

## DMA Parent Guide – Option A

## Version history

<i>Version</i>	<i>Date</i>	<i>Change log</i>
1.0	25 February 2022	Initial Version
1.1	XX April 2023	Updates to document: <ol style="list-style-type: none"><li>1. Additional information and updates in Unit 2-1, 2-2 &amp; 2-4</li><li>2. Added Unit 2-3 for instructions on (2FA) Google Authentication</li></ol>

<b>Chapter 1: Introduction</b>	<b>4</b>
<b>Chapter 2: Getting Started</b>	<b>5</b>
Unit 2-1 - Onboarding your account	6
Unit 2-2 - Sign-In	8
Unit 2-3 - Reset Password	11
Unit 2-4 - 2FA Google Authentication	13
<b>Chapter 3: Parent Portal User Interface Overview</b>	<b>14</b>
Unit 3-1 - Dashboard	14
Unit 3-2 - Card Layout	15
Unit 3-3 - Device Details	17
Unit 3-4 - Webfilter Reports	20
<b>Chapter 4: Option A Functions</b>	<b>22</b>
Unit 4-1 - Managing Web Content	22
URL Tester	23
Custom Web Filter	25
YouTube Filter	32
Removing Custom Web Filter	33
Unit 4-2 - Blocking your child's device	34
Unit 4-3 - Sleep Hours	37
Unit 4-4 - Rules	38
Step 1 - Creating a Schedule	38
Step 2 - Creating a Rule	40
Step 2.1 Overwrite School Sleep Hours	42
Step 2.2 Setting Up Web Filter Rules	46
Unit 4-5 - Viewing Reports	53
<b>Chapter 5: Application Installation</b>	<b>56</b>
Unit 5-1 - Chromebooks	56
Unit 5-2 - iPads	60
Installing iPad apps	64
Uninstalling iPad apps	68
Disabling the App Store	71
<b>Troubleshooting Guide</b>	<b>72</b>

## Chapter 1: Introduction

This guide is written for parents of students who have devices enrolled into the Device Management Application (DMA) programme under the Ministry of Education (MOE).

It describes the functions that you, as a parent, have access to. There are three options that are presented to parents to manage your child's device after school hours:

### **Default Option**

As the name implies, you will be placed on this option if you did not choose from the next two options. This option basically presents you with a dashboard from which you can view your child's/ward's browsing activity.

### **Option A**

If you wish to have more flexibility with the device, you can select Option A where you can choose to install applications and customize your child's/ward's sleep timing while retaining the web filtering function to protect your child from unsafe content.

### **Option B**

Parents who wish to have total control of the device after school hours can select Option B. In addition to having the ability to install applications of choice, all browsing activities on the device are not logged when under Option B.

It is important to note that by not logging browsing activities, there is no content filtering to filter unsafe contents for the child/ward. There are also no imposed sleep hours on the devices meaning that the child/ward will be able to use the device at any time after school hours.

**If you have any questions, please contact your respective school's DMA Administrator.**

## **Chapter 2: Getting Started**

When the programme becomes available, you will, by default, be placed under the **Default Option** group unless you inform the school of your choice of either the **Option A** or **Option B** group.

If you are on **Option A** or **(opt-in) Default Option**, you will receive an email from Mobile Guardian informing you to set up your account after the school has provisioned the parent account for your child.

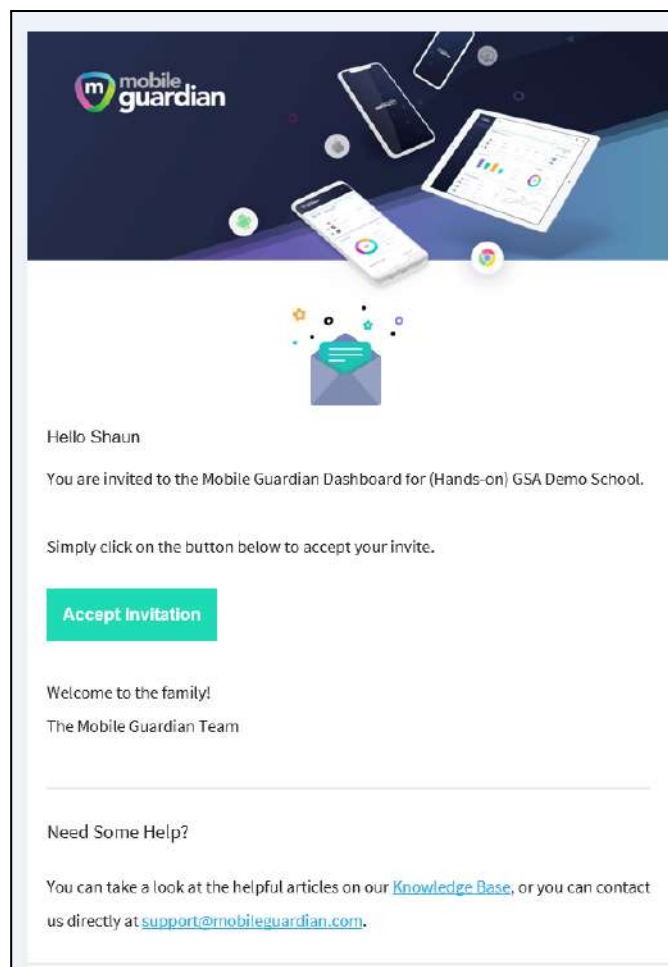


Figure 2.1 An example of the email that is sent to parents

Please check your **SPAM** folder if you do not see the email in your **INBOX**.

If you did not receive an email invitation, you may obtain an onboarding link from your child/ward's school.

## Unit 2-1 - Onboarding your account

Click on the “**Accept Invitation**” button, and your Web browser will launch the Mobile Guardian site to continue with the onboarding process.

You will then see the following Account Activation Page. Click the “**Accept Invitation**” button to activate your account (The token is different for each parent).

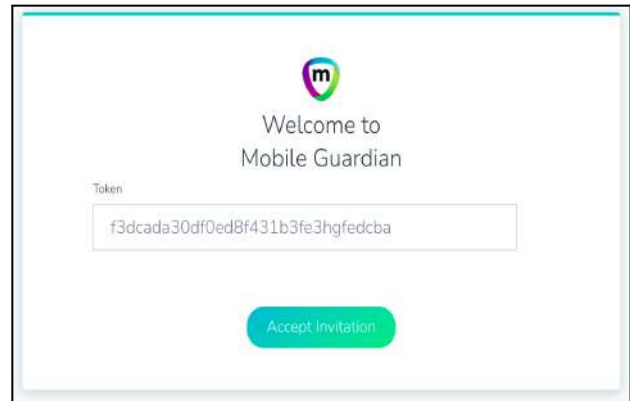


Figure 2.1.1: Account Activation Page

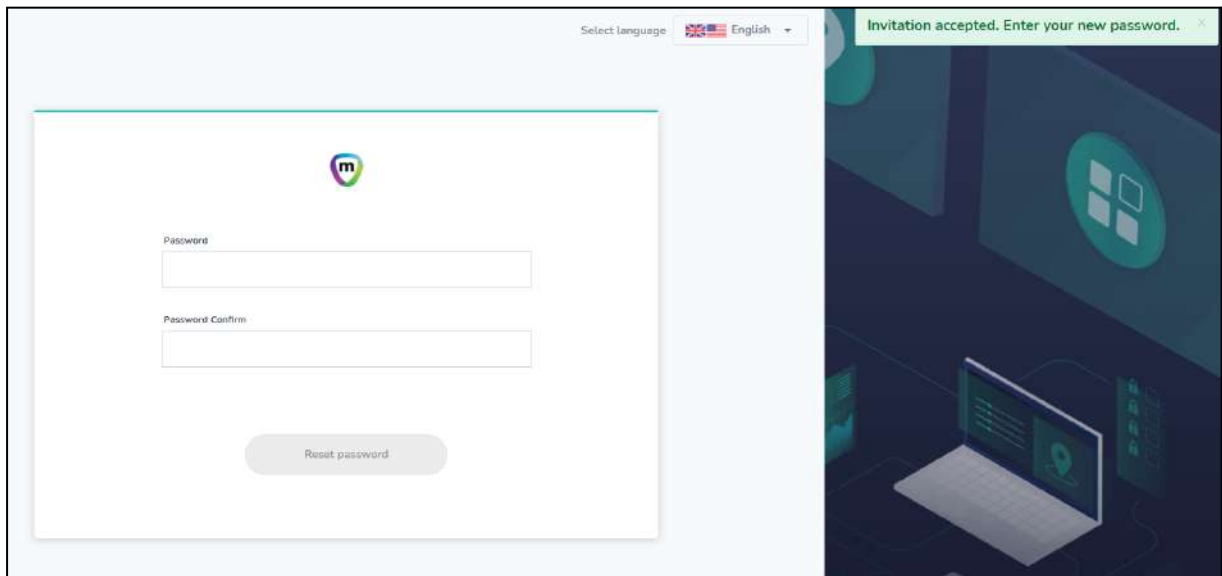
**Note:** Please inform your child/ward’s school to resend the email or send you a manual activation link if you did not receive the activation email.

**Not getting the Reset Password Page after accepting the invitation?**

Use the ‘Forget Password?’ link on the Login Page to reset your password.

You can also use this link: <https://sg-portal.mobileguardian.com/#/forgot-password>

In the next screen, at the top right corner, you will see a pop-up notice in green with the notification "**Invitation accepted. Enter your new password**".

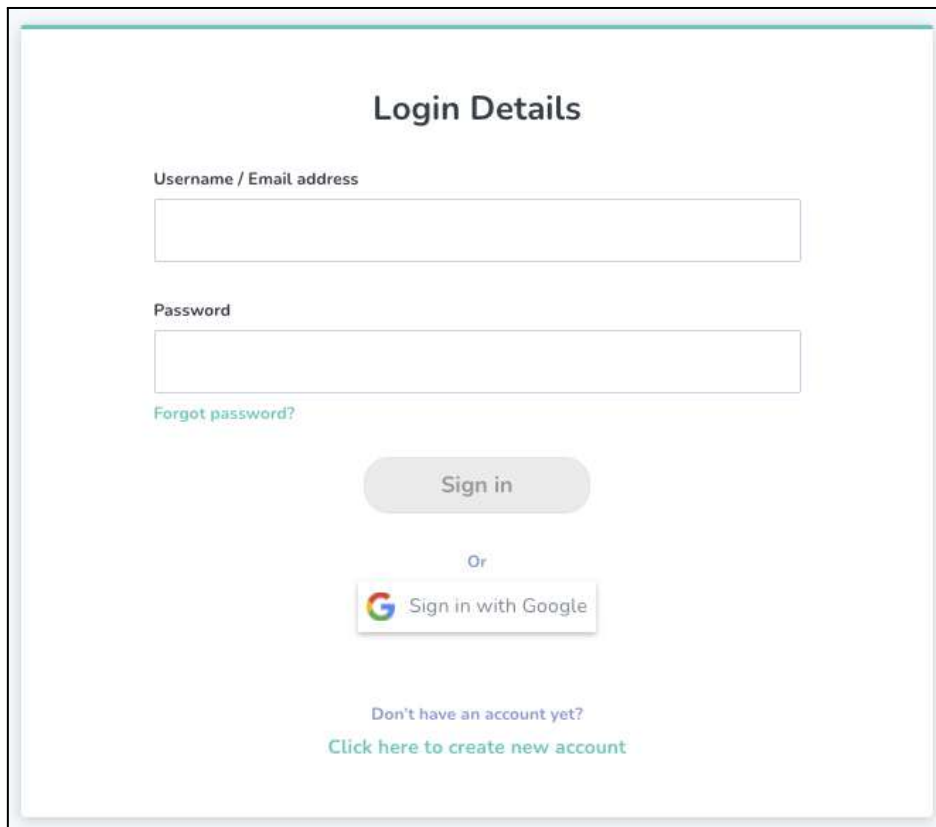


*Figure 2.1.2: Reset Password page*

**Note :** If you did not receive the Password Reset Page mentioned in the previous page. Please use the '**Forget Password ?**' link on the sign-in page to reset your password.

When done resetting your password, you will be brought back to the login screen, where you can enter your email address and your newly set password.

Sign in using the Username and Password fields.



The screenshot shows a login page titled "Login Details". It features two input fields: "Username / Email address" and "Password". Below the password field is a link "Forgot password?". A "Sign in" button is positioned below the links. Underneath the button is the word "Or" and a "Sign in with Google" button featuring the Google logo. At the bottom, there is a link "Click here to create new account" preceded by the text "Don't have an account yet?".

*Figure 2.1.3: Login Page*

**Note :** Please sign in using your email and password on this page.  
DO NOT use the “**Sign in with Google**” button as you might encounter unforeseen issues with your account.



## Unit 2-2 - Sign-In

Subsequently, when you need to sign in again, you can go to this URL directly:

<https://sg-portal.mobileguardian.com>

Alternatively, visit [www.mobileguardian.com](http://www.mobileguardian.com) and click "Login" near the top-right corner.



Figure 2.2.1: Link to login from [www.mobileguardian.com](http://www.mobileguardian.com)

Next, select “Asia-Pacific” as the location to sign into on the pop-up screen below.

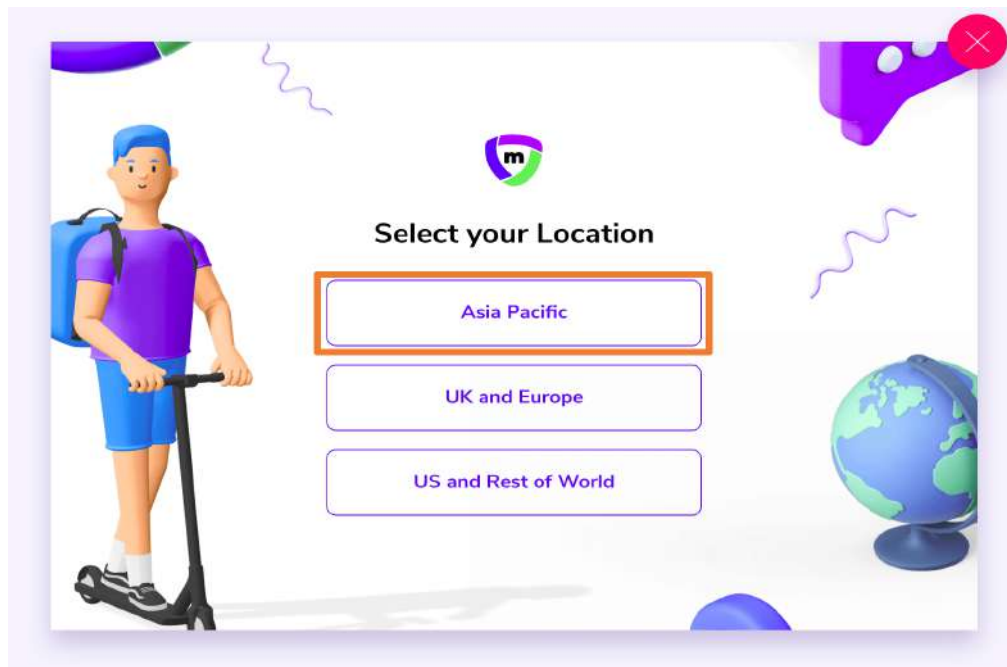
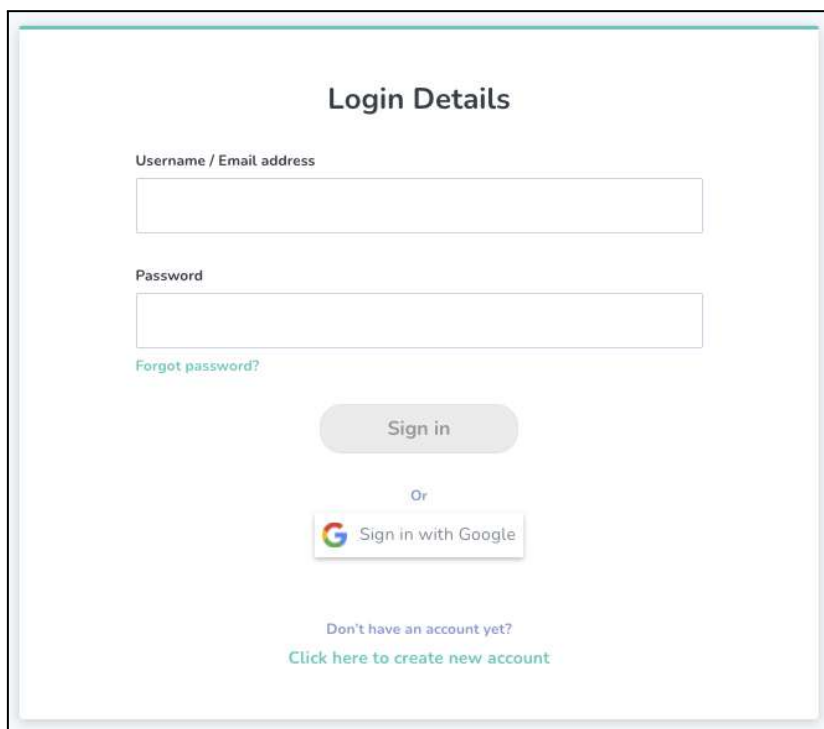


Figure 2.2.2: Selection of location on the Login Portal

Sign-in using the Username/Email Address and Password fields.

**Note :** Please do not use the “Sign in with Google” button, otherwise you might encounter an error.

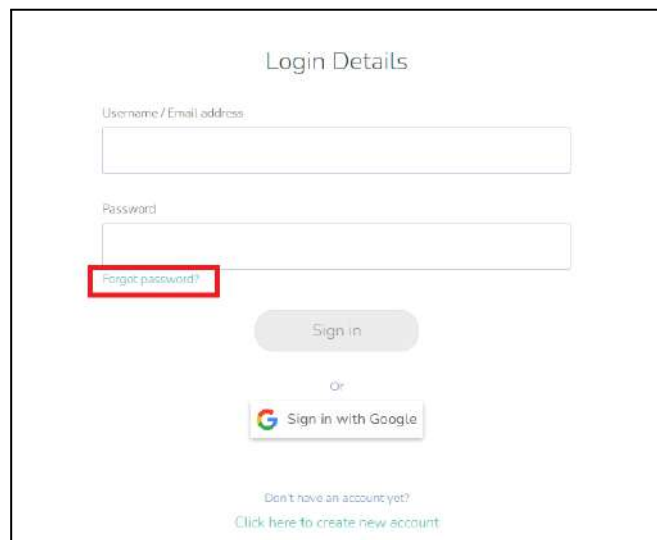


The screenshot shows the 'Login Details' page of the Mobile Guardian application. It features a title 'Login Details' at the top. Below the title are two input fields: 'Username / Email address' and 'Password'. A link 'Forgot password?' is positioned below the password field. A 'Sign in' button is centered below the input fields. Below the button is the word 'Or'. Underneath 'Or' is a 'Sign in with Google' button, which includes the Google logo. At the bottom of the page, there is a link 'Click here to create new account' preceded by the text 'Don't have an account yet?'.

Figure 2.2.3: Login Page

## Unit 2-3 - Reset Password

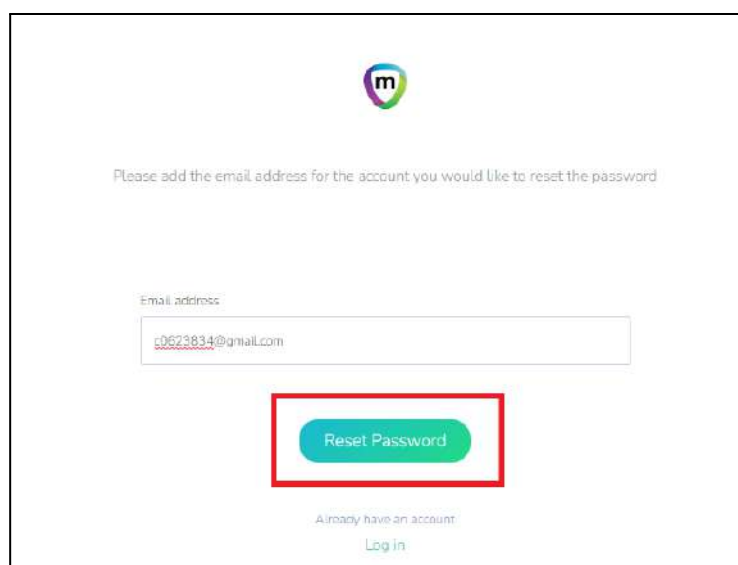
If you have forgotten your password or do not see the Reset Password page while activating your account, you may click on “Forgot password?” to reset your password.



The image shows a login form titled "Login Details". It contains two input fields: "Username / Email address" and "Password". Below the password field is a link labeled "Forgot password?" which is highlighted with a red rectangular box. Below the input fields is a "Sign in" button. Underneath the button is the word "Or" and a "Sign in with Google" button. At the bottom of the form, there is a link that says "Don't have an account yet? Click here to create new account".

Figure 2.3.1: “Forgot password?” link in the Login Page

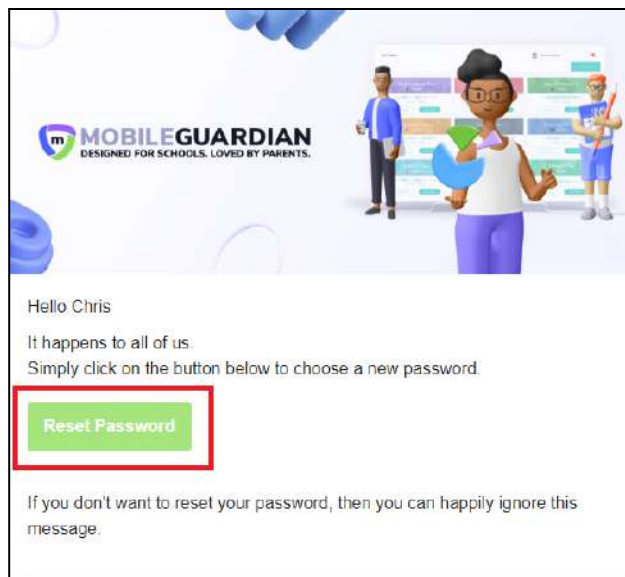
Enter your email address and click on the **Reset Password button**. You will receive an email alert in your designated email inbox.



The image shows a screen for resetting a password. At the top is the mobile guardian logo. Below it is the text "Please add the email address for the account you would like to reset the password". There is an input field labeled "Email address" containing the text "c0623834@gmail.com". Below the input field is a green button labeled "Reset Password" which is highlighted with a red rectangular box. At the bottom of the screen, there is a link that says "Already have an account? Log in".

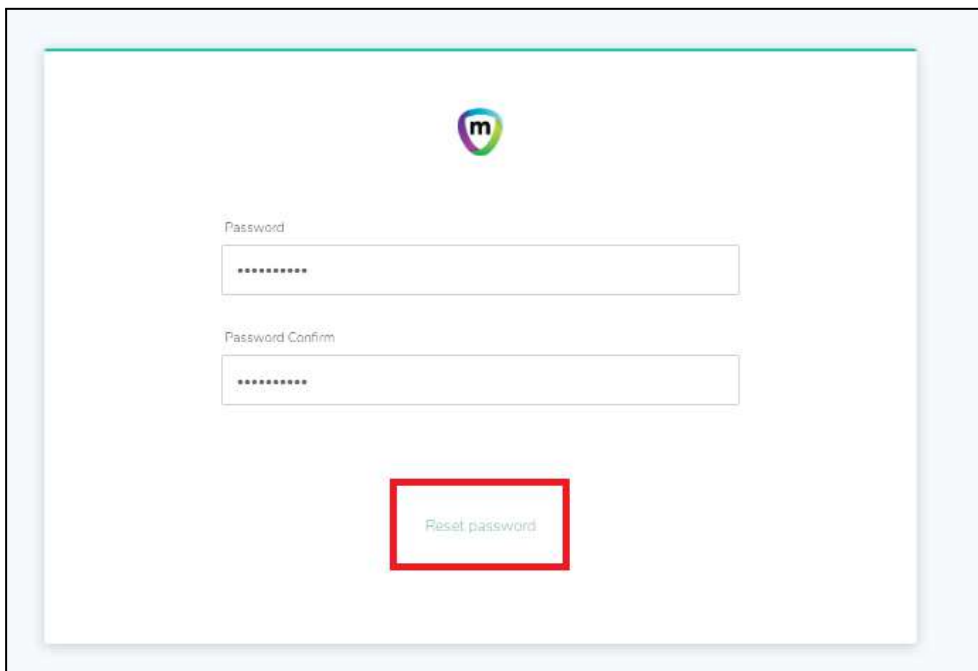
Figure 2.3.2: Prompt screen to enter email address for password reset

Click the **Reset password** button shown in the email.



*Figure 2.3.3: Reset Password Email*

Enter the new password twice and click on the **Reset password** button.

A screenshot of the Mobile Guardian password reset interface. At the top center is the Mobile Guardian logo. Below the logo are two input fields: "Password" and "Password Confirm". Both fields contain a series of asterisks (\*\*\*\*\*). Below these fields is a green button with the text "Reset password", which is highlighted with a red rectangular border.

*Figure 2.3.4: Reset Password Interface*

Once the reset is completed, you will be brought to the login page to sign in.

## Unit 2-4 - 2FA Google Authentication

Once you are signed in to the dashboard, you will see the home screen containing the parent's details on the bottom left.

**Note :** Do not activate the Google authenticator (2FA). Once it is activated, you will be asked to enter Google Authentication code (2FA) on the login page each time you login to your parent account. You will not be able to login into your account if you do not have the Google authenticator code.

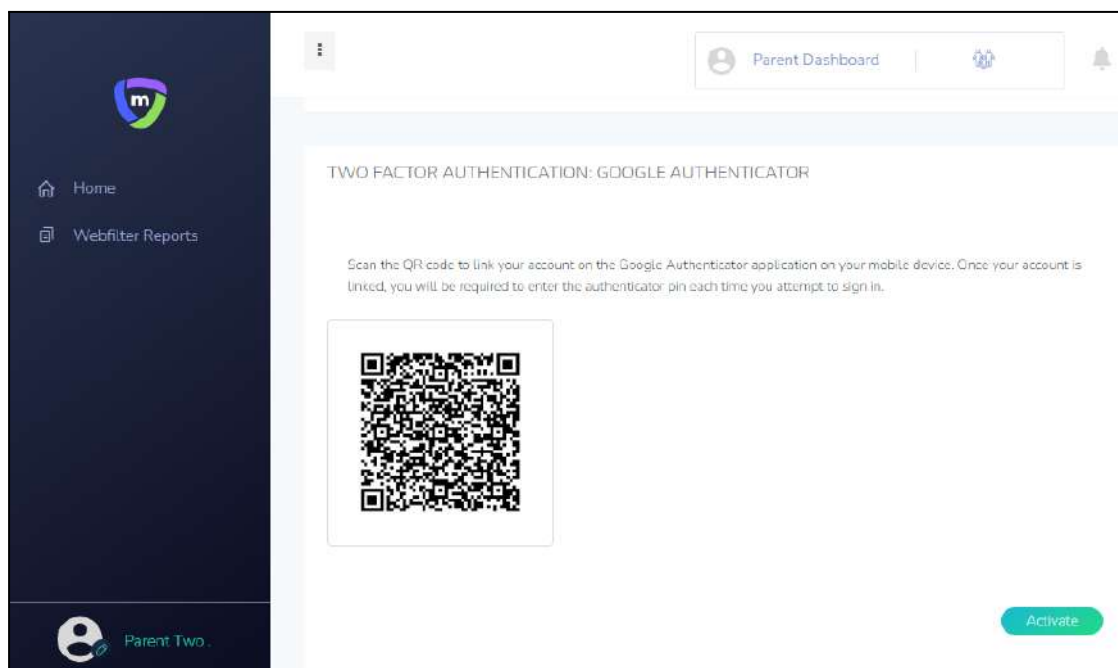


Figure 2.4.1: Google Authenticator (2FA) screen

## Chapter 3: Parent Portal User Interface Overview

The functions available under the Option A dashboard are described below.

### Unit 3-1 - Dashboard

Once you are signed-in to the dashboard, you will see the Home screen containing a card of your child/ward. The parent dashboard will have the "**Schedules**" and "**Block**" functions (circled below).

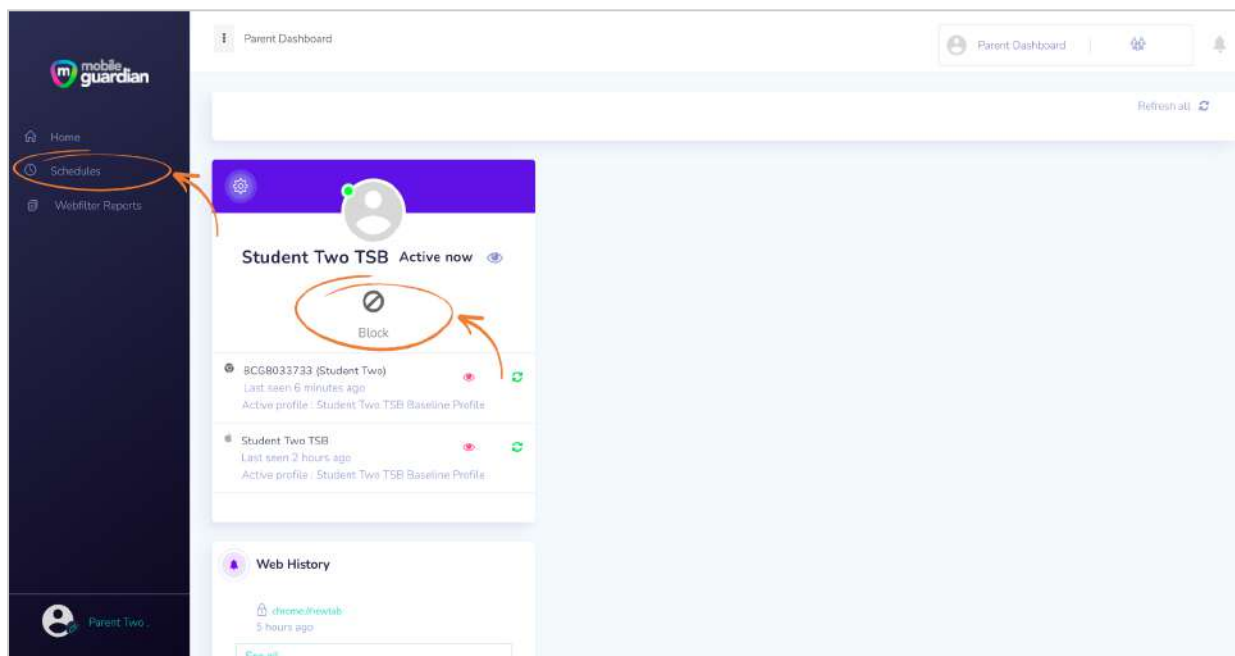


Figure 3.1.1: Option A Dashboard

## Unit 3-2 - Card Layout

Each child/ward is represented in the parent dashboard using a card layout. This section describes the various buttons and information contained in the card.

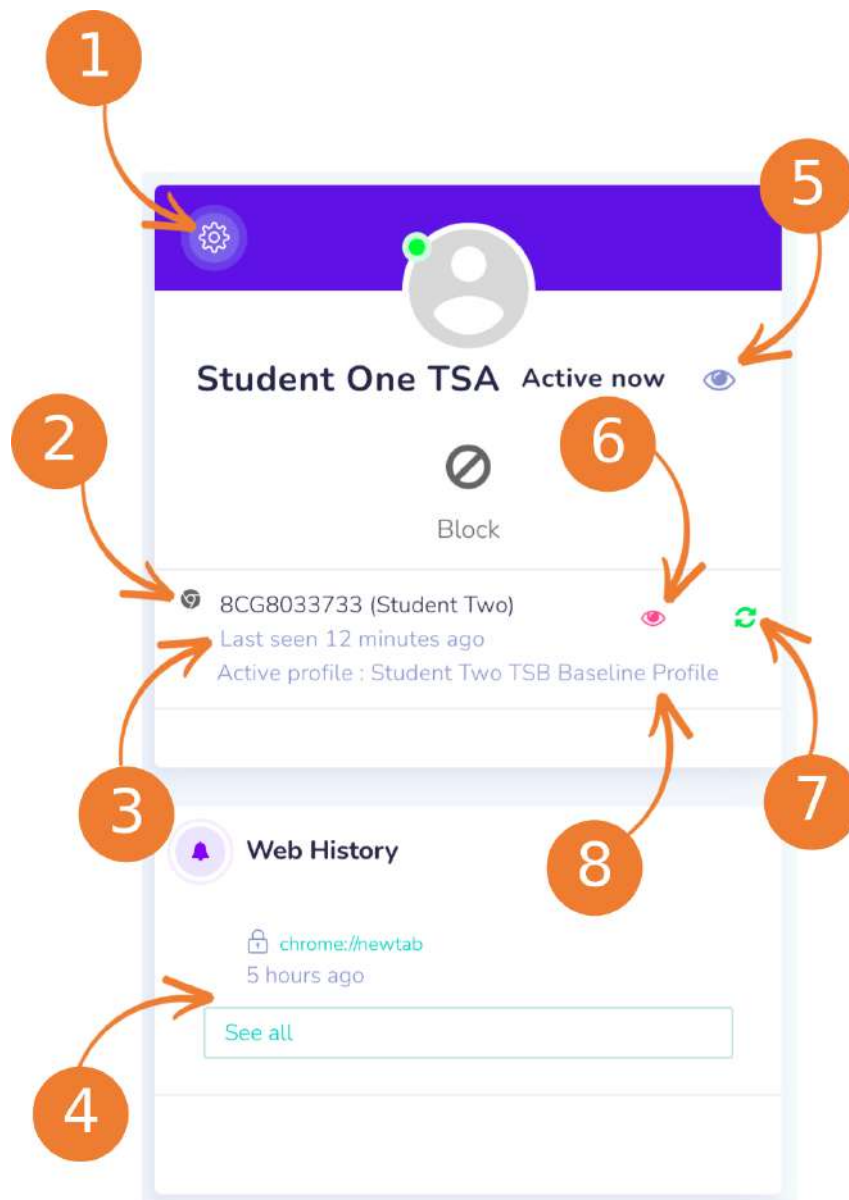


Figure 3.2.1: Card representation of a child's device

1. **Settings**

Clicking on the gear icon brings up a dropdown menu showing "**Settings**" and "**Refresh all**". The "**Refresh all**" button performs the same as item #7 since each child has only 1 device under the DMA programme.

2. **An icon representing the device type**

In this example, the icon shows a Chrome logo which indicates that the child/ward is using a Chromebook. If the child/ward is using an iPad, the icon will be the Apple logo. The name after the icon will show either the serial number of the device or the name of the child/ward depending on the naming policy adopted by the school.

3. **The date/time when the device was last reported online**

This value is a snapshot of the last date/time when the device was last synced with the Mobile Guardian Server to get the DMA policies.

4. **The browsing history of the child/ward**

This section shows the latest activities within the last 24 hours. To see earlier activities, click on the "**See all**" button. Please use the web-filter report on the main menu to review the activities.

5. **Detailed view of the child/ward**

6. **Detailed view of the device**

7. **Refresh device button**

This button sends a command to the device to update itself with DMA policies. In some cases where the device is not updating itself with the right profile (see #8), this button can be used to bring the device up to date.

8. **Name of active profile**

The name of the profile that is being applied by the device. This name can change throughout the day as the device switches profile (e.g school hours, after school hours, sleep hours, parent profile).



### Unit 3-3 - Device Details

The details of a device can be viewed by clicking on the Detailed view button (eye icon) in the child/ward's card.

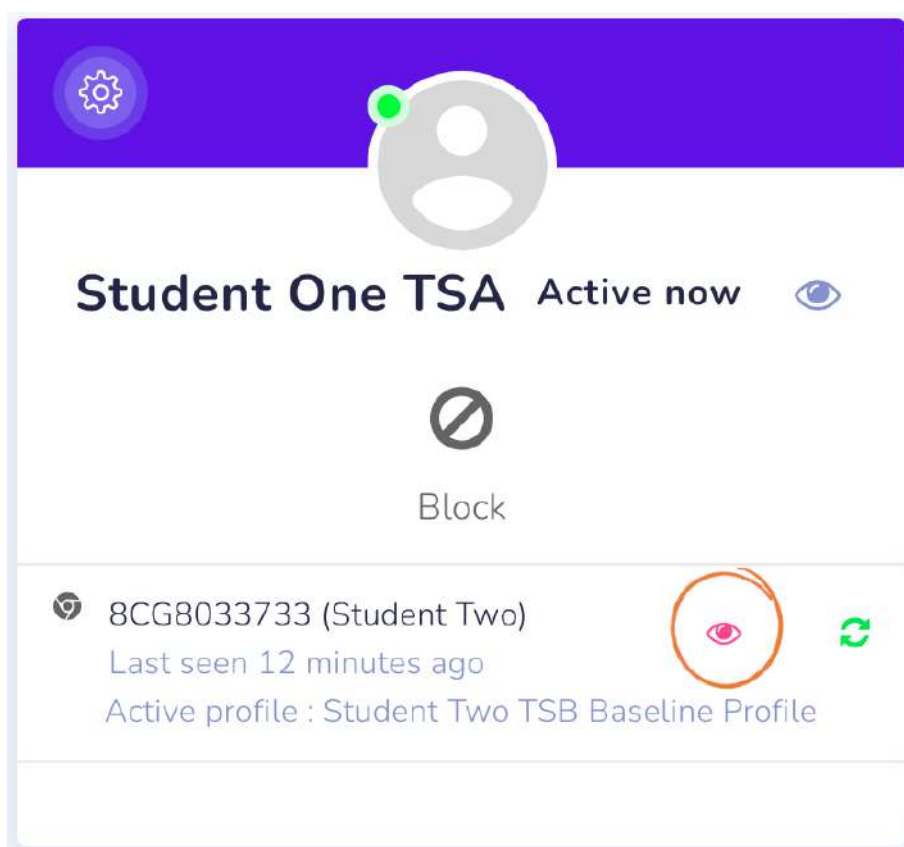


Figure 3.3.1: Button to view device details

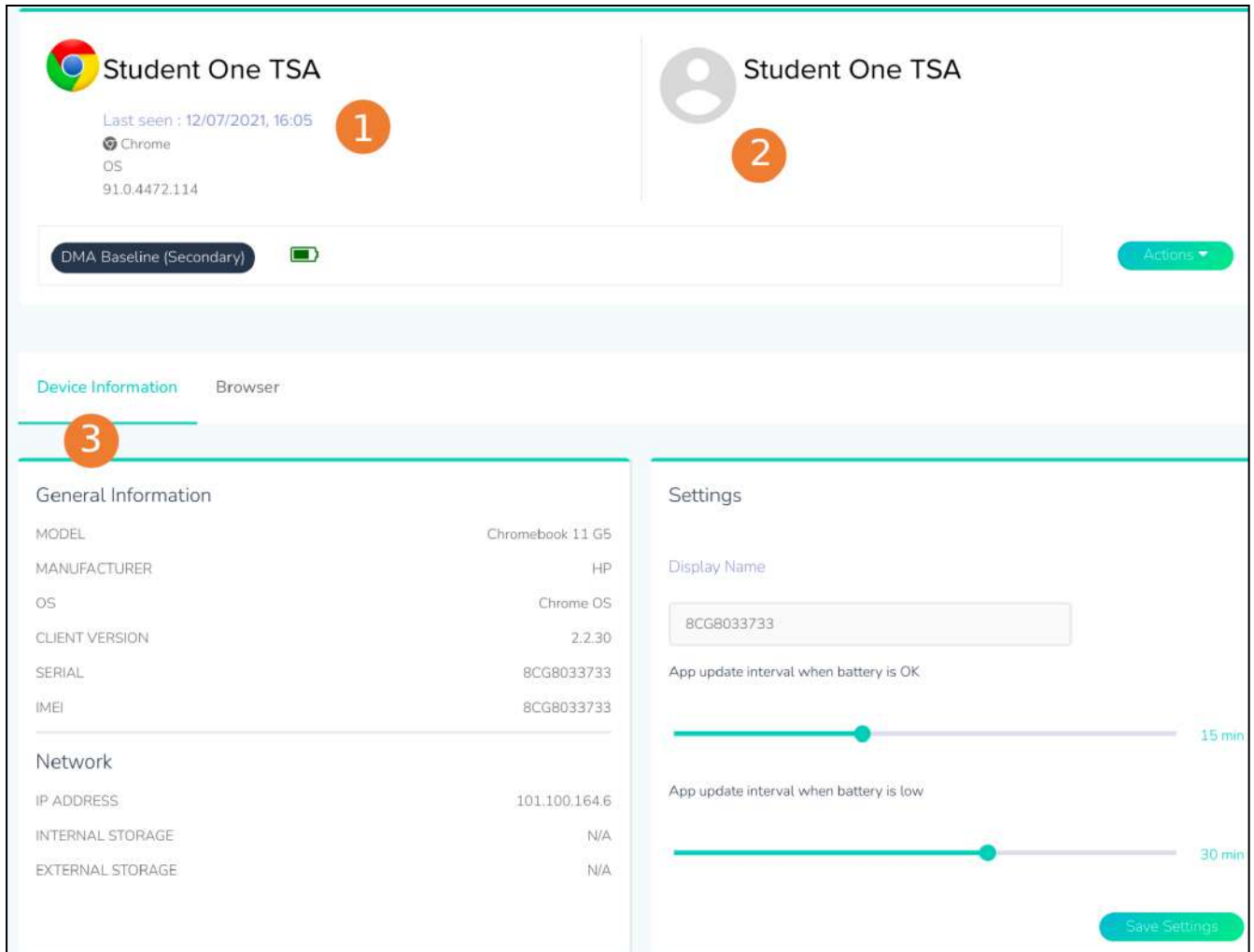


Figure 3.3.2: Device Detail page

1. This section provides more details on the device including the version of the operating system (OS) and the battery level.
2. This section shows the name of the child registered on the device.
3. There are two tabs in this row that provide more information about the device and the registered child. (See below.)
  - a. **Device information** - This tab shows more information about the device such as the make and model of the device under General Information. Under Settings, the display name of the device is displayed but not modifiable.
  - b. **Browser** - This tab shows the browsing history of the child/ward on the device. Select the period to extract browsing history. If there is no browsing history logged, you will see the message "**No browser activity for selected range.**"

*Note : The update interval settings should be left at the default values (15 mins and 30 mins) as changing those settings may affect the performance of the device in getting policy updates.*

## Unit 3-4 - Webfilter Reports

The Webfilter Reports option in the side menu presents a consolidated view of the browsing history of the child/ward on the device.

This page lists browsing activity for the last 24 hours by default. If there is no activity, you will see an empty listing as shown below.

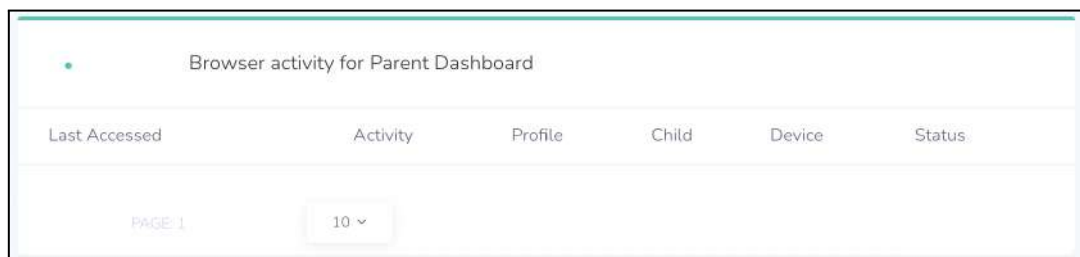


Figure 3.4.1: Empty listing page for browser activity

Click on the "Filter" button at the top-right of the page to reveal the dropdown menu as shown below.

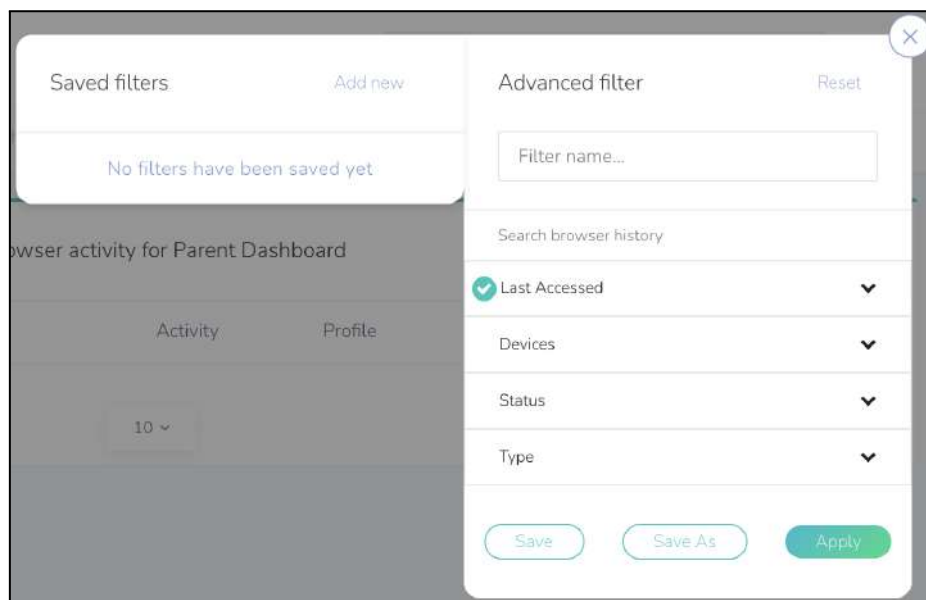
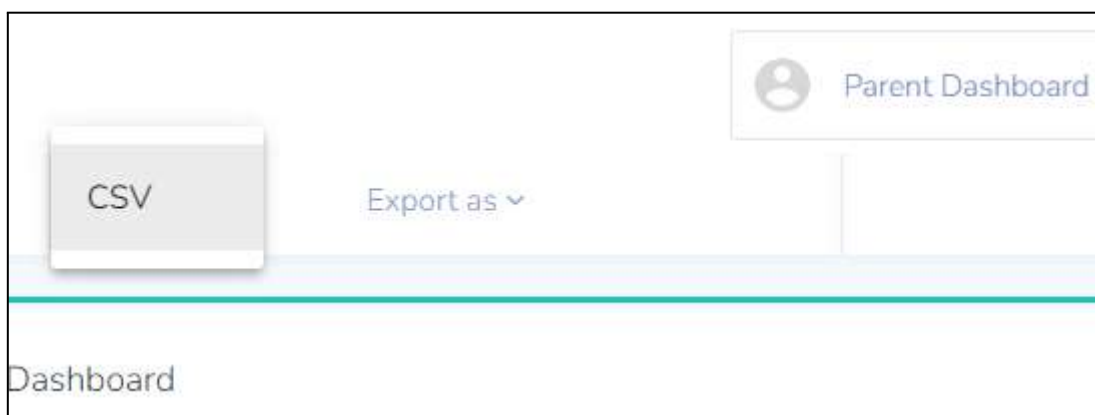


Figure 3.4.2: Dropdown menu for filter

Click on "**Last Accessed**" to reveal a list of date ranges. Select the required date range and click on "**Apply**" to update the listing.

### Downloading the Web Filter Reports

The listing of browser activities on the page can be downloaded by clicking on **Export as** at the top of the page. This presents a dropdown menu for selecting the format of the report, which can then be downloaded.



*Figure 3.4.3: Dropdown menu for format selection*

## Chapter 4: Option A Functions

Option A provides the following:

- Ability to modify Web content filtering
- Flexibility to change sleep hours timing

### Unit 4-1 - Managing Web Content

Parents who opt for Option A have the ability to modify the content filtering protection provided by Mobile Guardian.

**Note:** If you do not modify any filters, the device will adopt the school's policy as though it is under the Default Option.

To modify the filter, click on the gear icon on the student card, then click on "**Settings**" in the dropdown menu.

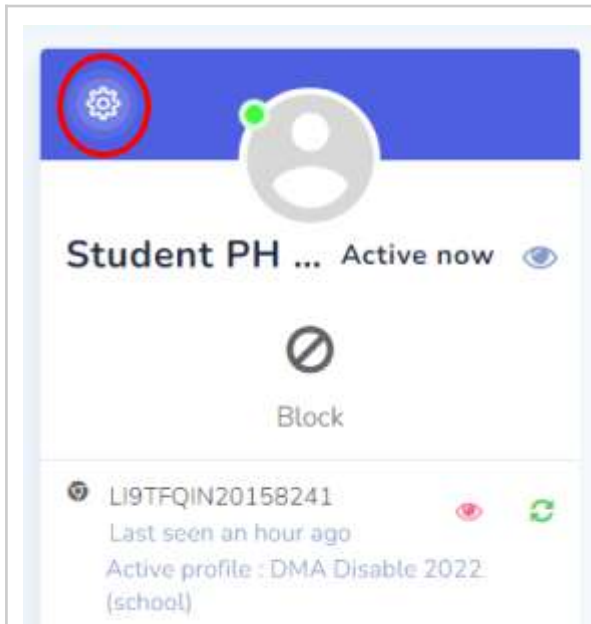


Figure 4.1.1: Gear icon on student card

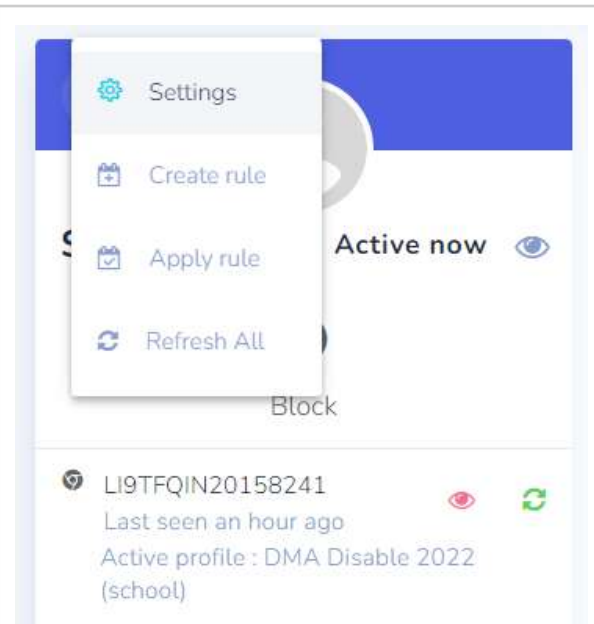


Figure 4.1.2: Dropdown menu

Then click on the "**Safe content**" panel to open the Web Filter page.

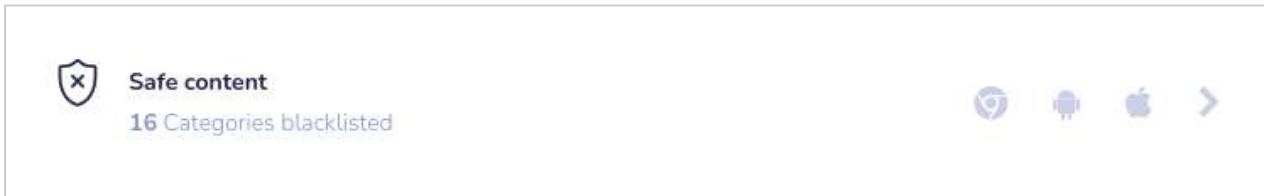


Figure 4.1.3: "Safe content" section

By default, when you visit the Web Filter page, the option is turned off, as shown below:



Figure 4.1.4: Web filter toggle switch.

As mentioned earlier, even if this option is not enabled, the Web filter created by the school is still in effect. This can be confirmed by using the **URL Tester**.

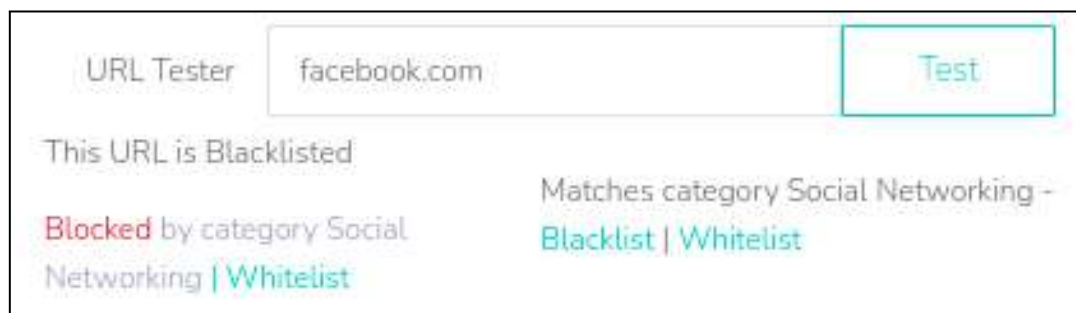
## URL Tester

To check whether an URL is filtered, enter the URL into the **URL Tester** and click on "**Test**".



Figure 4.1.5: URL Tester

The two figures below show the results of a blocked URL and one that is not.



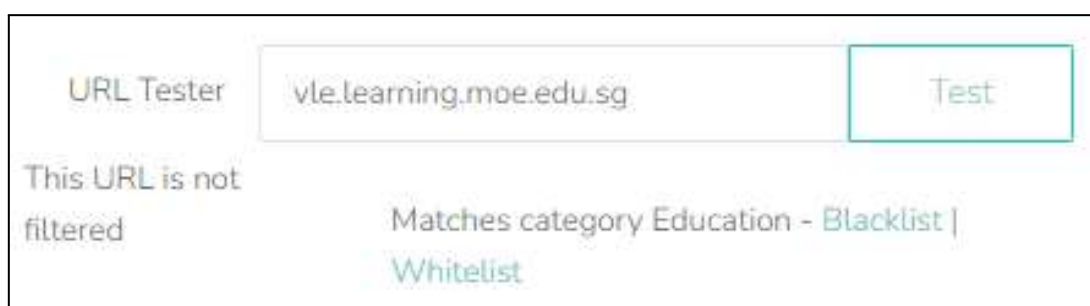
URL Tester

This URL is Blacklisted

**Blocked** by category Social Networking | [Whitelist](#)

Matches category Social Networking - [Blacklist](#) | [Whitelist](#)

Figure 4.1.6: Example of a URL that is blocked



URL Tester

This URL is not filtered

Matches category Education - [Blacklist](#) | [Whitelist](#)

Figure 4.1.7: Example of a URL that is not blocked



## Custom Web Filter

To create your own custom Web Filter, turn on the **“Enable filter”** option.

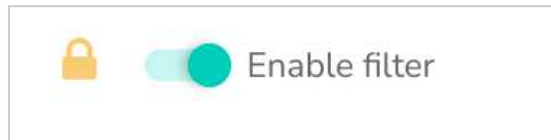


Figure 4.1.8: Turning on the Web Filter

This brings up other options in the page as shown below.

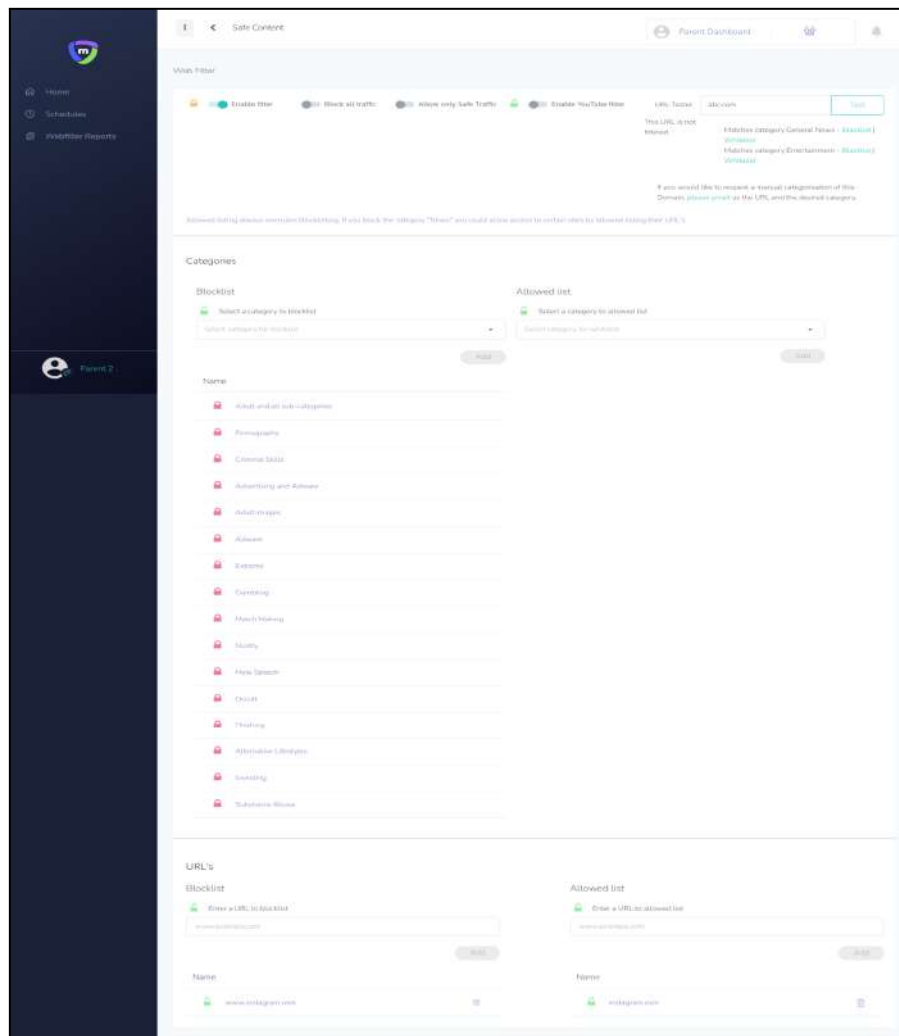


Figure 4.1.9: Options that are enabled after Web Filter is turned



*Figure 4.1.10: Options that are available after Web Filter is turned*

When **Block all traffic** is turned on, the child will not be able to access any website **at all**



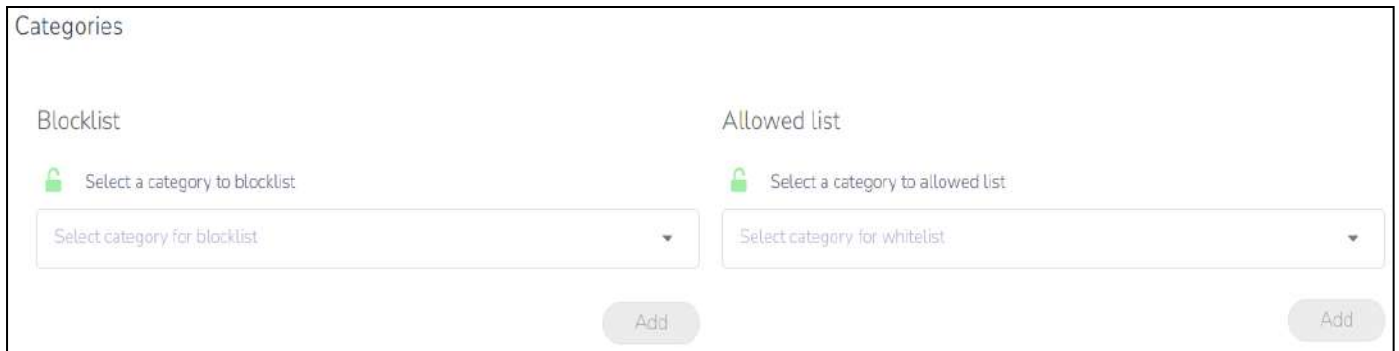
*Figure 4.1..11: Block all traffic is enabled*

When **Allow only Safe Traffic** is turned on, the child will only be able to access sites based on explicitly whitelisted category URLs under the categories allowed list



*Figure 4.1.12: allow only safe Traffic is enabled*

The categories section shown below provides functionality for blocking/allowing website categories.



Categories

**Blocklist**

Select a category to blocklist

Select category for blocklist

Add

**Allowed list**

Select a category to allowed list

Select category for whitelist

Add

*Figure 4.1.12: Web Filter Categories*

Click on the dropdown arrow to reveal the list of categories for selection to add to the blacklist. Websites that fall into any of the blacklisted categories are blocked from access by the child.

There are some websites that fall under multiple categories. If one of the categories is placed in the Whitelist, the website becomes accessible. This is best explained with an example. The website [expressvpn.com](https://expressvpn.com) is categorized under both Security and Web Proxy. If the Web Proxy category is placed in the Blacklist, this website is not accessible. To make it accessible, the Security category can then be placed under the Whitelist.

**Note: Blacklisting is to block browsing for a particular category while whitelisting is to allow browsing.**

Note that when you turn on the Web filter, there is a list of categories already added to the blacklist. The **Red padlocks** next to the categories indicate that they are not removable.

These are from the baseline policy set forth by the Ministry of Education (MOE). They represent categories that are strictly out of bounds, and are not exempted under any circumstance.

There are other categories that have been blacklisted but not set with a red padlock. Such blacklisted categories are not propagated here.

















Name
 Criminal Skills
 Nudity
 Alternative Lifestyles
 Pornography
 Substance Abuse
 Gambling
 Match Making
 Adult images
 Adult and all sub-categories
 Occult
 Adware
 Phishing
 Extreme
 Hate Speech
 Investing
 Advertising and Adware

Figure 4.1.3: Preset blacklisted categories

Further down the page is the section on URLs.

Figure 4.1.4: URL blacklist/whitelist entry fields

These fields let you enter specific URLs to blacklist/whitelist.

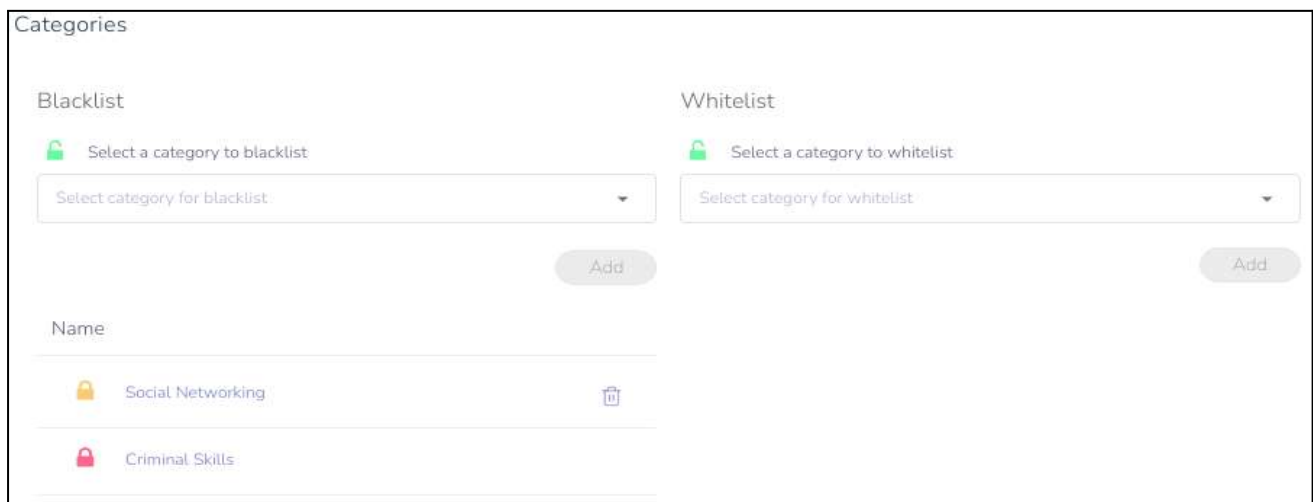
### Example Scenario

To block facebook.com but allow other social networking websites to be accessible by your child, you can key in www.facebook.com and add the web address into the URL blacklist. You can confirm the action of blacklisting by using the URL Tester.

<p>Figure 4.1.5: Blacklisting facebook.com</p>	<p>Figure 4.1.6: Testing the blacklist</p>

Should you decide to block all the social networking websites, you can simply add **"Social Networking"** to the **category blacklist** instead. Once that is done, you can remove facebook.com from the **URL blacklist**.

While **"Social Networking"** is blacklisted by **category blacklist**, you may still whitelist specific social media sites via the **URL whitelist**.



Categories

Blacklist

Select a category to blacklist

Select category for blacklist

Add

Whitelist

Select a category to whitelist

Select category for whitelist

Add

Name




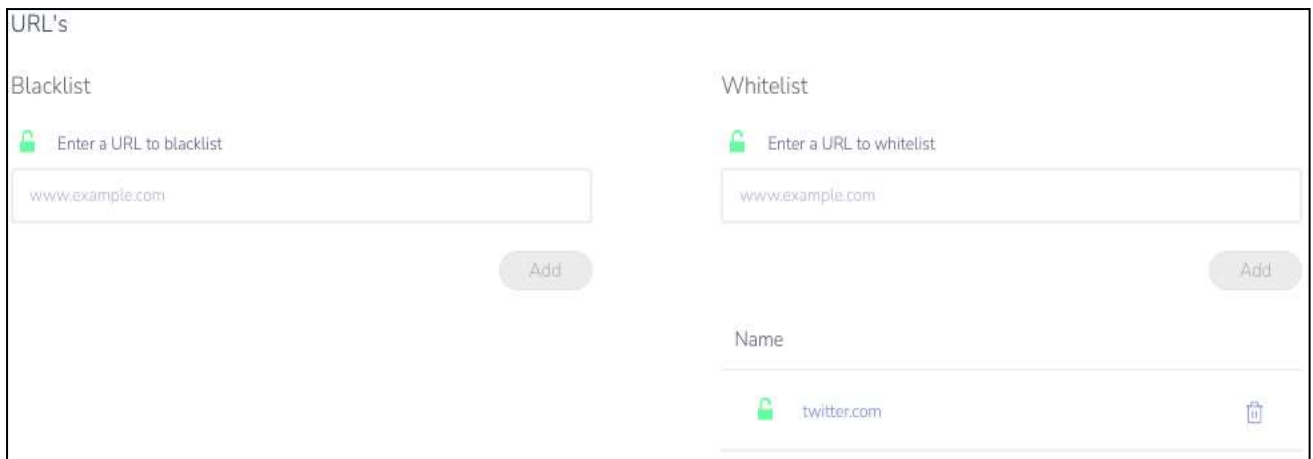
-  Social Networking 
-  Criminal Skills

Figure 4.1.7: Blacklisting of "Social Networking" category



URL's

Blacklist

Enter a URL to blacklist

www.example.com

Add

Whitelist

Enter a URL to whitelist

www.example.com

Add

Name



-  twitter.com 

Figure 4.1.8: Whitelisting of twitter.com

You can confirm the action of whitelisting by using the URL Tester.

### Note About Baseline Profile

As described in the section "[Unit 4-1 - Managing Web Content](#)", if the custom Web filter is not turned on, the device takes on the school's policy, similar to devices under the Default Option.

If the school does not create its own after school hours profile, the default profile that is applied is the *baseline profile*. The baseline profile contains settings determined by MOE. The key thing to note about the baseline profile is that it enforces a set of categories of websites that are not accessible by students. This list of categories is indicated with red padlocks (shown in Figure 13n: Preset blacklisted categories). These categories are enforced no matter what profile the device takes on.

In addition to these categories with the red padlocks, the baseline profile also blacklists the following categories with an amber padlock:

	Social Networking	
	Games	
	Web Chat	

*Figure 4.1.9: Web categories blacklisted with amber padlock*

Websites in these three categories are blocked from access when the baseline policy is applied. To allow access to websites in these categories, the custom filter in the parent dashboard needs to be turned on.

Take for example facebook.com - this website is blocked in the baseline profile. The personal learning device takes on the baseline profile by default after school hours. This means that the child is unable to access this website. To allow the child to access this website, you need to turn on the custom Web filter (see section "[Custom Web Filter](#)").

By turning on the custom Web filter, the baseline profile no longer applies and the three categories with the amber padlock are no longer blacklisted, and thus the child is able to access facebook.com

Note: Any of these three categories, and other categories as well, can be added to the blacklist in the parent dashboard at any time.

## YouTube Filter

The YouTube filter toggle switch is only accessible if Web Filter is turned on.

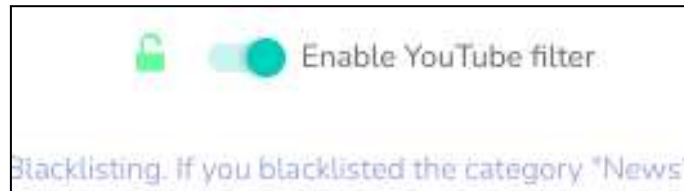



Figure 4.1.10: Turning on YouTube filter

Turning on the YouTube filter switch brings up the YouTube Filter panel at the bottom of the page.

Youtube Filter

Categories


Blacklist

 Select a category to blacklist

Select category for blacklist

Add

Whitelist


 Select a category to whitelist

Select category for whitelist

Add

Channels


Blacklist

 Enter a URL to blacklist

www.example.com

Add

Whitelist


 Enter a URL to whitelist

www.example.com

Add

Videos


Blacklist

 Enter a URL to blacklist

www.example.com

Add

Whitelist

 Enter a URL to whitelist

www.example.com

Add

Figure 4.1.11: Filter options for YouTube



There are three options for filtering YouTube - by category, by channel and by URL.

There is a dropdown menu for you to select the categories to filter the YouTube videos by category.

To filter YouTube channels, you can specify URLs that begin with "**https://www.youtube.com/channel/**"

To filter specific YouTube videos, you can specify URLs that begin with  
"**https://www.youtube.com/watch?v=**"

### Removing Custom Web Filter



*Figure 4.1.12: Disabling web filter*

Any custom Web filter that was added can be easily removed by turning the Web filter toggle switch off. This is a quick and easy way to revert to the school's baseline policy without having to undo each and every setting.

When you turn the Web filter back on, your settings will be restored.

## Unit 4-2 - Blocking your child's device

You can block your child's device by using the block button in the card layout .

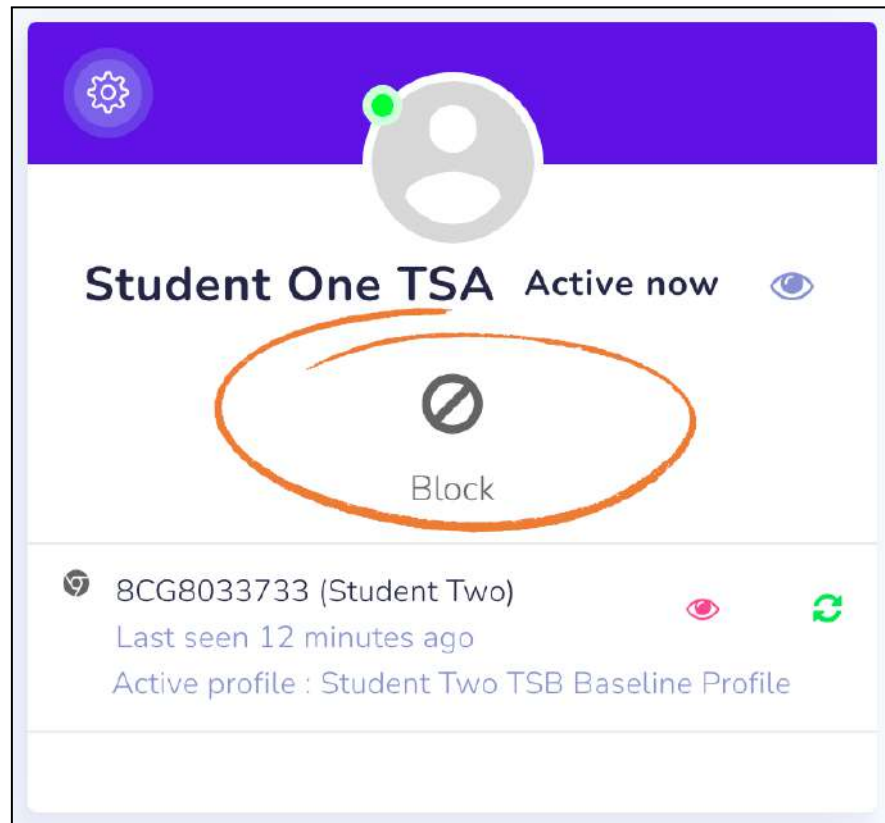


Figure 4.2.1: Block option on the card layout

Clicking on the button brings up a dialogue box:

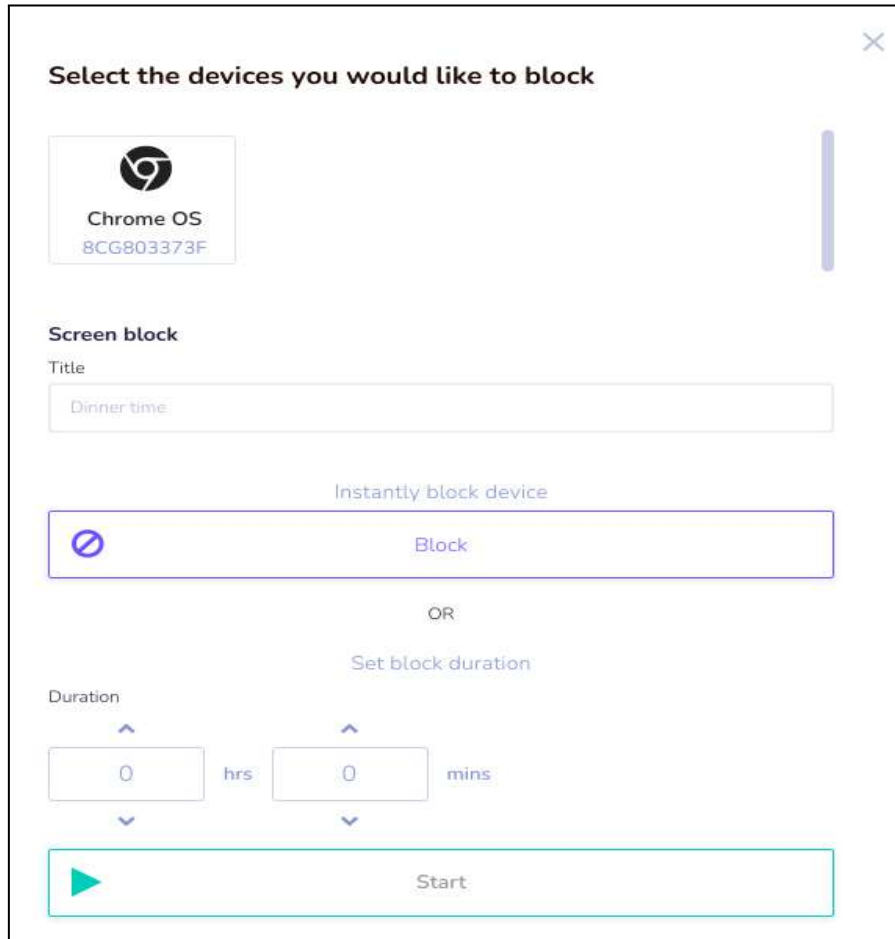


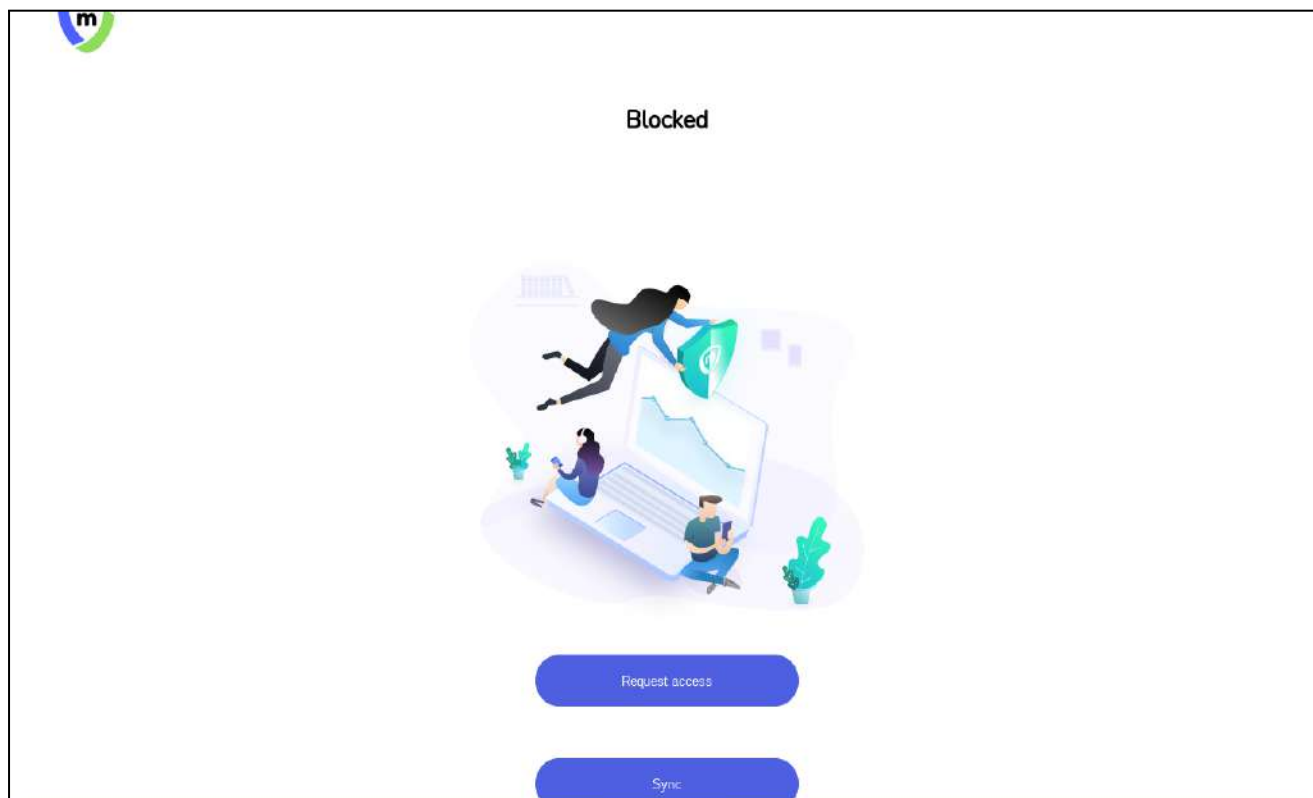
Figure 4.2.2: Dialogue box for blocking of device

Select the device that you wish to block (for the DMA programme, there will only be one device per child), then enter a title for the block screen.

You can choose to block the device instantly by selecting the **Block** option. Note that this option **does not have an expiry or time limit**. This means that if you wish to unblock the device, it has to be done by you from the dashboard as well.

Alternatively, you can choose a duration for which the device will be blocked, and then click on **Start**. The device will be blocked after you click start and will remain so for the duration that has been set.

## Blocked Screens on Chromebooks & iPads



*Figure 4.2.3: The Blocked screen shown on a device*

The block screens for the devices may have additional information (such as the message entered in the dialogue box). The request access and sync button are also shown..

## Unit 4-3 - Sleep Hours

The guidelines on proper device usage recommends the sleep hours to be set from 11 pm to 6 am the next day. However, schools, at their discretion, can decide on whether to create a **Sleep Hours** profile at all, and, if so, at what time it should be enforced.

When the **Sleep Hours** profile is in-force, the device shows a block screen that prevents the usage of the device during the night, to facilitate rest time.

You have the choice of setting sleep hours for your child that is different from the school's profile. To do so, you first create a schedule, described in the next section..

## Unit 4-4 - Rules

Rules are like presets that can be reused over and over again. A rule can contain:

- Web Filter
- YouTube Filter
- Device Restrictions

**Note: Please ensure that the timezone is Singapore (GMT+8)**

### Step 1 - Creating a Schedule

First, go to Schedules on the menu dashboard and click on the "Add New +" button.

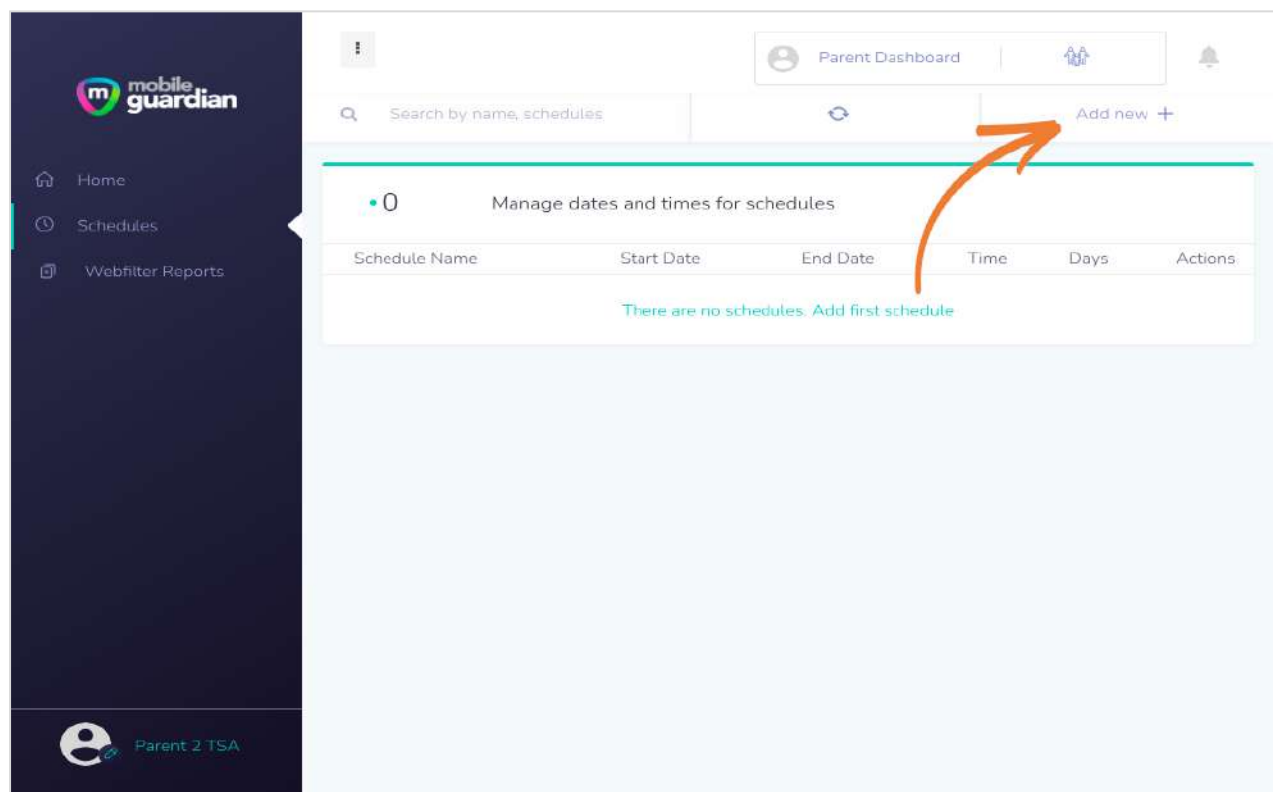
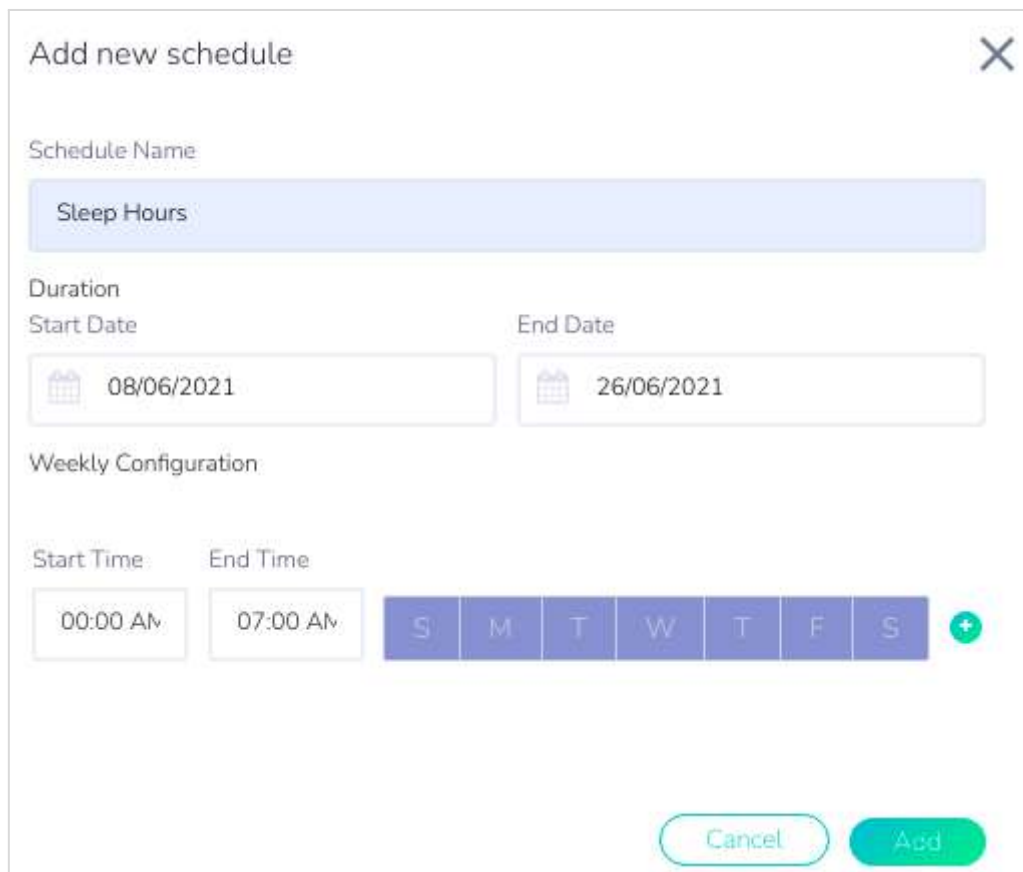


Figure 4.4.1: Creation of a new schedule



The form is titled "Add new schedule" and includes a close button (X) in the top right corner. It contains the following fields and sections:

- Schedule Name:** A text input field with the value "Sleep Hours".
- Duration:** A section containing two date pickers:
  - Start Date:** A date picker showing "08/06/2021".
  - End Date:** A date picker showing "26/06/2021".
- Weekly Configuration:** A section containing two time pickers and a day selector:
  - Start Time:** A time picker showing "00:00 AM".
  - End Time:** A time picker showing "07:00 AM".
  - Day Selector:** A row of seven buttons labeled "S", "M", "T", "W", "T", "F", and "S", all of which are currently selected (highlighted in blue). A green plus button is located to the right of the "S" button.
- Buttons:** At the bottom right, there are two buttons: "Cancel" (light blue) and "Add" (green).

Figure 4.4.2: Entry fields for creating a schedule

You will need to specify the following:

- Schedule Name
- Start Date and End Date for the duration
- Start Time and End Time to be applied for the day
- The days for which the schedule is to be applied

After creating the schedule, proceed to create the *rule*.

## Step 2 - Creating a Rule

Click on the gear icon in the card layout (see [Figure 3.2.1: Gear icon on student card](#) for the location) and then select "**Create rule**".

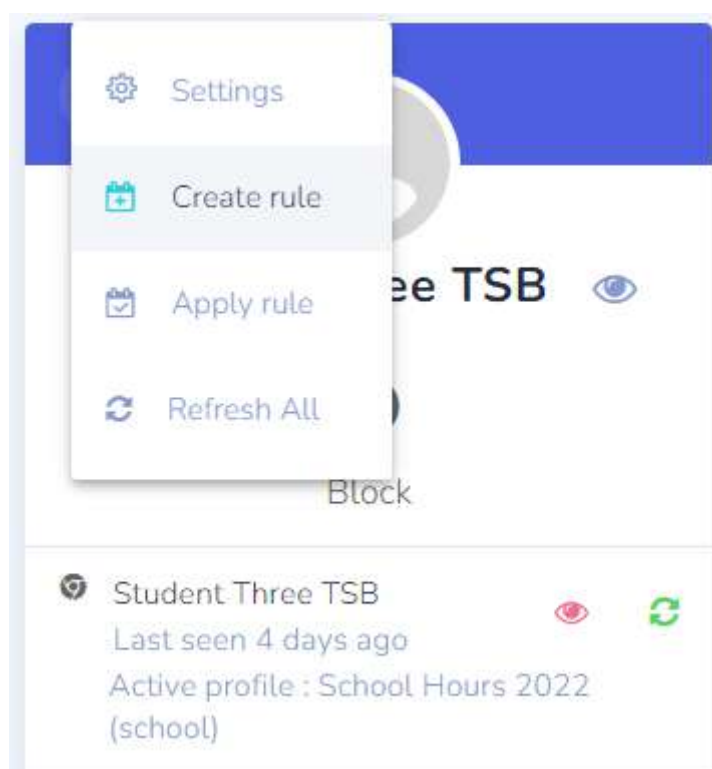


Figure 4.4.3: Dropdown menu to create a rule for custom sleep hours



1. Give the rule a name that you can easily identify.
2. The name of your child will be displayed here. You ***must*** click on the name to select it before the "Create" button at the bottom becomes enabled.
3. This message will appear on the block screen.
4. Select "***When activated at a specific time***" to set your custom sleep hours.
5. Click on the arrow next to Anytime - this will bring up a dropdown menu showing the available schedule.
6. Click "**Create**" when done.

**Set up your rules below**

Give your rule an easily recognizable name

1 → Sleep Time

Who should this rule apply to?

2 → Student Two

☒ Apply device block to limit screen time

Block screen message

3 → Bedtime

Where and when should this rule be applied?

☐ When activated manually

4 → ☒ When activated at a specific time

When should this rule be applied?

5 → Anytime ▾

Add New Schedule +

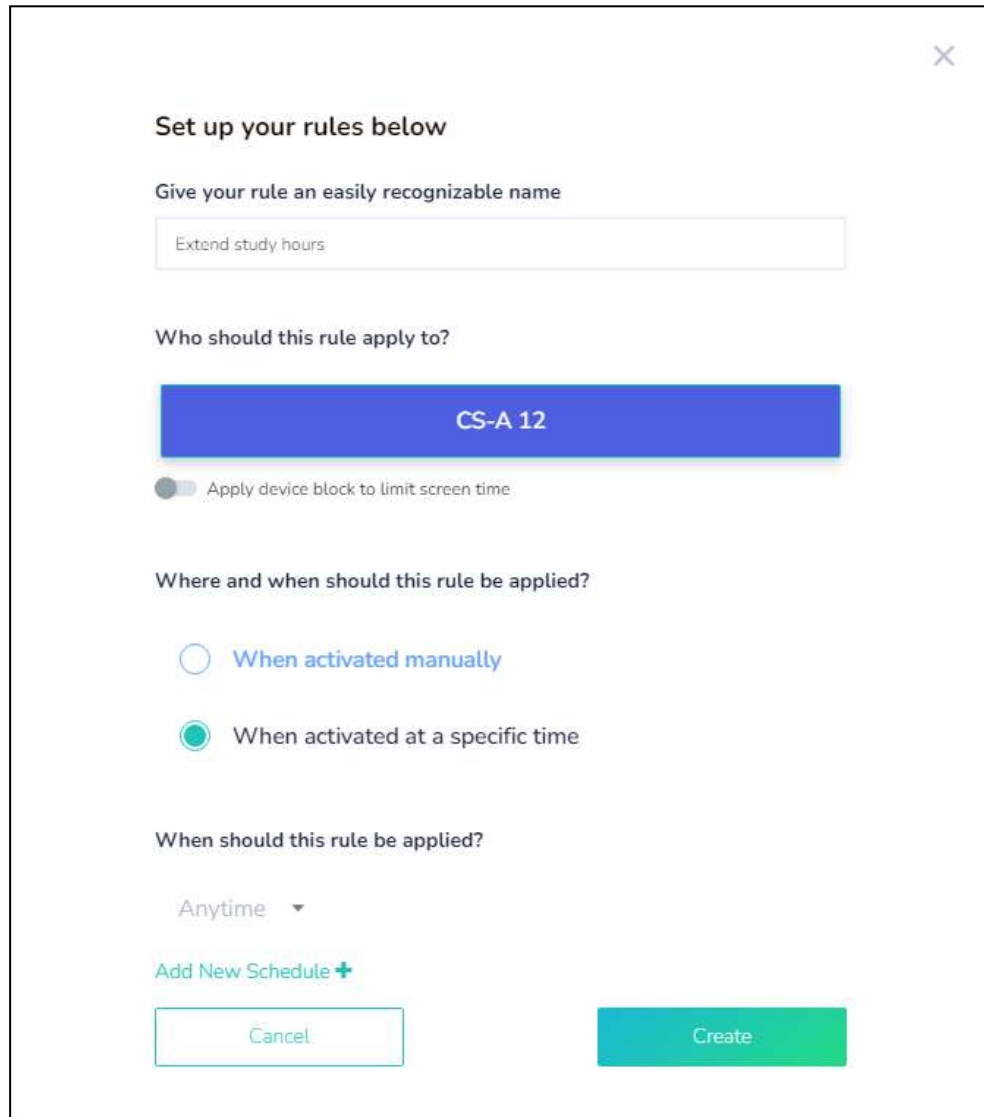
Cancel Create

Figure 4.4.4: Dialogue box for creating a rule

### Step 2.1 Overwrite School Sleep Hours

To extend the device usage for your child past sleep hours' timing, you will need to create a rule and schedule and apply it to the device in order to overwrite the school default sleep hours.

Set up the rule as shown below:

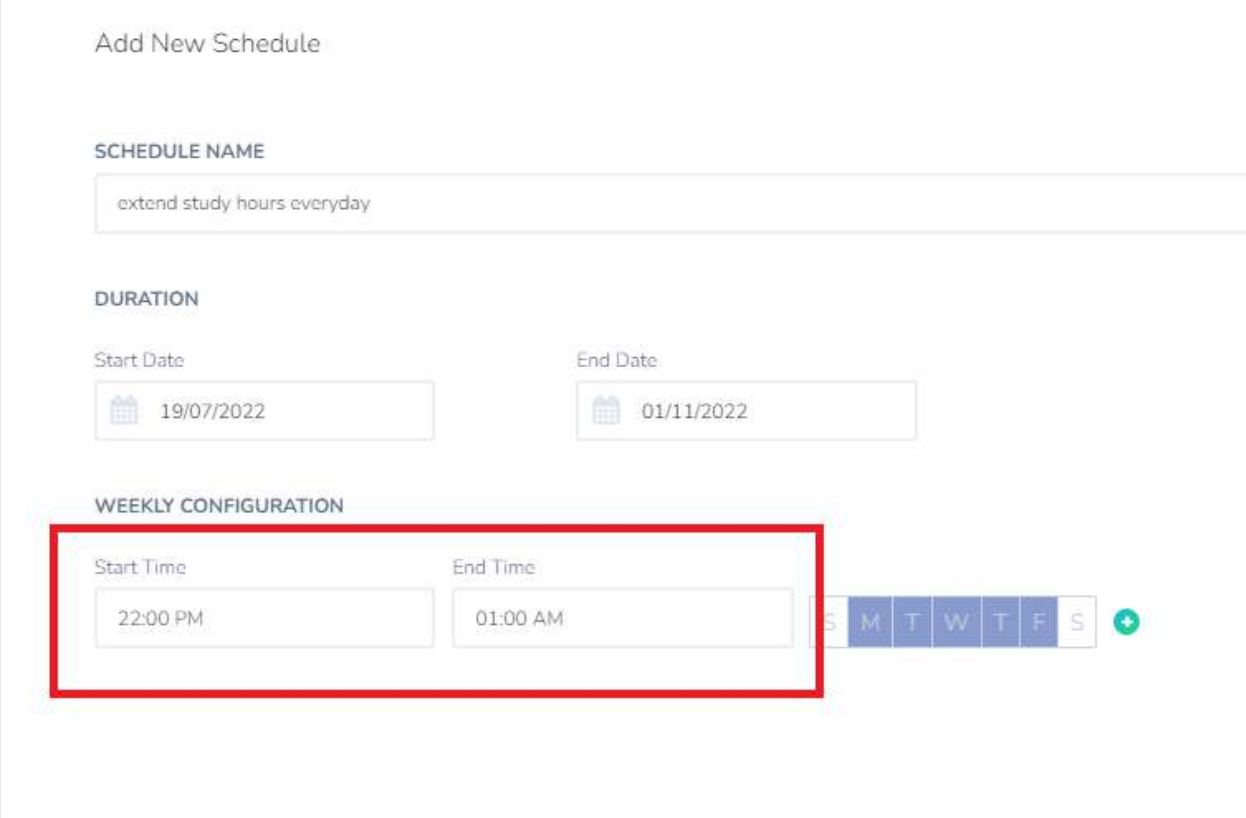


The screenshot shows a dialog box titled "Set up your rules below" with a close button (X) in the top right corner. The dialog contains the following fields and options:

- Give your rule an easily recognizable name**: A text input field containing "Extend study hours".
- Who should this rule apply to?**: A blue button labeled "CS-A 12".
- Apply device block to limit screen time**: A toggle switch that is currently turned off.
- Where and when should this rule be applied?**: Two radio button options:
  - ☐ When activated manually
  - ☒ When activated at a specific time
- When should this rule be applied?**: A dropdown menu currently set to "Anytime".
- Add New Schedule**: A link with a plus icon.
- Buttons**: "Cancel" and "Create" buttons at the bottom.

Figure 4.4.5: Rules Set Up

If the school sleep hours are from 11:00 pm to 6:00 am, and you would like to extend from 11:00 pm to 1:00 am, you will need to set the start time to be at least an hour earlier (**for example 10:00 pm**). This will override the school default sleep hours and allow the child to use the device until 1:00 am.



Add New Schedule

**SCHEDULE NAME**

extend study hours everyday

**DURATION**

Start Date: 19/07/2022

End Date: 01/11/2022

**WEEKLY CONFIGURATION**

Start Time: 22:00 PM

End Time: 01:00 AM

S M T W T F S +

Figure 4.4.6: Add New Schedule

Click on **Create** after the schedule is added to activate the rule.

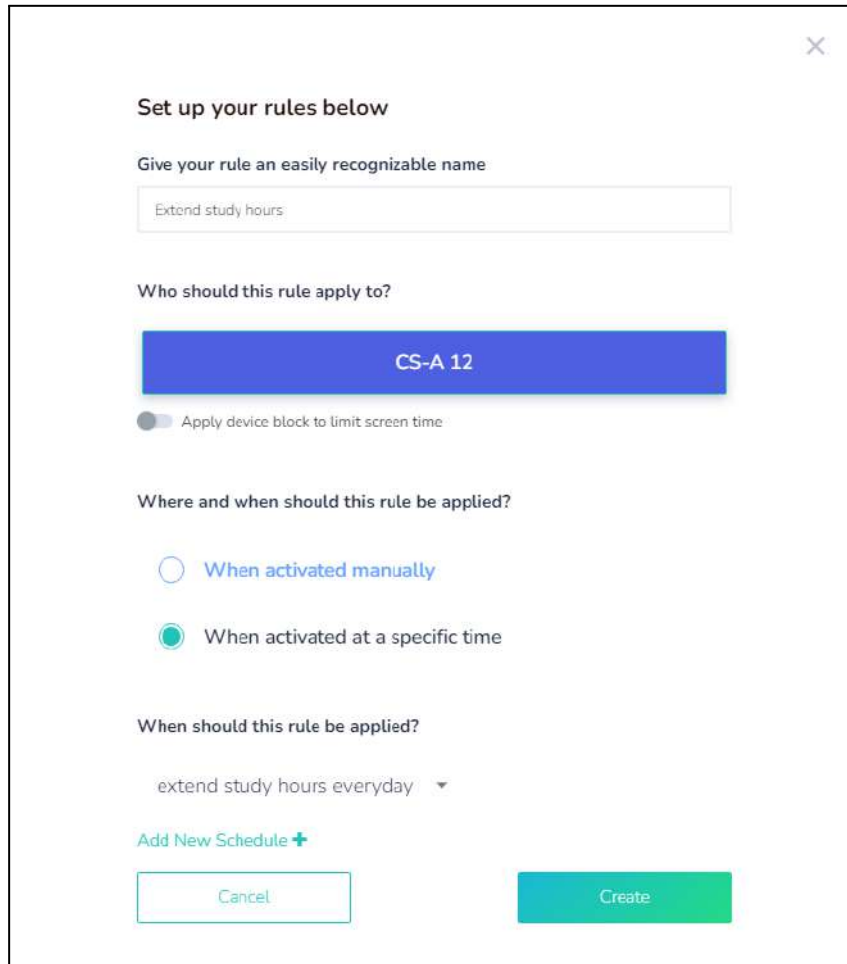


Figure 4.4.7: Create New Schedule

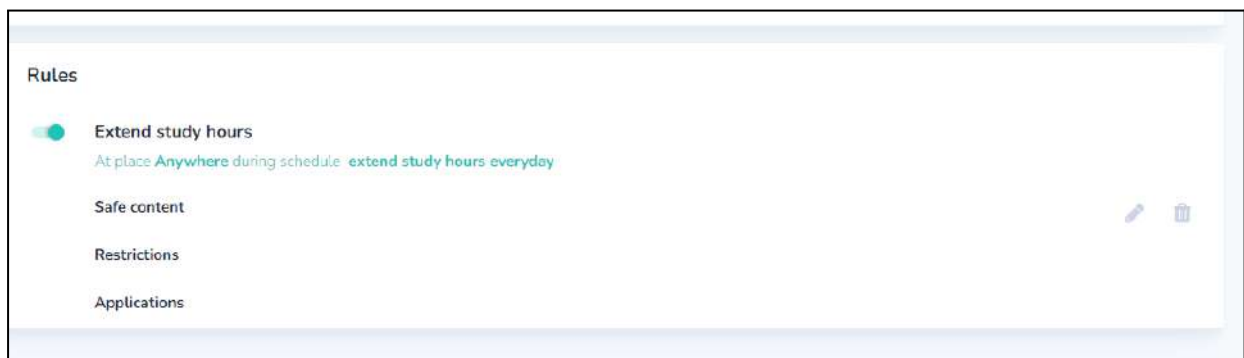


Figure 4.4.8: New Schedule Added

#### Things to note when setting sleep hours for your child/ward

1. This will override the sleep hours timing imposed by the school (if any).
2. If the sleep hours are set past the school's starting time, your child/ward's device will still switch to school hours.

Example:

**Sleep hours timing set by you:** 10.00pm - 9.00am

**School hours:** 8.00am - 3.00pm

Device will still **switch back to school hours at 8am.**

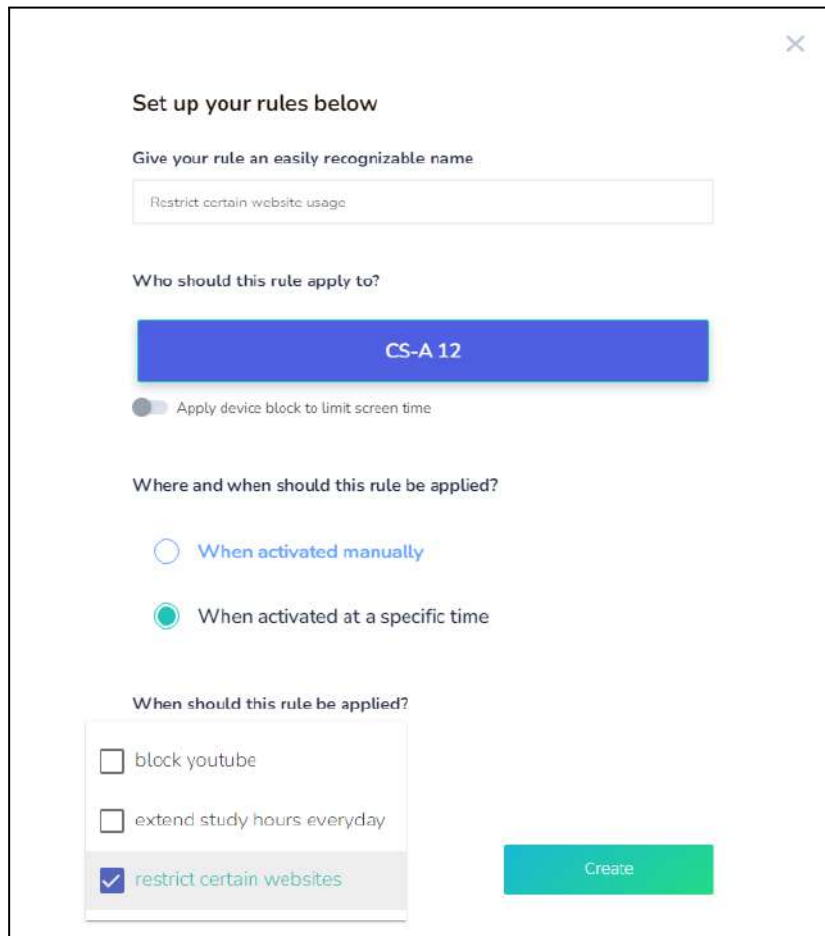
#### Step 3 - Make the necessary settings

- Web Filter (refer to [Custom Web Filter](#))
- YouTube Filter (refer to [YouTube Filter](#))

## Step 2.2 Setting Up Web Filter Rules

To restrict your child's access to certain websites, you can create rules and schedules and apply them to the device at a specific time.

Set up a rule as shown below



Set up your rules below

Give your rule an easily recognizable name

Restrict certain website usage

Who should this rule apply to?

CS-A 12

☐ Apply device block to limit screen time

Where and when should this rule be applied?

☐ When activated manually

☒ When activated at a specific time

When should this rule be applied?

☐ block youtube

☐ extend study hours everyday

☒ restrict certain websites

Create

Figure 4.4.9: Rules Setup - Restrict Certain Websites

Once the **rule** is created, click on the pen highlighted in red below to access the rules setting



Figure 4.4.10: Editing Restrict Certain Website Usage

Click on **safe content** to view or add sites to the URL blacklist or allowed sites

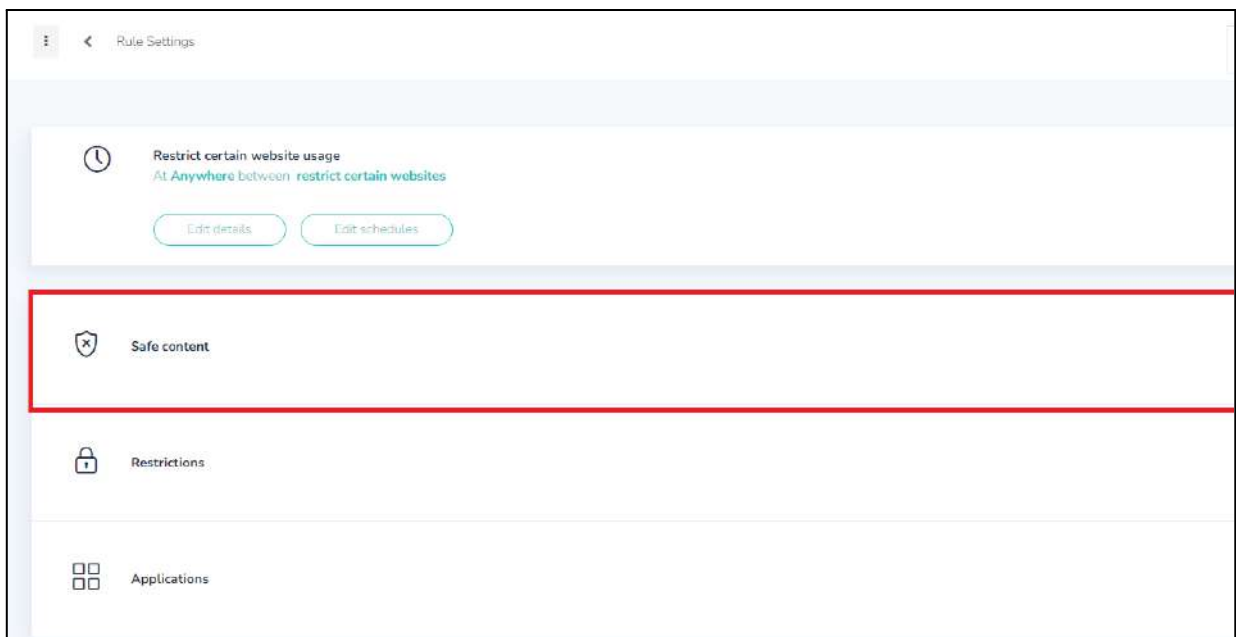


Figure 4.4.11: Restrict Certain Website Usage - Safe Content

Turn on **Enable filter**.

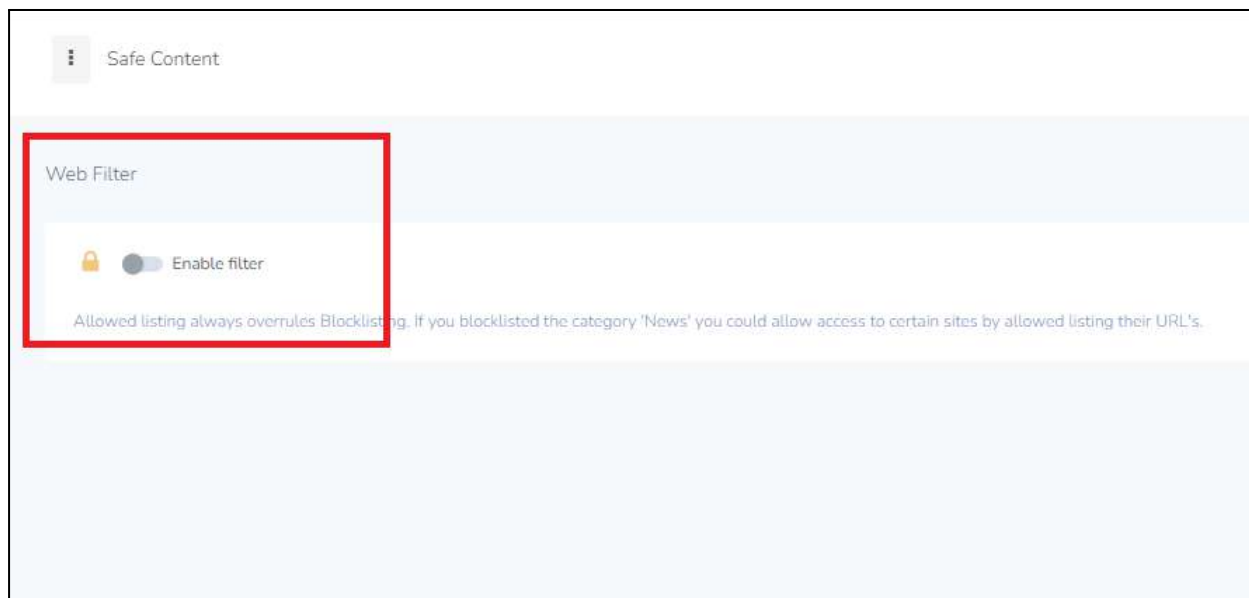


Figure 4.4.12: Safe Content - Enable Filter



You can turn on **either block all traffic** or **allow only safe traffic** for further restrictions on web browsing.



Figure 4.4.13: Restrict Certain Website Usage - Safe Content

There are four **pre-configured categories**, most restricted sites are already included within these categories.

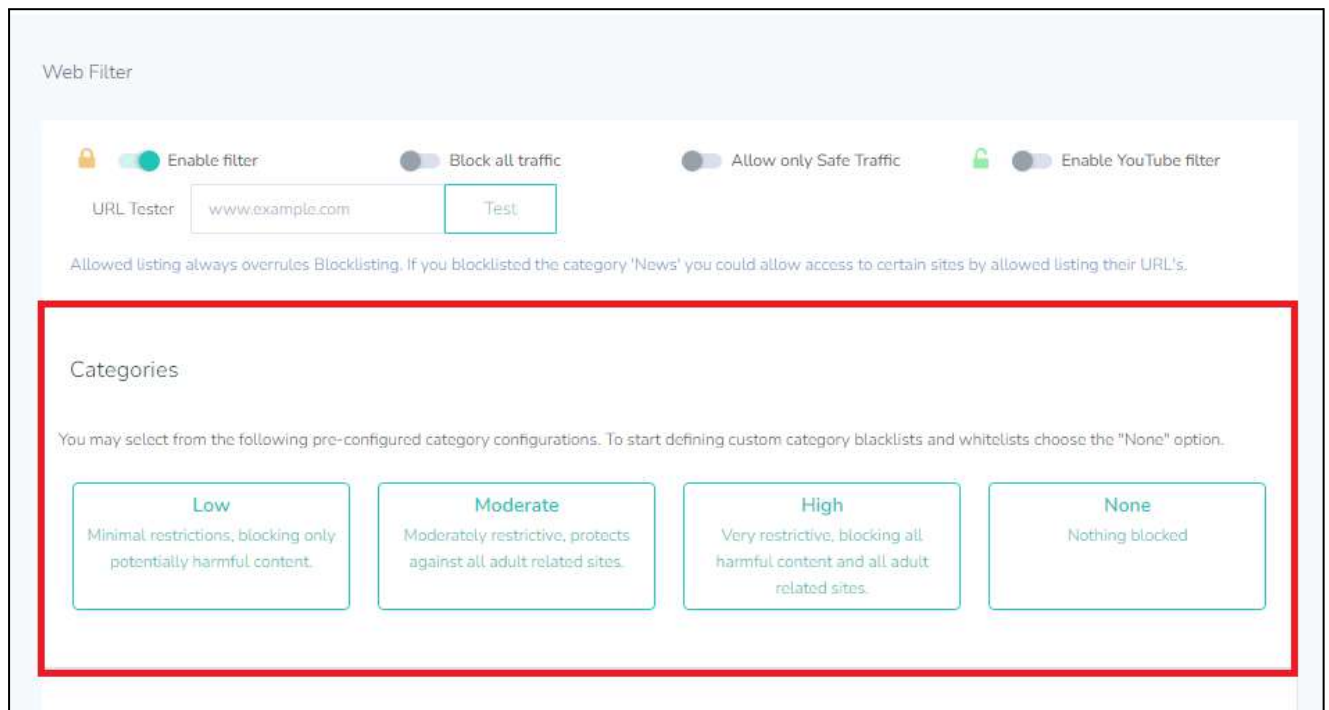


Figure 4.4.14: Web Filter - Categories

**Example:** If you had selected the **High** category, 31 categories of websites will be blocked, including: gambling, adult images, web chat, games, etc.. This will be sufficient in blocking most sites with harmful content.

Safe Content

Blocklist

Select a category to blocklist

Select category for blocklist

Add

Name

Health

Hate Speech

Gambling

Sex Education

Adult images

Extreme

File sharing

Web Chat

Adult and all sub-categories

Figure 4.4.15: Safe Content - Add Category to Blocklist

Page 50 of 72

Websites may be added to the **URL blacklist**.

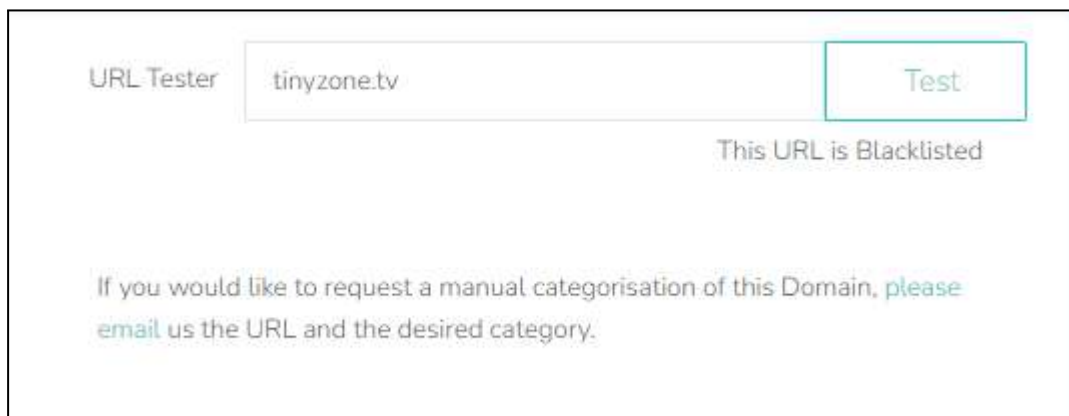


The screenshot shows the 'URL's Blocklist' section. At the top, there is a text input field with the placeholder 'www.example.com' and an 'Add' button. Below this, a table lists the blocked URLs. The first entry, 'tinyzone.tv', is highlighted with a red border. The table has columns for 'Name' and an action icon (a trash can).

Name	
 tinyzone.tv	

Figure 4.4.16: Safe Content - Add URL to Blocklist

Use the **URL Tester** to verify if a particular URL is blocked.



The screenshot shows the 'URL Tester' section. It features a text input field containing 'tinyzone.tv' and a 'Test' button. Below the input field, the message 'This URL is Blacklisted' is displayed. At the bottom, there is a note: 'If you would like to request a manual categorisation of this Domain, please email us the URL and the desired category.'

URL Tester

This URL is Blacklisted

If you would like to request a manual categorisation of this Domain, please email us the URL and the desired category.

Figure 4.4.17: URL Tester - This URL is Blacklisted

To grant access to specific websites, add them to the **Allowed list**.



The screenshot shows the 'Allowed list' section of the Mobile Guardian interface. At the top, there is a heading 'Allowed list' and a green padlock icon followed by the text 'Enter a URL to allowed list'. Below this is a text input field containing 'www.example.com'. To the right of the input field is a grey 'Add' button. Below the input field is a table with one row. The table has a header row with the text 'Name'. The data row contains a green padlock icon, the URL 'https://www.nationalgeographic.com', and a trash can icon. The entire table is highlighted with a red border.

Figure 4.4.18: Allowed List

Use the **URL Tester** to verify that access to a particular URL is allowed.



The screenshot shows the 'URL Tester' interface. It features a text input field containing 'https://www.nationalgeographic.com/' and a green 'Test' button. Below the input field, the text 'This URL is Whitelisted' is displayed. At the bottom, there is a message: 'If you would like to request a manual categorisation of this Domain, please email us the URL and the desired category.' The 'email us' part is a link.

Figure 4.4.19: URL Tester - The URL is Whitelisted

## Unit 4-5 - Viewing Reports

Click on **Webfilter Reports**, highlighted in red below. This will allow you to view your child's web browsing history.

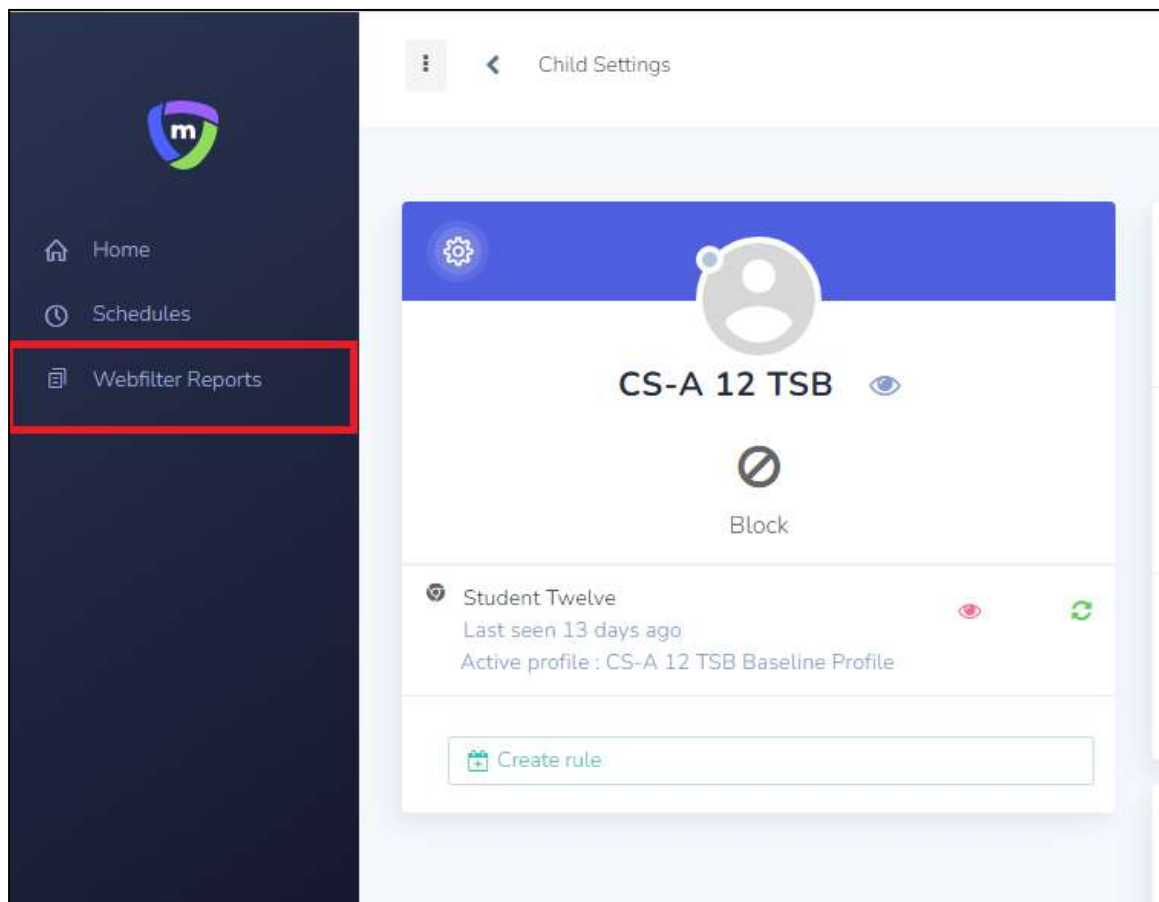


Figure 4.5.1: Access to Webfilter Reports

In **Advanced Filter**, select the date range to view your child's browsing history.

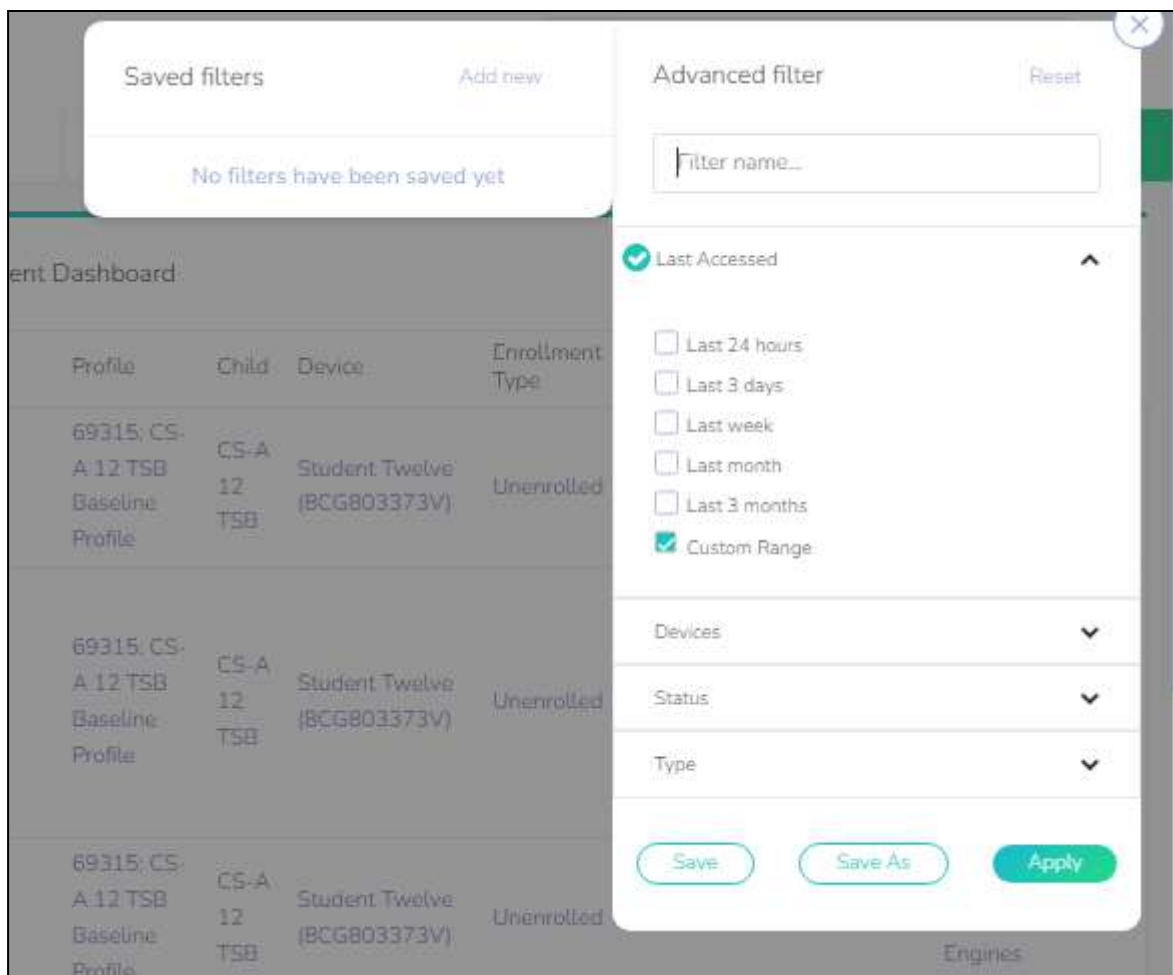


Figure 4.5.2: Webfilter Reports - Advanced Filter

Browser activity for Parent Dashboard			
Last Accessed	Activity	Profile	Child
19/07/2022, 15:33	<a href="https://www.google.com/search?gs_ssp=ejz4tTP1T...">https://www.google.com/search?gs_ssp=ejz4tTP1T...</a>	69315: CS-A 12 TSB Baseline Profile	CS-A 12 TSB
19/07/2022, 15:33	<a href="https://www.channelnewsasia.com/">https://www.channelnewsasia.com/</a>	69315: CS-A 12 TSB Baseline Profile	CS-A 12 TSB
19/07/2022, 15:33	<a href="https://www.google.com/search?q=channelnewsasia&amp;...">https://www.google.com/search?q=channelnewsasia&amp;...</a>	69315: CS-A 12 TSB Baseline Profile	CS-A 12 TSB
19/07/2022, 15:32	<a href="https://tinder.com/">https://tinder.com/</a>	69315: CS-A 12 TSB Baseline Profile	CS-A 12 TSB
19/07/2022, 15:32	<a href="https://www.google.com/search?q=tinder&amp;rlz=1CAQ...">https://www.google.com/search?q=tinder&amp;rlz=1CAQ...</a>	69315: CS-A 12 TSB Baseline Profile	CS-A 12 TSB
19/07/2022, 15:32	<a href="https://www.youtube.com/">https://www.youtube.com/</a>	69315: CS-A 12 TSB Baseline Profile	CS-A 12 TSB

Figure 4.5.3: Browser Activity for Parent Dashboard

### Important Note

Parents will **only be able** to view the child's browsing activity **after school hours**.

Parents **will not** be able to view the browsing activity **during school hours**.

## Chapter 5: Application Installation

### Unit 5-1 - Chromebooks

This section describes how you can enable the Chrome Web Store to install Apps/Extensions.

#### Important Note

By default, the Chrome Web Store is blocked by the school to prevent students from installing applications not conducive for learning purposes.

Should you wish to allow Chrome Apps/Extensions to be installed, they will remain usable during school hours. Thus, it is important to make sure that your child/ward installs **ONLY** appropriate extensions.

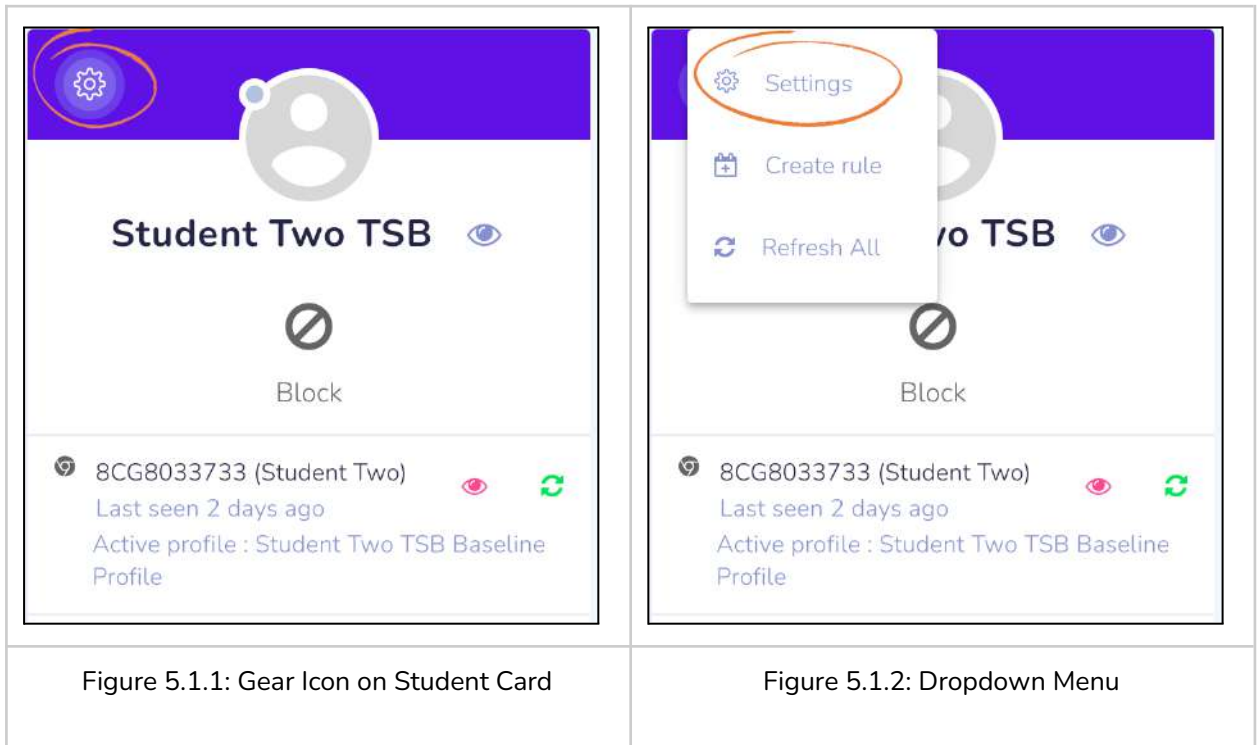
#### Enabling access to the Chrome Web Store

By default, the Chrome Web Store is blocked by the school, however if you wish to allow your child to install apps/extensions, you may override this using the following steps.

The Chrome Web Store is accessible at <https://chrome.google.com/webstore>



To modify the filter, click on the gear icon on the student card, then click on **"Settings"** from the dropdown menu.



Then click on the **"Safe Content"** panel to open the Web Filter page.

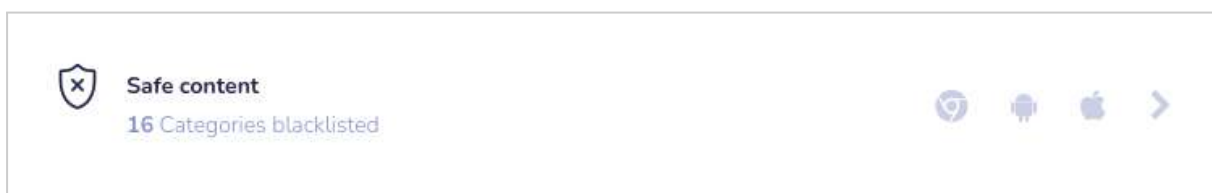
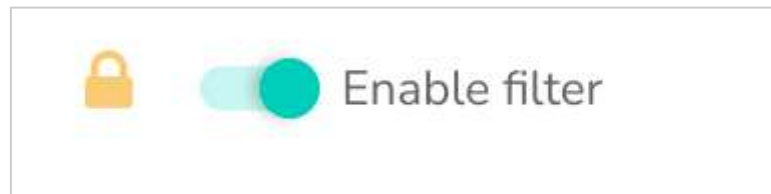


Figure 5.1.3: Safe Content Section

The option is turned off by default, as shown below:



*Figure 5.1.4: Web Filter - Enable Filter*



*Figure 5.1.4: Turning on the Web Filter*

Scroll to the bottom of the page. The Blacklist section lists URLs that students cannot access on their devices. By ensuring that the URL <https://chrome.google.com/webstore> is not in this list, students will be able to access the Chrome Web Store.

### **Installing Chrome Apps/Extensions from the Chrome Web Store**

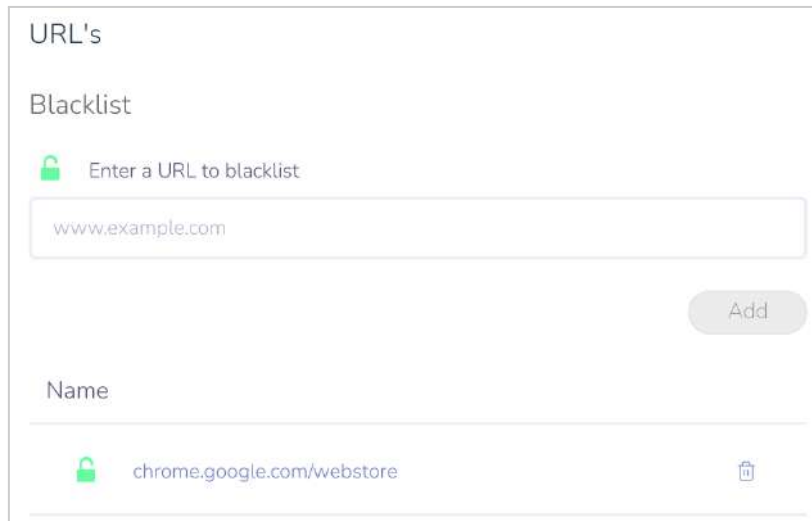
By turning on access to the Chrome Web Store, students are able to go to <https://chrome.google.com/webstore> to install Chrome apps/extensions from the Chrome Web Store.

### Disabling Access to the Chrome Web Store



The Chrome Web Store may be disabled by either:

- A. Adding the Chrome Web Store URL (chrome.google.com/webstore) to the URL black list, OR
- B. Turning off the Web filter

This will prevent the students from installing new apps/extensions from the Chrome Web Store. Note that this does *not* remove the apps/extensions installed by the students. The school administrator is also not able to remotely remove these apps/extensions installed by the students. In other words, the removal of the student-installed apps/extensions can only be done by the students themselves.



The screenshot shows a web interface for managing a URL blacklist. At the top, it says "URL's" and "Blacklist". Below this is a section for adding new URLs, with a green lock icon and the text "Enter a URL to blacklist". A text input field contains "www.example.com", and an "Add" button is to its right. Below this is a section for the current blacklist, with a "Name" label. A table lists the blocked URLs, with the first entry being "chrome.google.com/webstore", preceded by a green lock icon and followed by a trash can icon for deletion.

Name
 chrome.google.com/webstore 

*Figure 5.1.5: Blacklist -Chrome Web Store blocked*

## Unit 5-2 - iPads

If your child/ward is using an iPad, the Apple App Store is blocked by the school's setting. This section describes how you can enable the Apple App Store on your child's/ward's device.

### Enabling the App Store

To enable the Apple App Store, go to the settings page (see [Figure 10: Gear icon on student card](#)) and select "**Restrictions**".

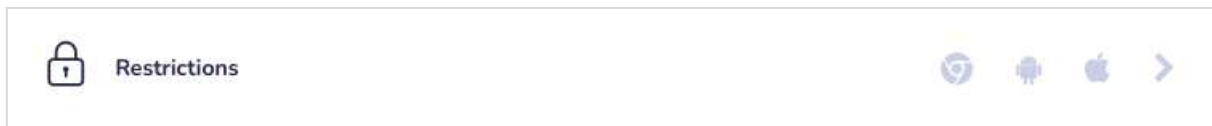


Figure 5.2.1: Restrictions

Select the "iOS" tab, then click on Details for the item "**Block application installation and removal**" to reveal more options. You can toggle availability of the App Store by selecting the checkbox for the item "**The App Store is disabled and its icon is removed from the Home screen. Users are unable to install or update their applications.**" Uncheck this option to enable Apple App Store or check it to disable.

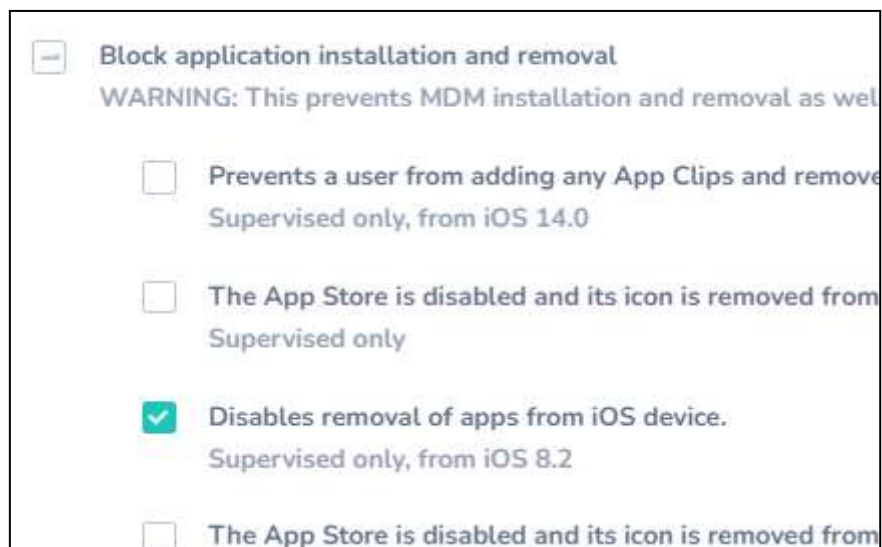


Figure 5.2.2: iOS Setting for Enabling the App Store

**Note:** The option "*Disables removal of apps from iOS device*" should be kept checked.

Scroll down, then click on the Details for the item "**Block Device Modification**". The item "**Account modification is disabled**" controls whether you are able to sign in with Apple ID on the device. (Uncheck to enable, check to disable.)



Figure 5.2.3: Account Modification is Disabled for Apple ID Sign-in

**Note:** To enable the App Store, you need to *uncheck* both of the following the items so that you can access the App Store *and* sign in with your Apple ID.:

**"The App Store is disabled and its icon is removed from the Home screen. Users are unable to install or update their applications."**

and

**"Account modification is disabled"**

Click on **Save** at the bottom-right corner of the screen to save the settings.

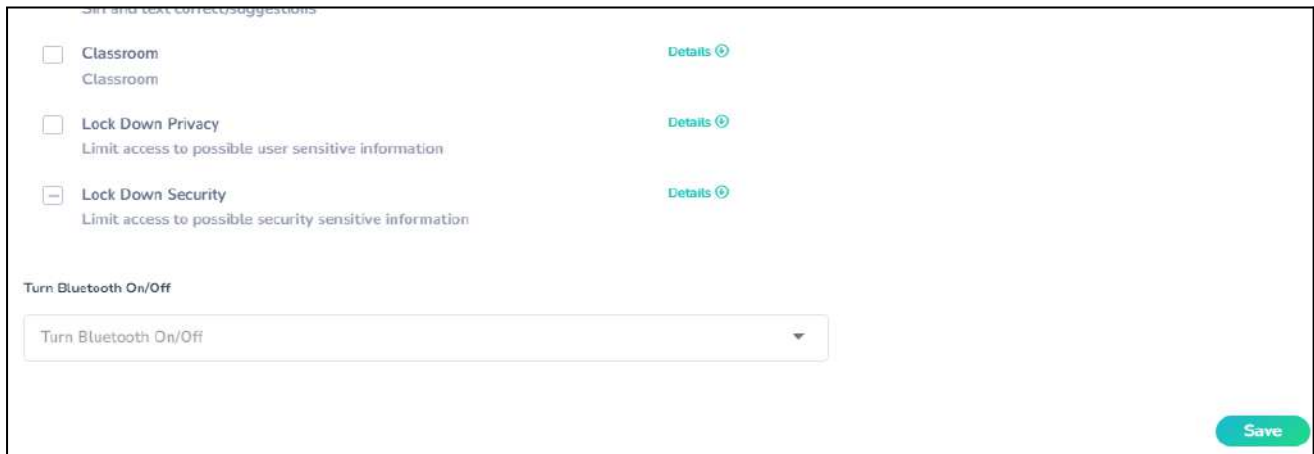


Figure 5.2.4: Location of Save button

Once these settings are turned on, go back to the home page and refresh the device so that the settings are "pushed" to the devices. The steps to do so are:

Click "Home" in the sidebar.

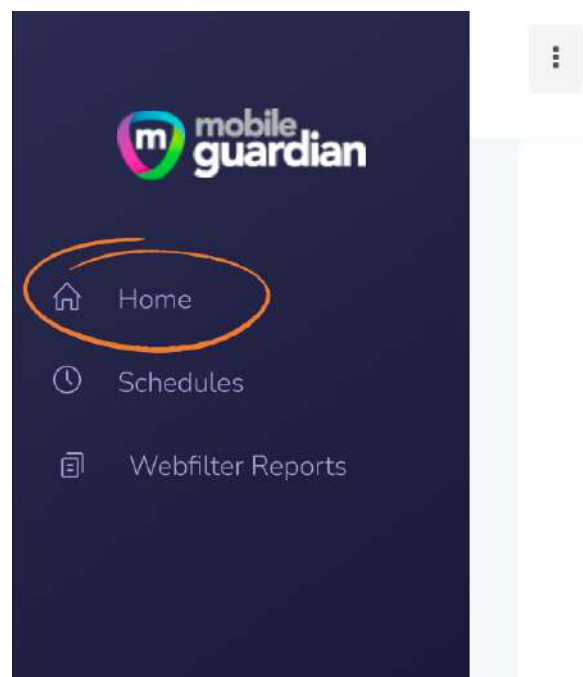
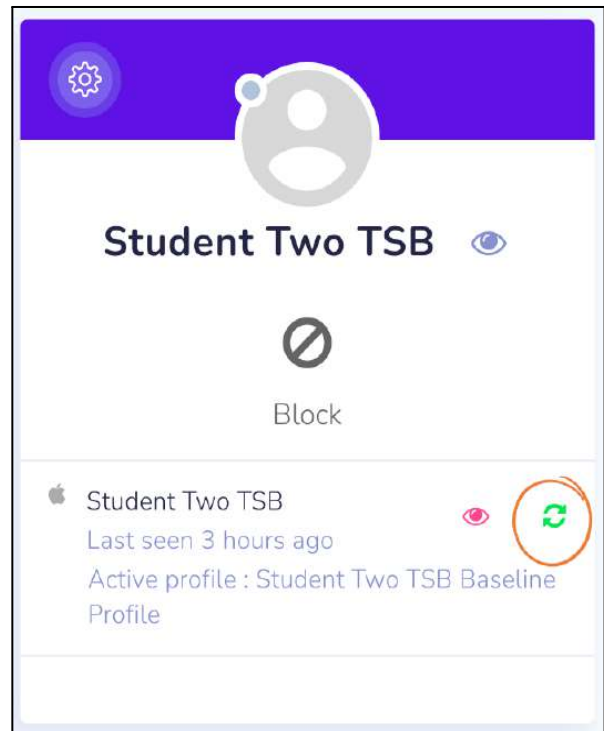


Figure 5.2.5: Home

Then click on the refresh button. This sends a command to the iPad to update itself with the new settings.

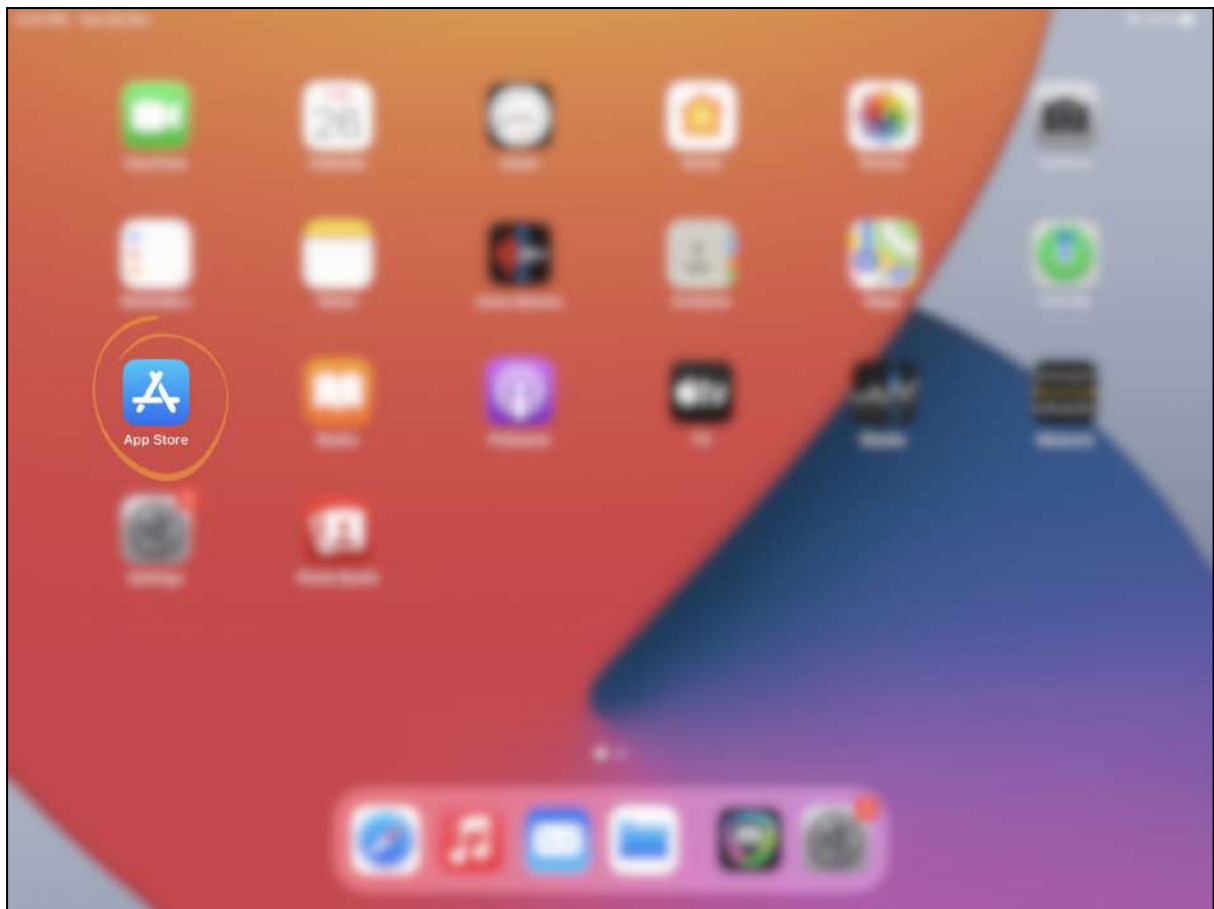


*Figure 5.2.6: Refresh*

**Note:** It is important to issue this refresh command after updating the settings. A common problem encountered where the App Store icon does not appear on the iPad has to do with the fact that the device has not been refreshed to receive the new settings.

### Installing iPad apps

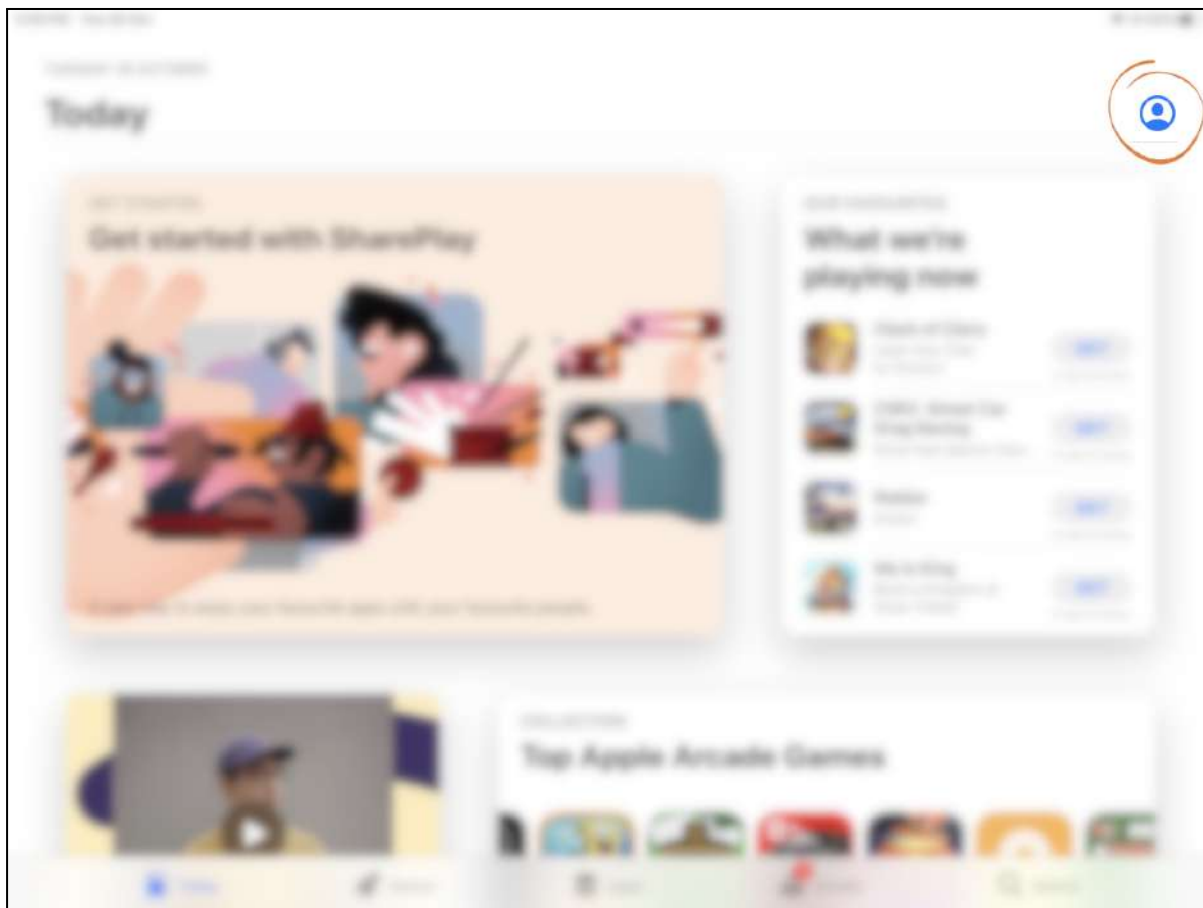
By following the steps described above, the student will then be able to see the App Store icon on the iPad and proceed to use it to search for apps in the App Store and install them.



*Figure 5.2.7: App Store icon on an iPad*

Tap on the App Store icon to bring up the App Store.





*Figure 5.2.8: Avatar icon in the App Store*

In the top right corner, there is an avatar icon. Tap on the icon to bring up the account sign-in page.

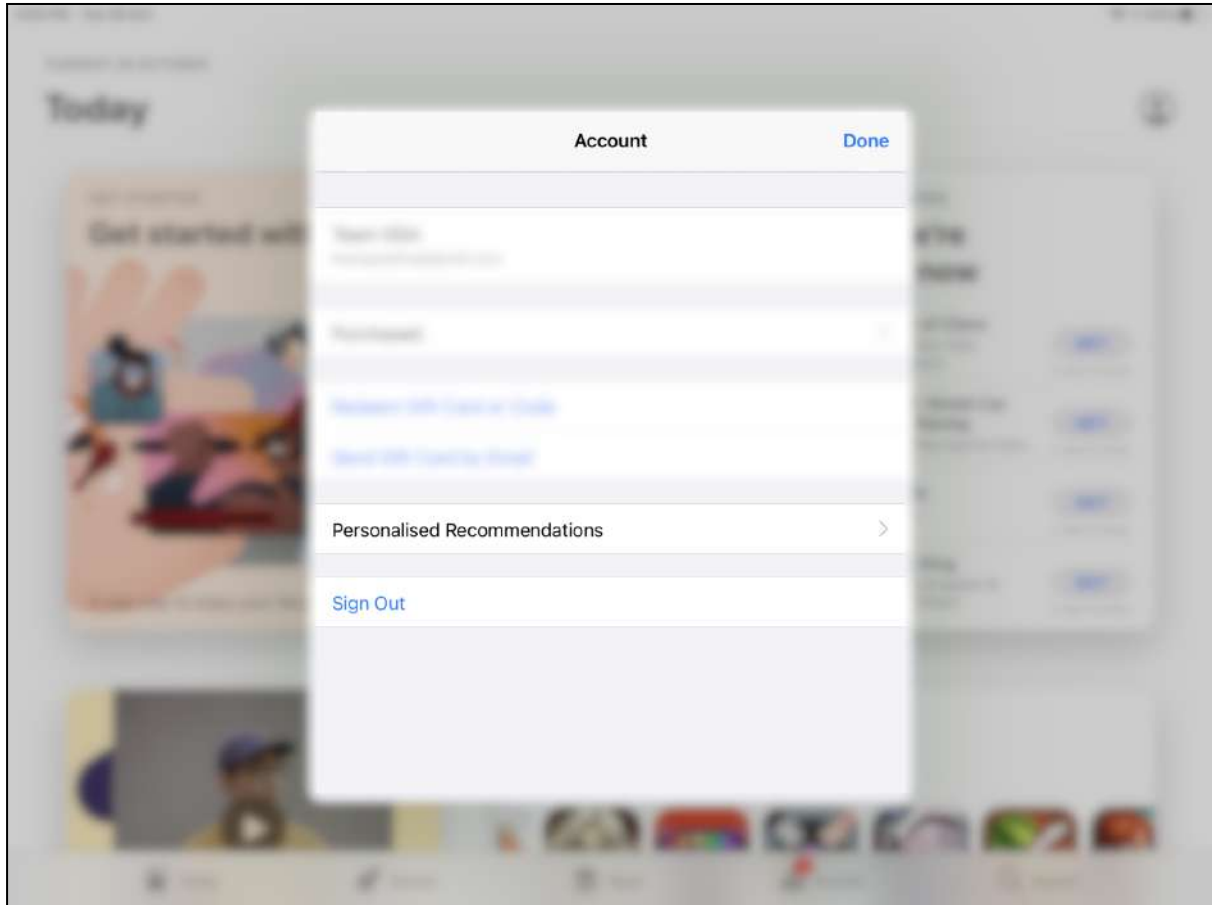
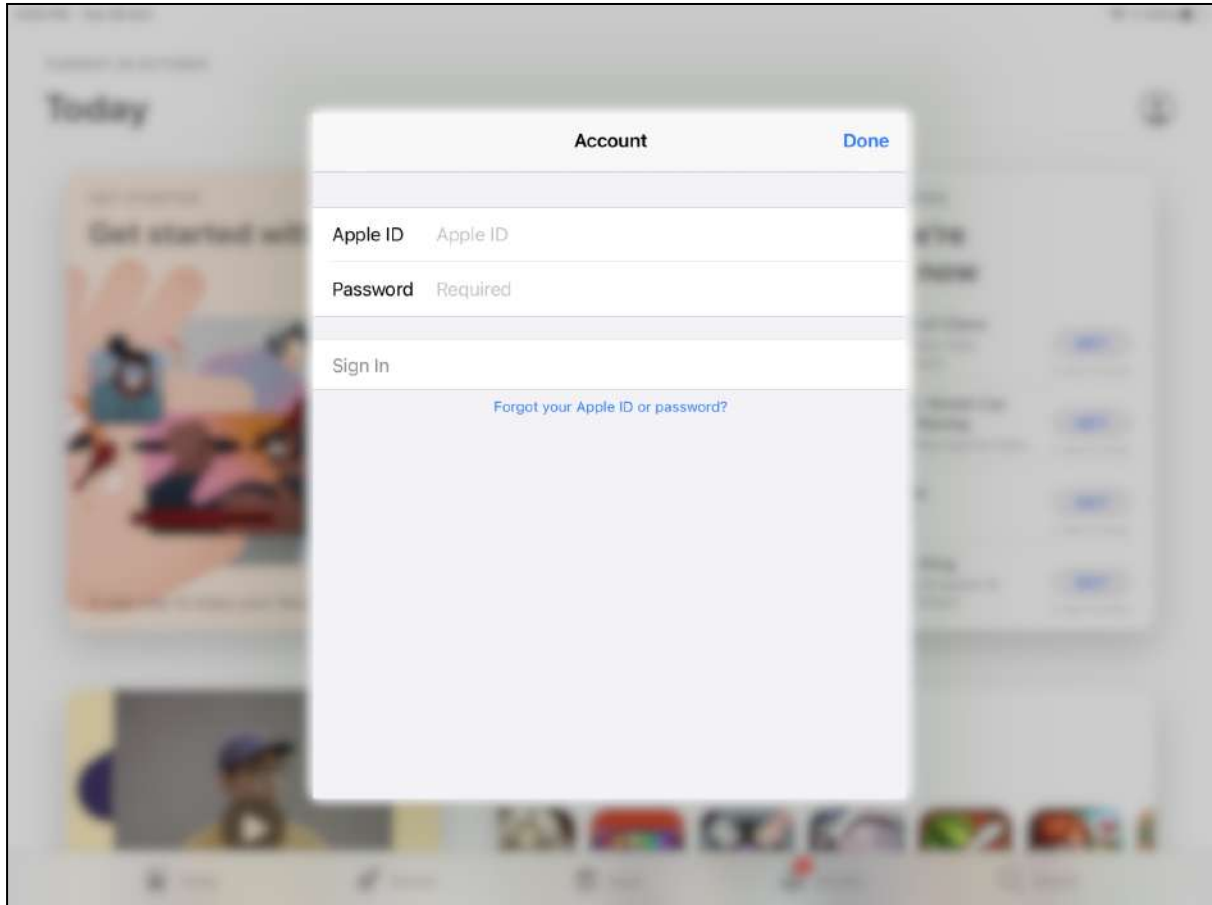


Figure 5.2.9: Existing account in App Store

If your child has been assigned an Apple ID by the school (also known as "managed Apple ID"), you may see an existing account..

If you wish to install custom applications, you need to sign out of the managed Apple ID account by tapping on the "Sign Out" button before proceeding with the next step.

Note: If you *do* sign out of the managed Apple ID account, your child needs to sign back in with the Apple ID account before he/she goes to school the next day as it may be needed for teaching and learning purposes (e.g. for use with Apple Classroom).



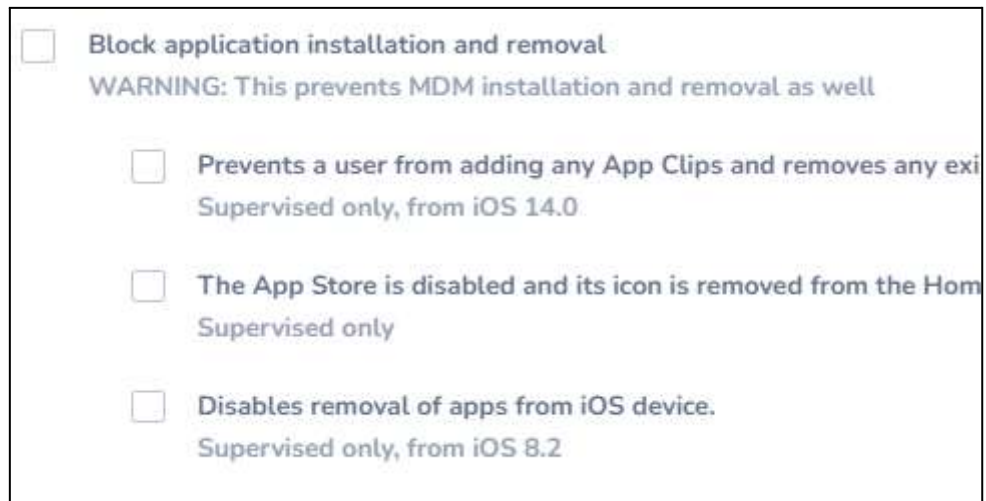
*Figure 5.2.10: Sign-in screen*

From the account sign-in page, enter your personal Apple ID and password, then tap "Sign In". After you are signed in, you will be able to install applications from the Apple App Store.

Note: If the account sign-in page is empty (as shown in the image above), it means that the setting "**Account modification is disabled**" is checked. This setting has to be unchecked (see Figure 18c).

## Uninstalling iPad apps

To do so, click on Details for the item "**Block application installation and removal**" to reveal more options. Uncheck the option "**Disables removal of apps from iOS device**" to allow apps to be removed from the iPad.



☐ **Block application installation and removal**  
WARNING: This prevents MDM installation and removal as well

- ☐ Prevents a user from adding any App Clips and removes any existing App Clips  
Supervised only, from iOS 14.0
- ☐ The App Store is disabled and its icon is removed from the Home screen  
Supervised only
- ☐ Disables removal of apps from iOS device.  
Supervised only, from iOS 8.2

Figure 5.2.11: Uncheck "Disables removal of apps from iOS device" to uninstall apps from the iPad

After saving this setting, remember to refresh the device for the setting to take effect.

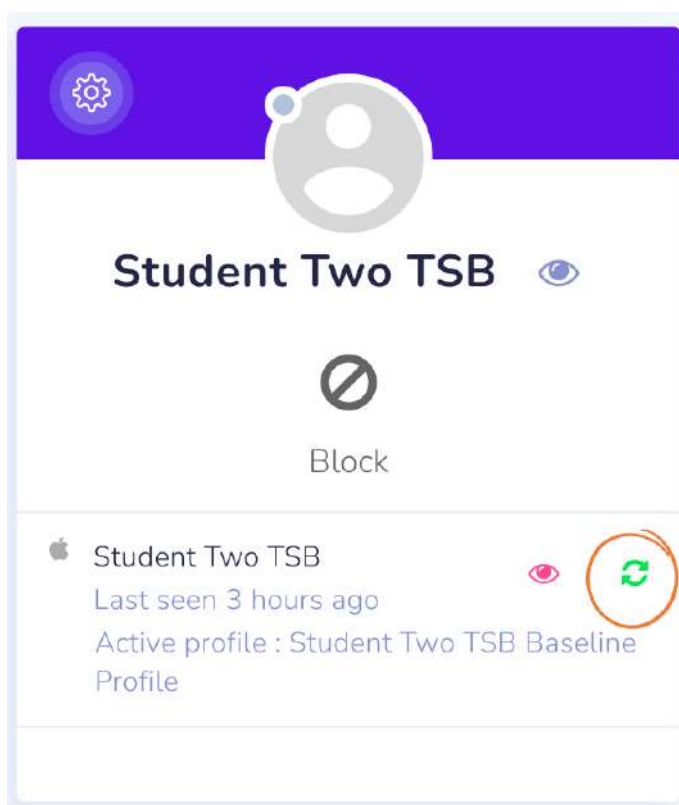


Figure 5.2.12: Refresh button to refresh the device with the new settings

After the desired apps have been uninstalled from the iPad, this setting needs to be turned back on.

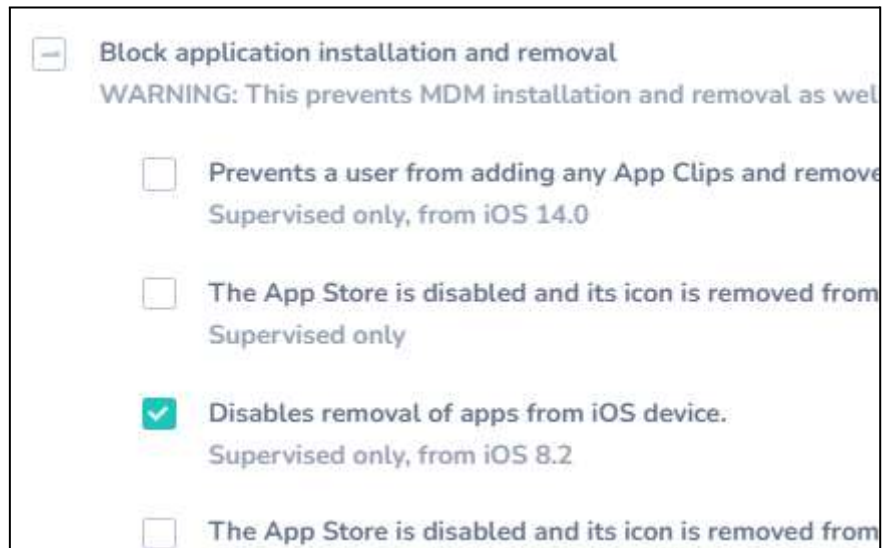


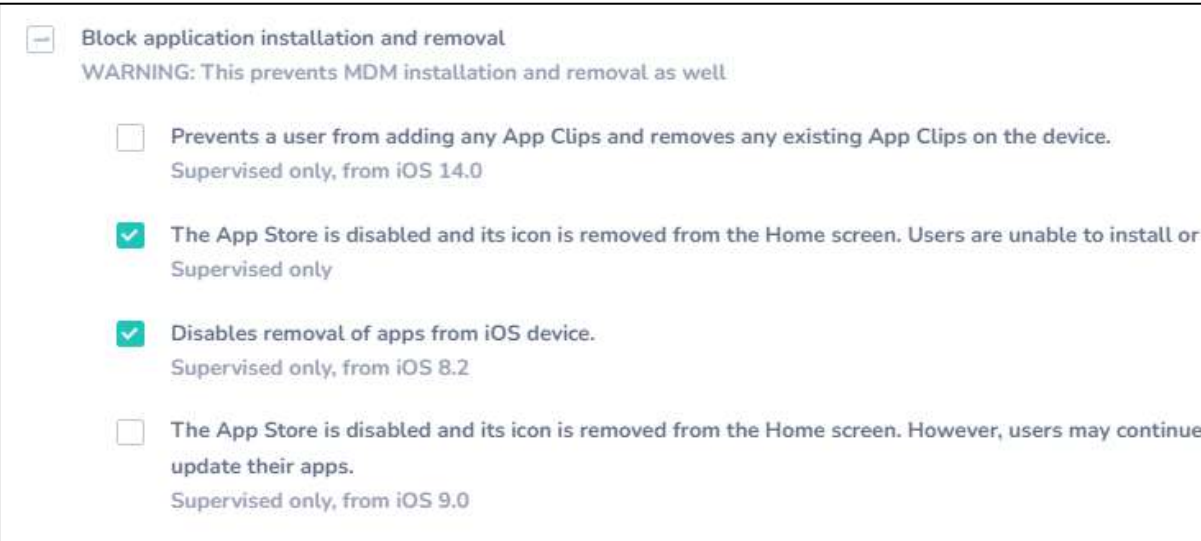
Figure 5.2.13: Restore the "Disables removal of apps from iOS device" to prevent uninstallation of other apps.

Similarly, after saving this setting, remember to click the Refresh button to refresh the device.

Note: It is important that the uninstallation of apps be performed under your supervision. This is because by turning on this capability, the Mobile Guardian app can also be uninstalled, thereby removing the content filtering protection.

## Disabling the App Store

To disable the App Store on the iPad, click on Details for the item "**Block application installation and removal**" to reveal more options. Check the option "**The App Store is disabled and its icon is removed from the Home screen. Users are unable to install or update their applications**" to prevent the App Store from appearing in the iPad.



☐ Block application installation and removal  
WARNING: This prevents MDM installation and removal as well

- ☐ Prevents a user from adding any App Clips and removes any existing App Clips on the device.  
Supervised only, from iOS 14.0
- ☒ The App Store is disabled and its icon is removed from the Home screen. Users are unable to install or update their applications.  
Supervised only
- ☒ Disables removal of apps from iOS device.  
Supervised only, from iOS 8.2
- ☐ The App Store is disabled and its icon is removed from the Home screen. However, users may continue to update their apps.  
Supervised only, from iOS 9.0

Figure 5.2.14: Setting To Disable App Store on iPad

After saving this setting, remember to click the Refresh button to refresh the device.

## Troubleshooting Guide

For basic troubleshooting of issues, visit the following link:

<https://helpdesk.gsatech.com.sg/portal/en/kb/articles/basic-troubleshooting-guide-for-parents>