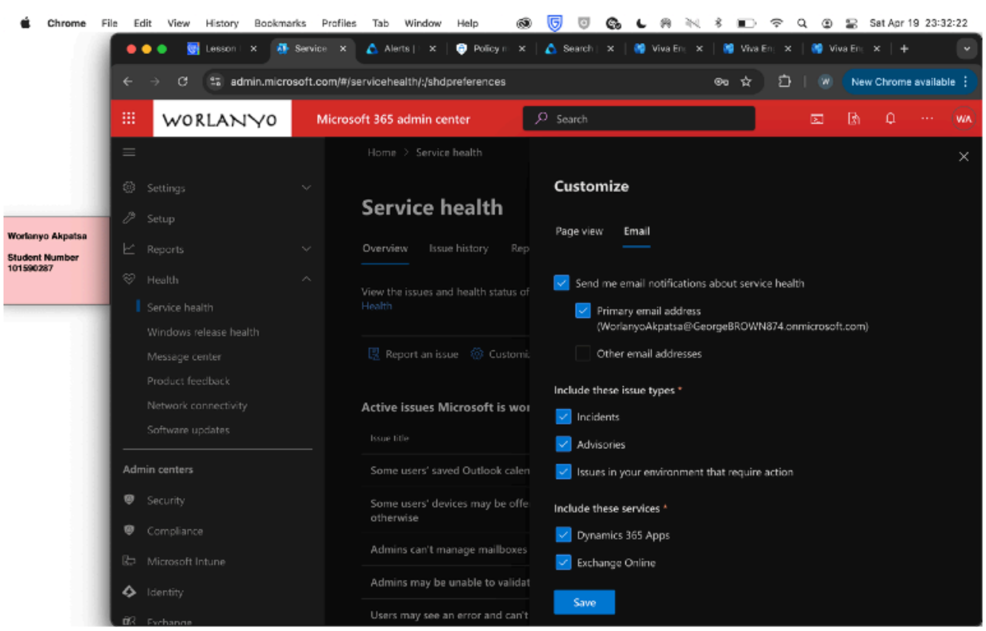
~~~~~~

Student Name: Worlanyo Akpatsa Term: Winter 2025
Student ID: 101590287

~~~~~~

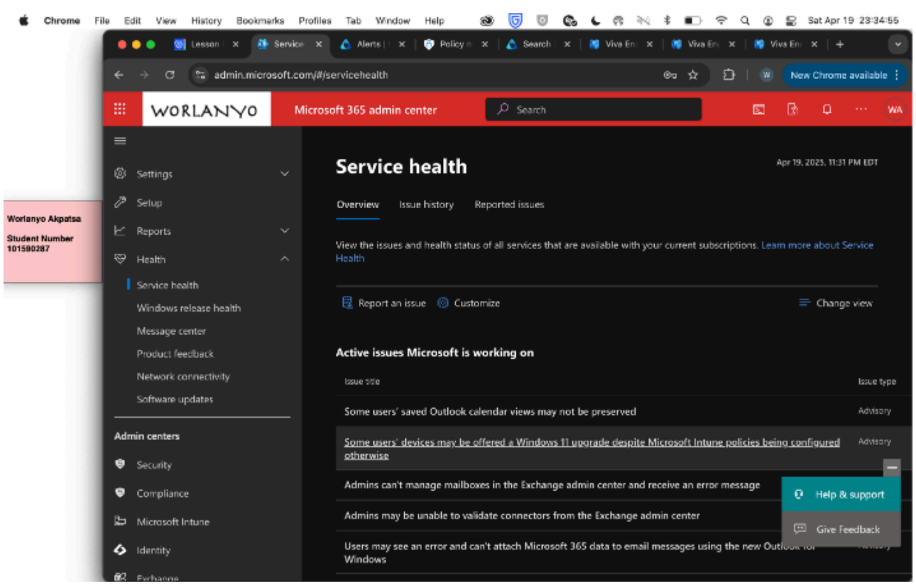
B: Click customize and set up email notifications about service health

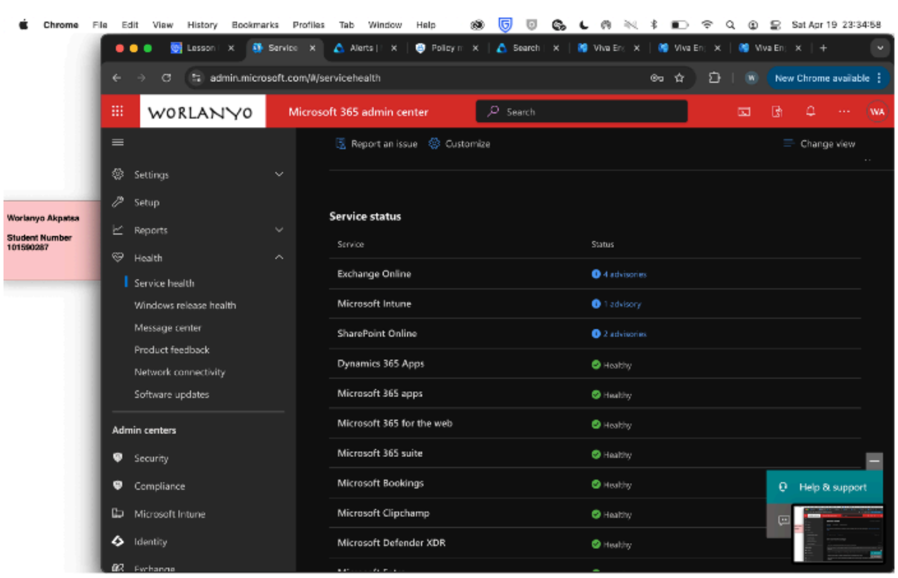




4.2: Monitor the Service Health Dashboard to ensure all services are running smoothly

A: Still in health->service health navigate through the different pages to see all reports on service health





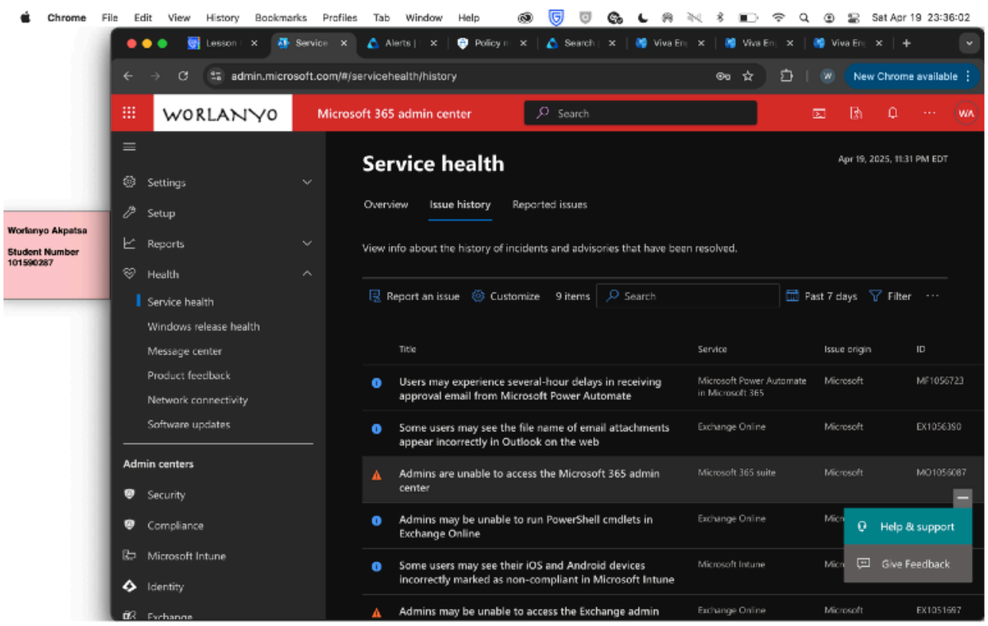
~~~~~~

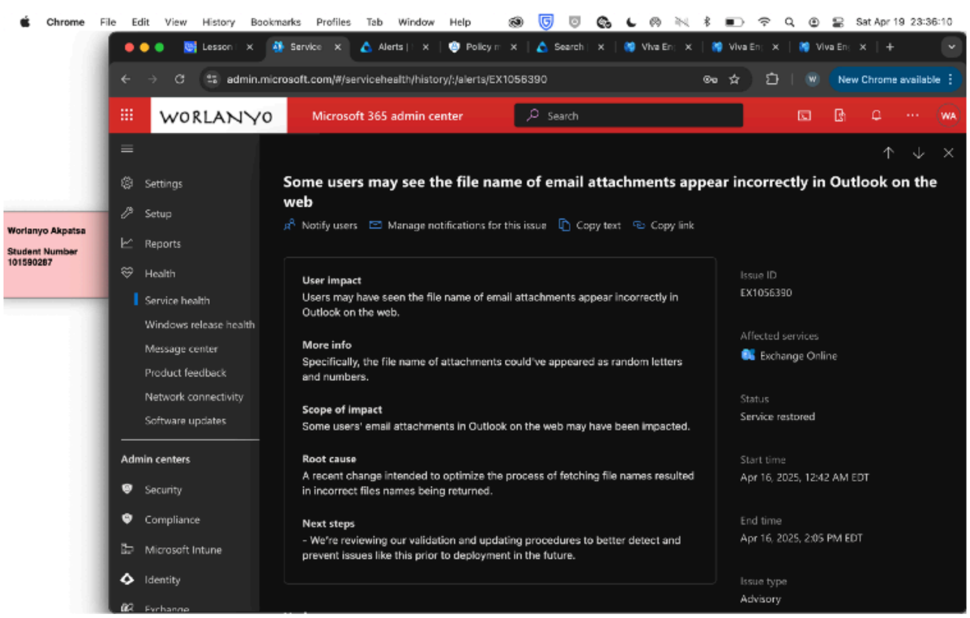
Student Name: Worlanyo Akpatsa
Student ID: 101590287

Term: Winter 2025

~~~~~~

More on service health





Task 4 Summary:

The last task was about monitoring and reporting which involved configuring audit logs, setting up alerts, generating usage reports and then implementing and monitoring service health. I learnt a lot from this.

To audit logs, one has to use the Compliance Center. While in the compliance center, I clicked on audit in the left pane and enabled auditing by clicking " start recording user and admin activity ". Then on the same page, I created two custom searches which included activities I had done earlier such as creating a user, a DLP policy, creating a site, uploading documents, engaging in added communities, etc.

I made sure to log in as one of the created users to do all these things too to generate some activity.

Next in this task, I had to create an alert to notify admins of suspicious activity. I used the MS defender and created an activity policy which detected multiple failed user sign in attempts. I tried to log in unsuccessfully more than 5 times (my setting) to see if it showed in alerts however it didn't. This is probably because alerts and policies take quite long to register.

After doing this, it was time for me to generate my user reports. I have done this before so it was a breeze. I navigated to 365 Admin Center and chose reports->usage in the left pane. This showed visual representation of all user activity on every single 365 platform. I was able to see a general overview of user reports and also detailed reports for specific platforms such as Sharepoint sites and exchange. This was really cool to do.

Finally, the last task of the activity; implementing and monitoring service health. Thankfully, it was easy just like the user reports because I used it quite frequently in my free time when using 365 Admin Center.

I had to navigate to health->service health in the left pane of the 365 Admin Center and this shows all the issues and health status of the services available in 365. I was able to see issue history, reported issues as well as an overview of my service health in general.

It was good to see and configure it again.

I am so glad to have done this class because it has taught me a new skill in Microsoft 365 I never thought I would have. I now have basic understanding of Microsoft 365 and how private companies and domains operate behind the scenes.

It is funny that after doing this, I just realized that the school, George Brown probably has a 365 subscription which is why all our emails are targeted to one domain. Something interesting I noticed.

All in all, I enjoyed this wonderful class.