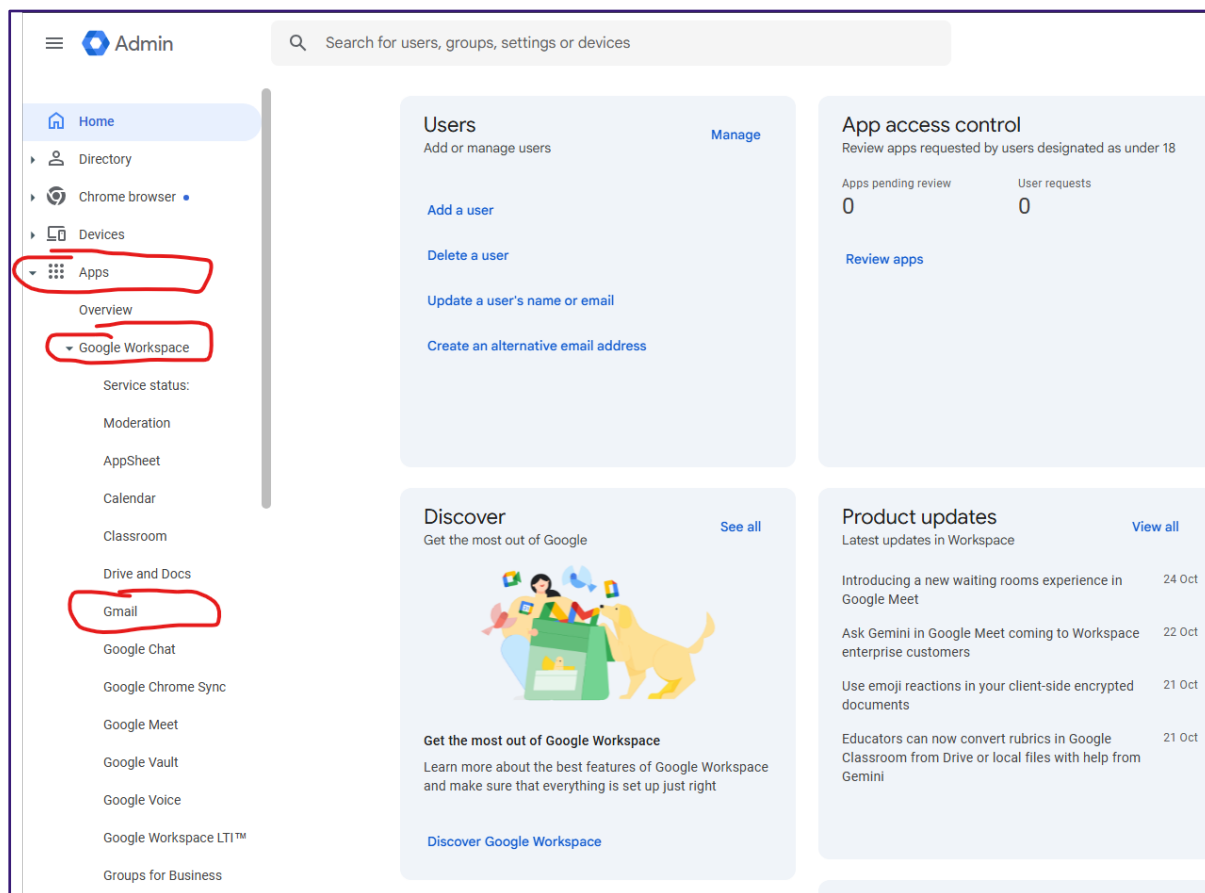


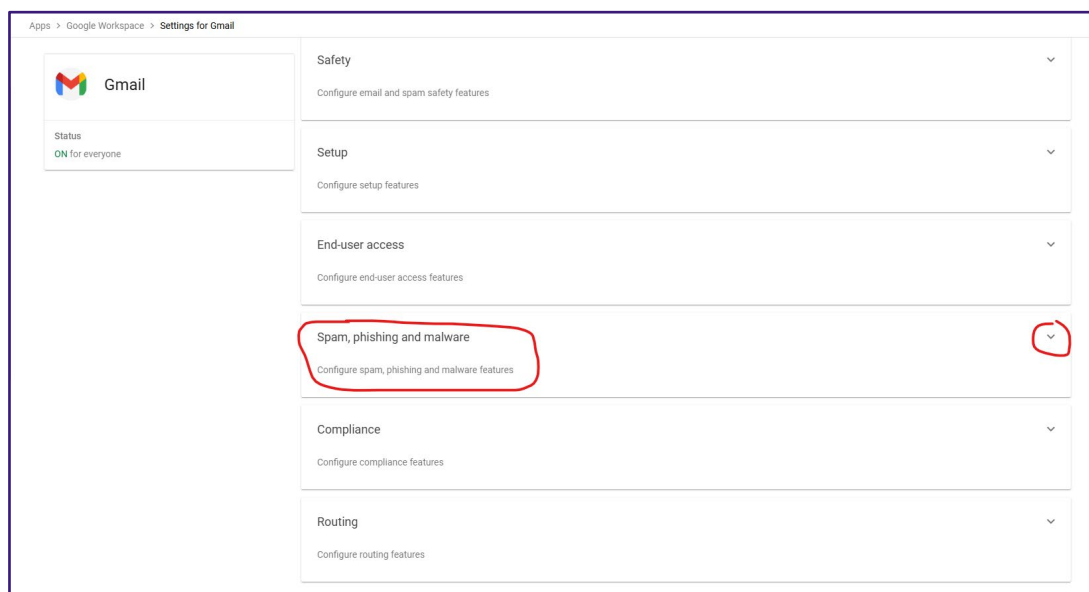


Google whitelist guide

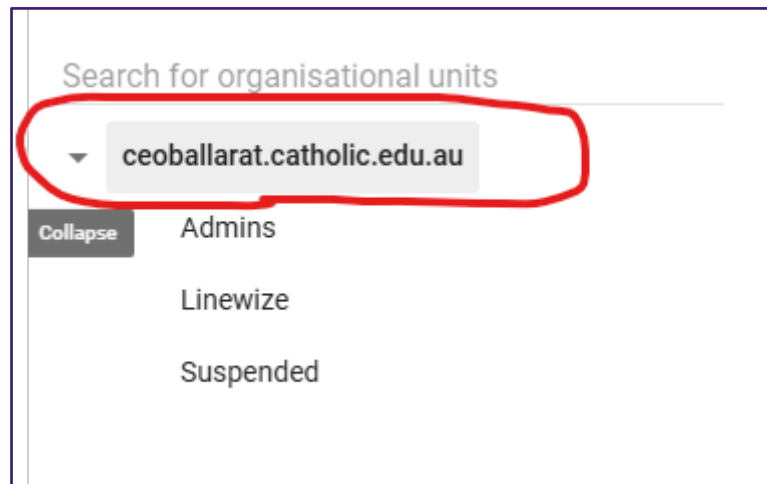
From the home page of Google Admin navigate to:
Apps > Google Workspace > Gmail



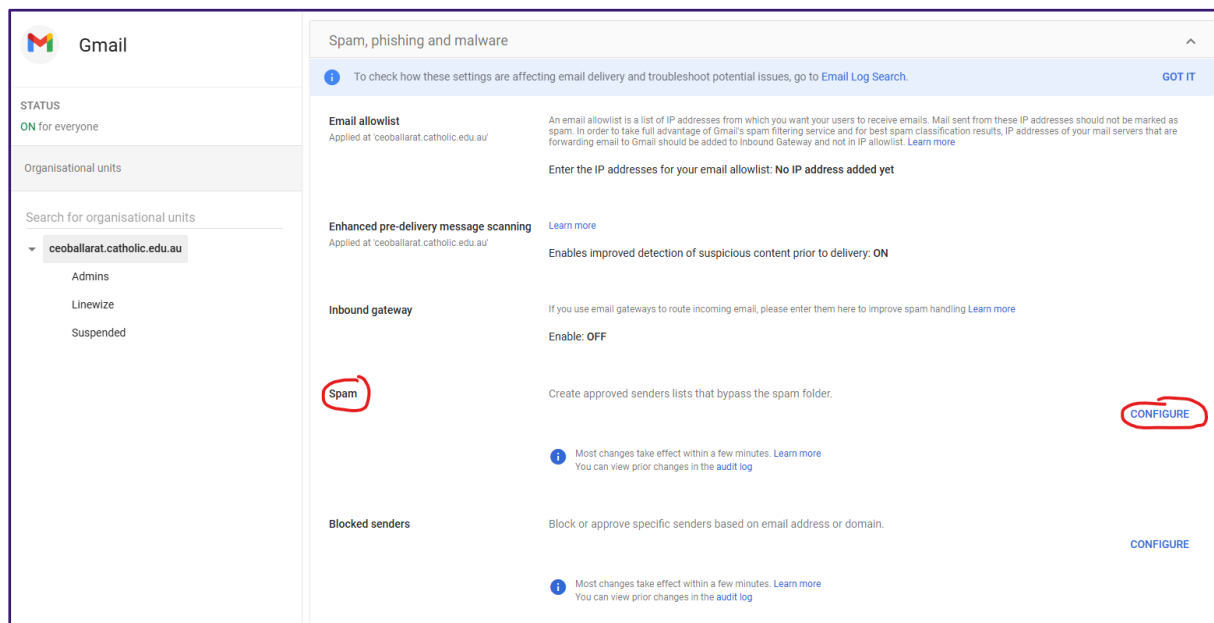
1) Scroll down and Navigate to 'Spam, phishing and malware' and expand the arrow



2) Select the Parent Organisational Unit



3) In the Spam section, click Configure on the right-hand side.



- 4) Under 'Options to bypass filters and warning banners' ensure the following boxes are selected and click 'Create or edit list'.

Add setting

Required. Enter a short description that will appear within the setting's summary.

All incoming messages are subjected to Google's spam filters. Messages that are detected as spam are automatically placed in the Spam folder.

Options

☐ Be more aggressive when filtering spam.

☐ Put spam in administrative quarantine

Default ▾

Options to bypass filters and warning banners

☒ Bypass spam filters for internal senders.

☒ Bypass spam filters for messages from senders or domains in selected lists.

No lists used yet.
[Use existing list](#) [Create or edit list](#)

☒ Bypass spam filters and hide warnings for messages from senders or domains in selected lists.

No lists used yet.
[Use existing list](#) [Create or edit list](#)

☐ Bypass spam filters and hide warnings for all messages from internal and external senders (not recommended).

CANCEL **SAVE**

- 5) Click 'ADD ADDRESS LIST'

**Gmail**

STATUS
ON for everyone

Manage address lists

Name	Type	Address count	Actions
ADD ADDRESS LIST			

Most changes take effect within a few minutes. [Learn more](#)
You can view prior changes in the [audit log](#)

6) Under Name* : Enter a name for the list – SIMON MFA

Add the email address to whitelist: eg otp@simonschools.net.

Click SAVE

The screenshot shows the 'Add address list' form. The 'Name *' field is circled in red and contains the text 'SIMON MFA'. Below it, a red arrow points from the 'ADD ADDRESS' button to the 'Address' field, which contains 'otp@simonschools.net'. The 'ADD ADDRESS' button is also circled in red. The form includes a search bar, a table with columns 'Address' and 'Authentication required (received mail only)', and a toggle switch. At the bottom, there are 'BULK-ADD ADDRESSES' and 'ADD ADDRESS' buttons, an information icon with text, and 'CANCEL' and 'SAVE' buttons.

Add address list

Name *

SIMON MFA

This field is required

Search address

Address

Authentication required (received mail only) [Learn more](#)

otp@simonschools.net

BULK-ADD ADDRESSES

ADD ADDRESS

i Most changes take effect within a few minutes. [Learn more](#)
You can view prior changes in the [audit log](#)

CANCEL SAVE

7) Return to the 'Spam, Phishing and Malware' page

Name the setting at the top

The screenshot shows the 'Spam, Phishing and Malware' page. The 'Spam' tab is selected, and the 'SIMON MFA' setting is visible. The page includes a 'Learn more' link and a description of spam filters.

Spam [Learn more](#)

SIMON MFA

All incoming messages are subjected to Google's spam filters. Messages that are detected as spam are automatically placed in the Spam folder.

- 8) Under "Options to bypass filters and warning banners," select Use existing list and choose your newly created list.

Options to bypass filters and warning banners

☒ Bypass spam filters for internal senders.

☒ Bypass spam filters for messages from senders or domains in selected lists.

No lists used yet.

[Use existing list](#) [Create or edit list](#)

☒ Bypass spam filters and hide warnings for messages from senders or domains in selected lists.

No lists used yet.

[Use existing list](#) [Create or edit list](#)

- 9) Click the X in the top left corner once you have highlighted the list.

× Select address lists

☒	Address list name	Number of addresses
☒	SIMON MFA	1

10) Repeat for 'Bypass spam filters and hide warnings for messages from senders or domains in selected lists.

Click SAVE

Options to bypass filters and warning banners

☒ Bypass spam filters for internal senders.

☒ Bypass spam filters for messages from senders or domains in selected lists.

SIMON MFA (1)

Don't use

[Use existing list](#) [Create or edit list](#)

☒ Bypass spam filters and hide warnings for messages from senders or domains in selected lists.

SIMON MFA (1)

Don't use

[Use existing list](#) [Create or edit list](#)

☐ Bypass spam filters and hide warnings for all messages from internal and external senders (not recommended).

CANCEL

SAVE

11) Confirm the rule appears as expected in the Spam settings

Spam						
	Description	STATUS	Source	Actions	ID	Values
	SIMON MFA	Enabled	Locally applied	Edit - Disable - Delete	fa2e6	Aggressive spam filtering: OFF Bypass internal senders: ON Bypass approved senders: ON Bypass approved senders and hide warning banners: ON Bypass spam filtering and hide warning banners: OFF Quarantine message: OFF
ADD ANOTHER RULE						
Most changes take effect within a few minutes. Learn more You can view prior changes in the audit log						