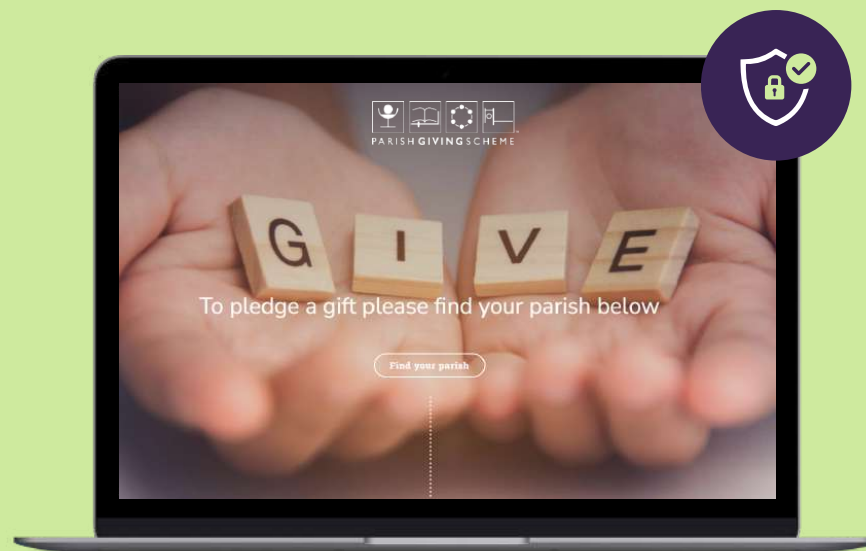




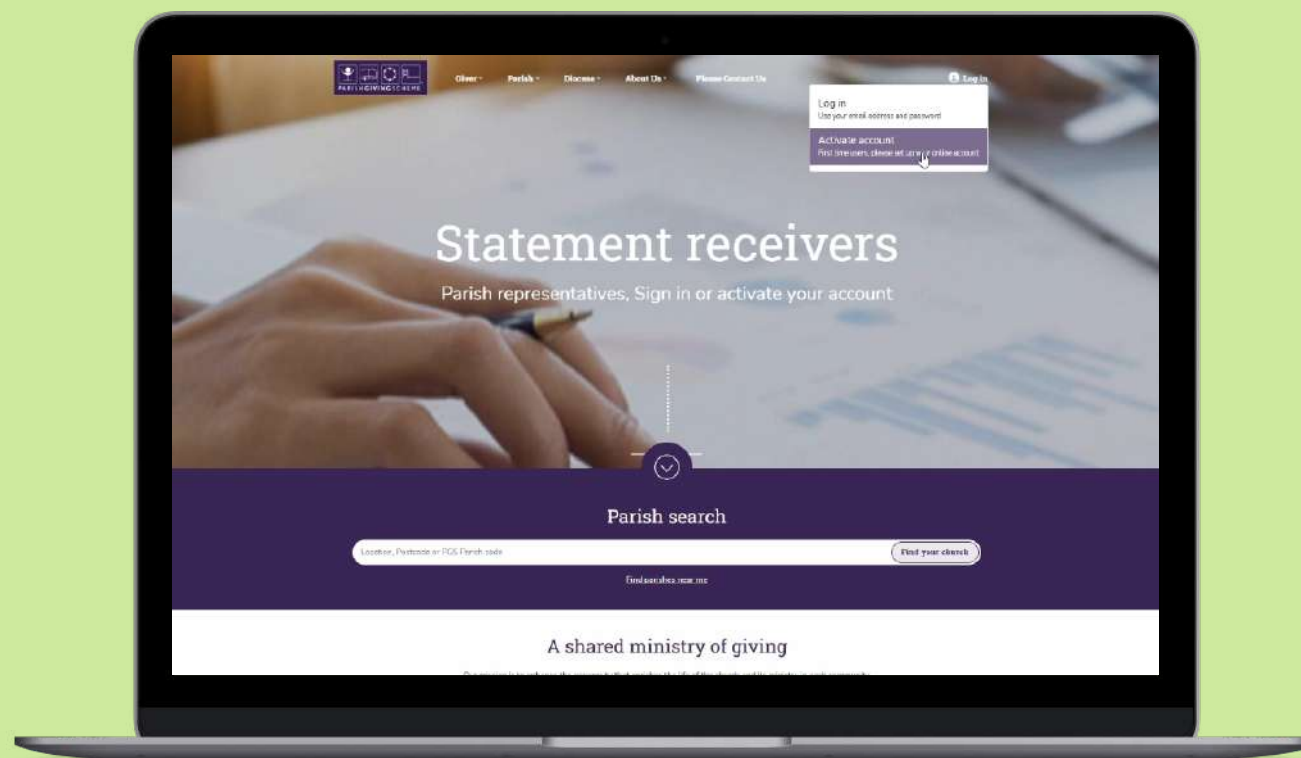
How to set up multi-factor authentication (MFA) for the first time



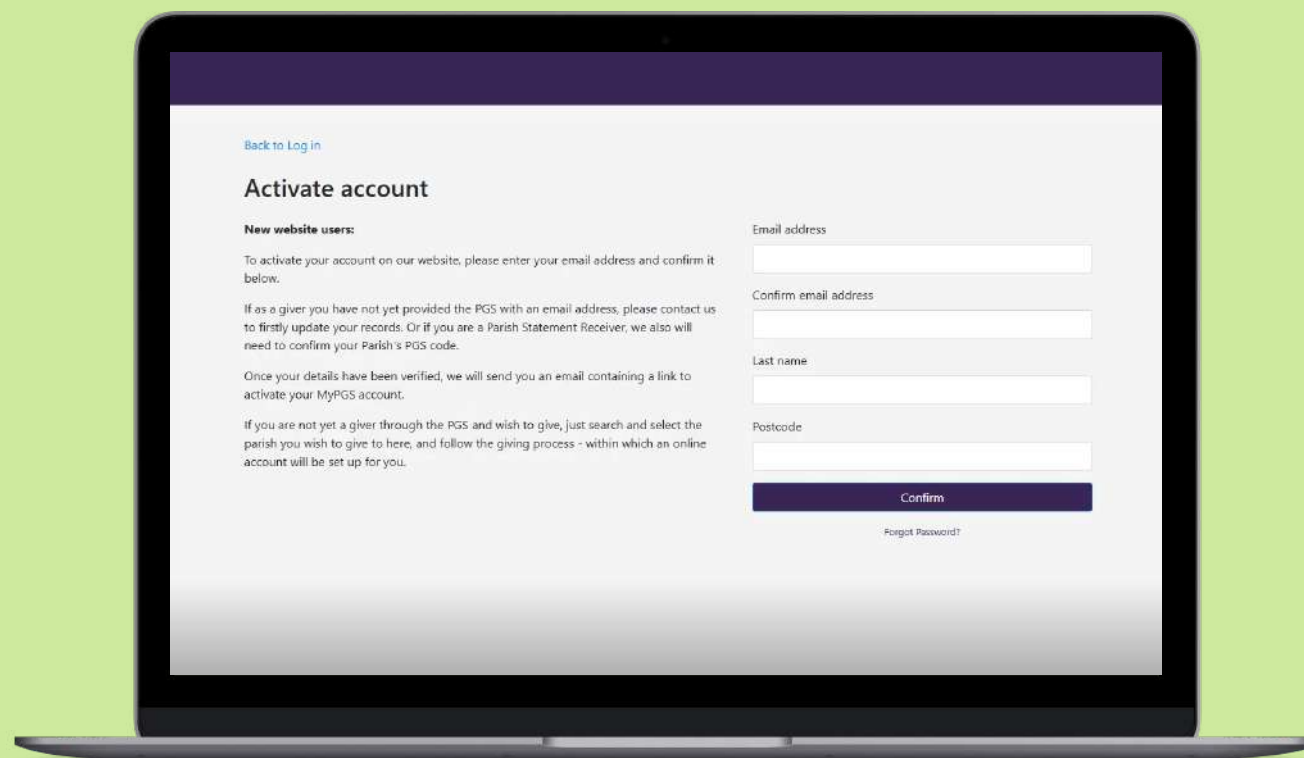


To maintain a high level of security for PGS users, we've updated our website which requires all users to update their password and set up multi-factor authentication. Multi-factor authentication is an extra layer of security for your account, designed to make sure that you are the only one who can access it, even if someone else knows your login details.

This guide will help you to set up multi-factor authentication for the first time and show you how to sign in to your PGS account going forward.



When you next log in to your PGS account on the new platform, you'll need to choose the option to 'Activate account'.



[Back to Log in](#)

Activate account

New website users:

To activate your account on our website, please enter your email address and confirm it below.

If as a giver you have not yet provided the PGS with an email address, please contact us to firstly update your records. Or if you are a Parish Statement Receiver, we also will need to confirm your Parish's PGS code.

Once your details have been verified, we will send you an email containing a link to activate your MyPGS account.

If you are not yet a giver through the PGS and wish to give, just search and select the parish you wish to give to here, and follow the giving process - within which an online account will be set up for you.

Email address

Confirm email address

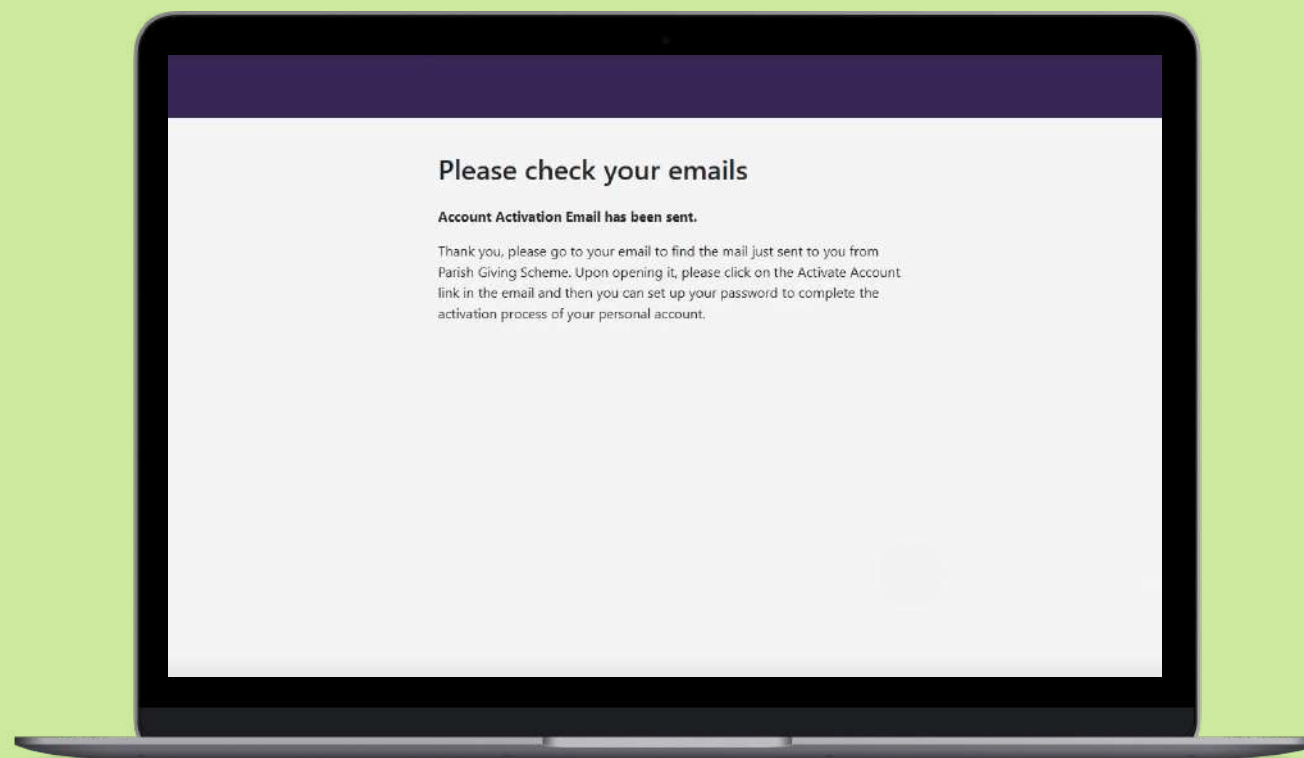
Last name

Postcode

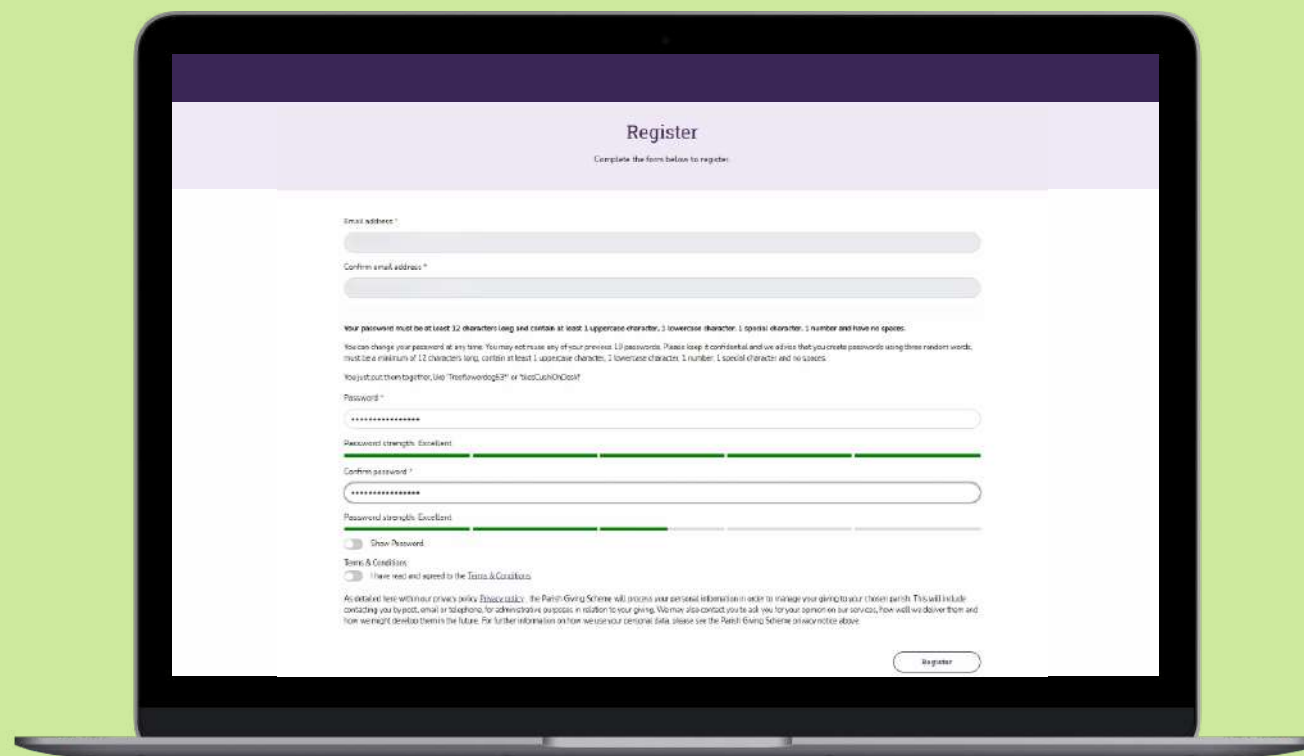
[Confirm](#)

[Forgot Password?](#)

You'll be prompted to enter and confirm the email address, last name and postcode associated with your account. Once you've completed the form, click 'Continue'.

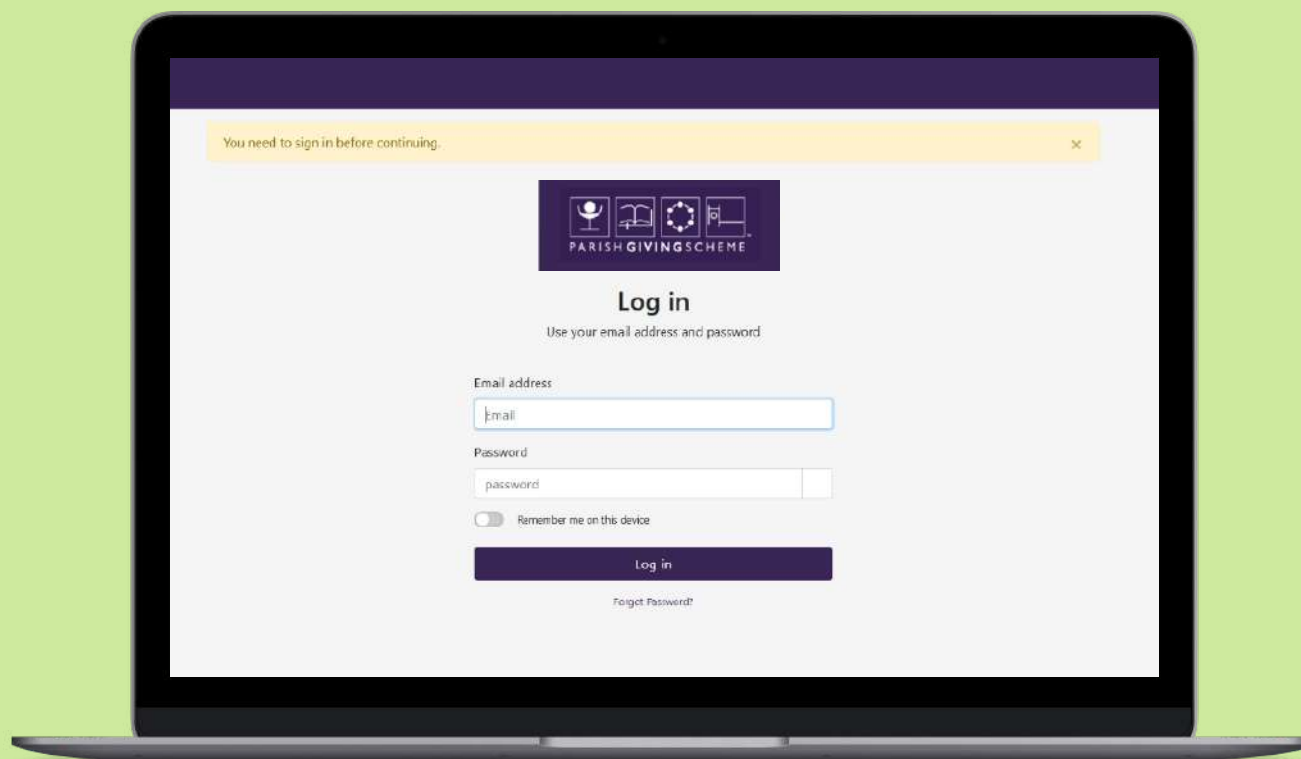


You will receive an email to the email address provided with a link to activate your account.

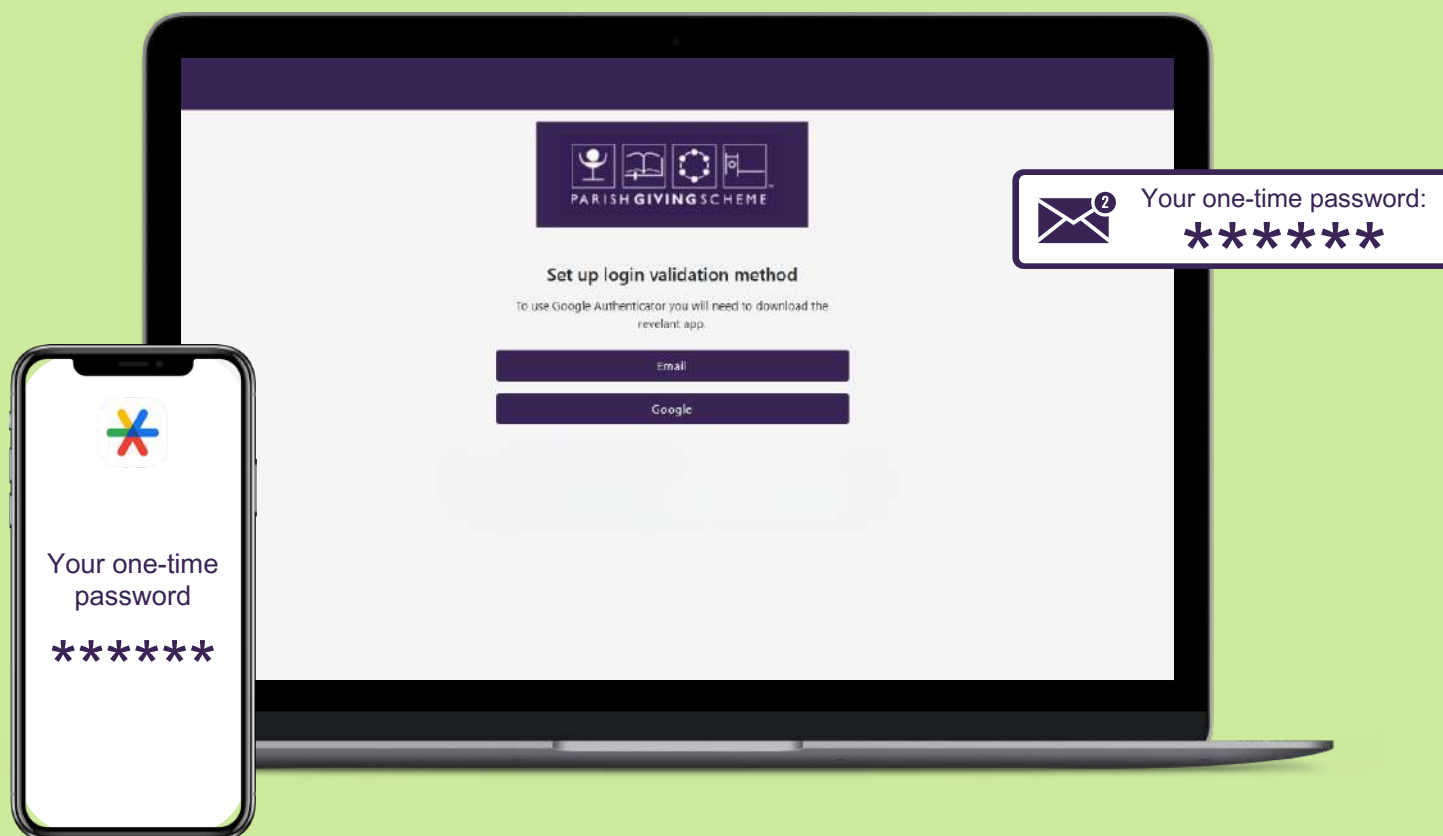


The laptop screen shows the 'Register' page of the Parish Giving Scheme. The page has a purple header with the title 'Register' and the instruction 'Complete the form below to register.' Below the header, there are two input fields for 'Email address' and 'Confirm email address'. A password policy section follows, stating that passwords must be at least 12 characters long and contain at least 1 uppercase character, 1 lowercase character, 1 special character, 1 number, and have no spaces. It also mentions that passwords can be changed at any time and should be a minimum of 12 characters long, containing at least 1 uppercase character, 1 lowercase character, 1 number, 1 special character, and no spaces. Examples of good passwords are 'TheParishGivingScheme' and 'TheParishGivingScheme123'. There are two input fields for 'Password' and 'Confirm password', each with a strength indicator. The password strength indicator shows 'Excellent' with a green bar. Below the password fields, there is a 'Show Password' toggle switch and a 'Terms & Conditions' section with a checkbox for 'I have read and agreed to the Terms & Conditions'. At the bottom right of the form is a 'Register' button.

Follow this link and set up a new password. You'll also need to read and accept the terms and conditions before clicking 'Register'.



You will then be taken to the login page on the PGS website to set up multi-factor authentication. You'll need to enter the email address and password for your PGS account, then click 'Log in'.

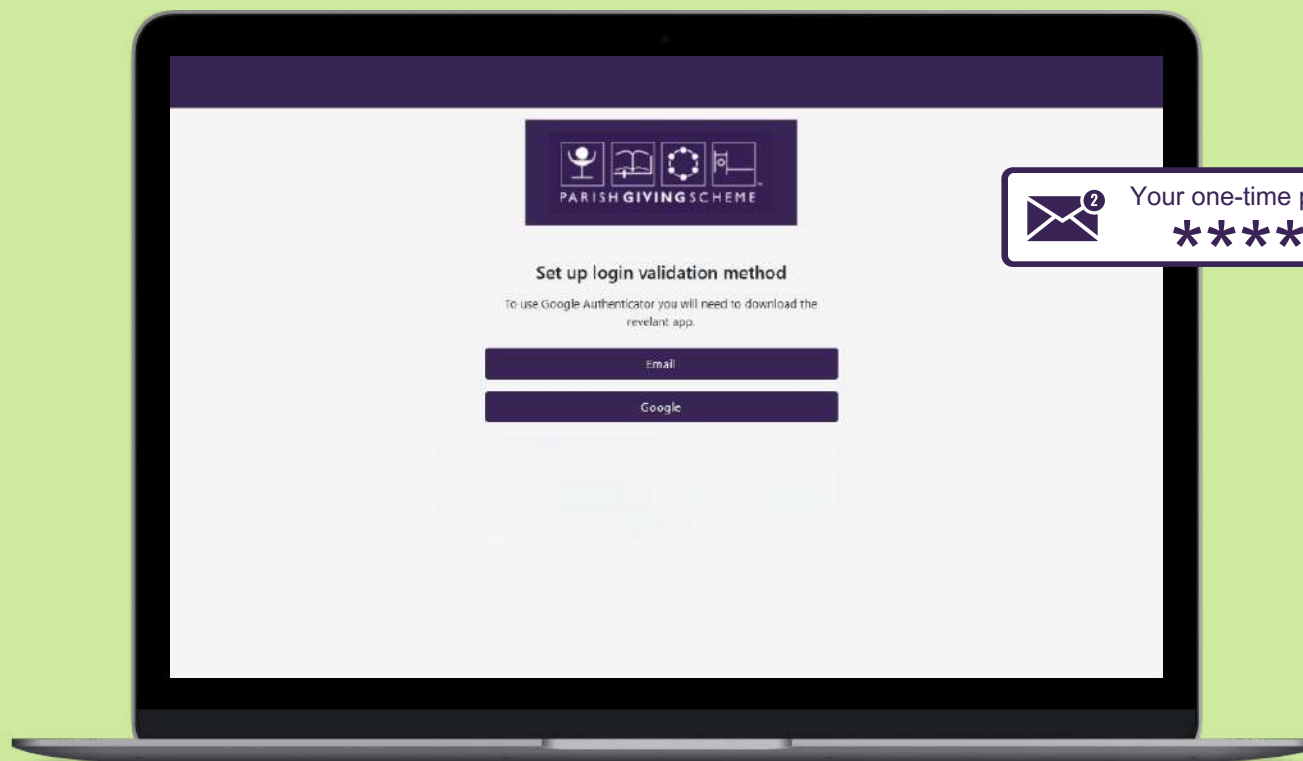


Decide how you would like to validate future logins to your PGS account. You can choose to receive a code through an email sent to your inbox, or through Google via an app on your smartphone.

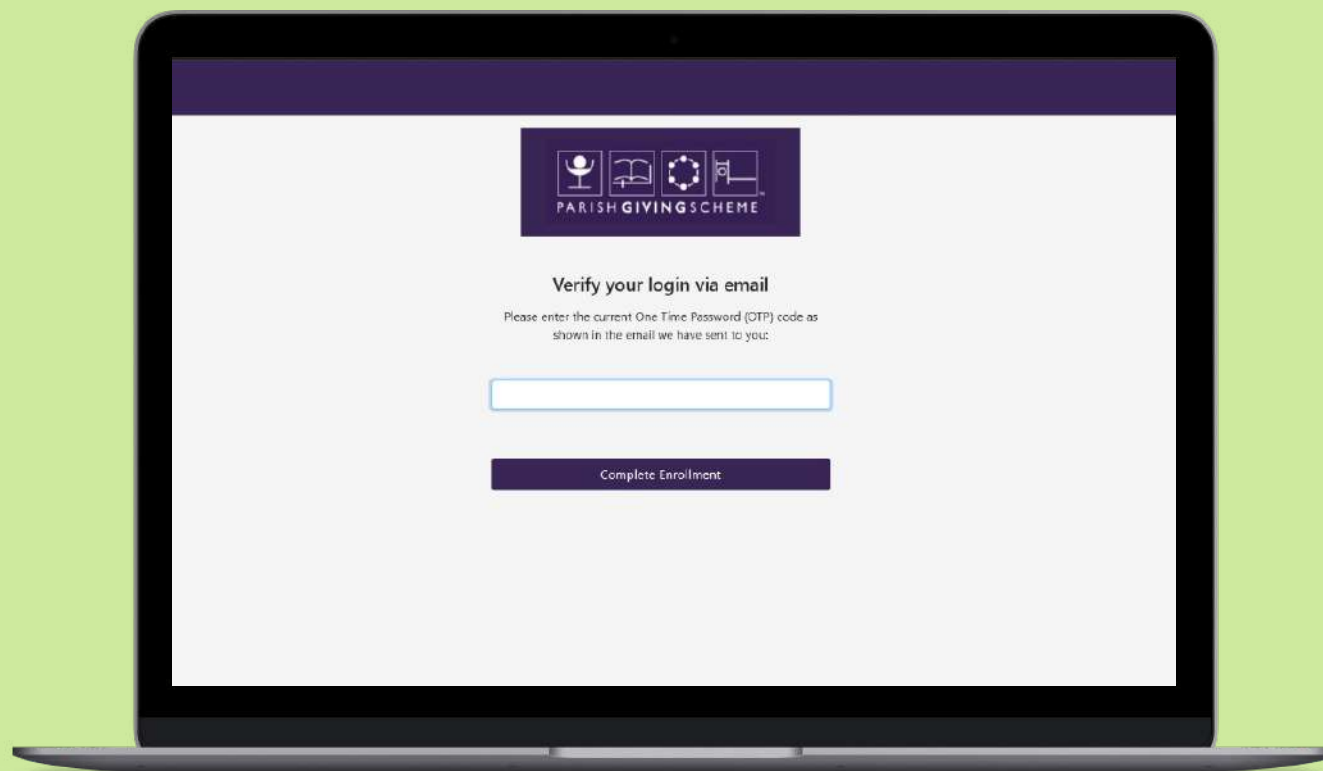


How to verify with email

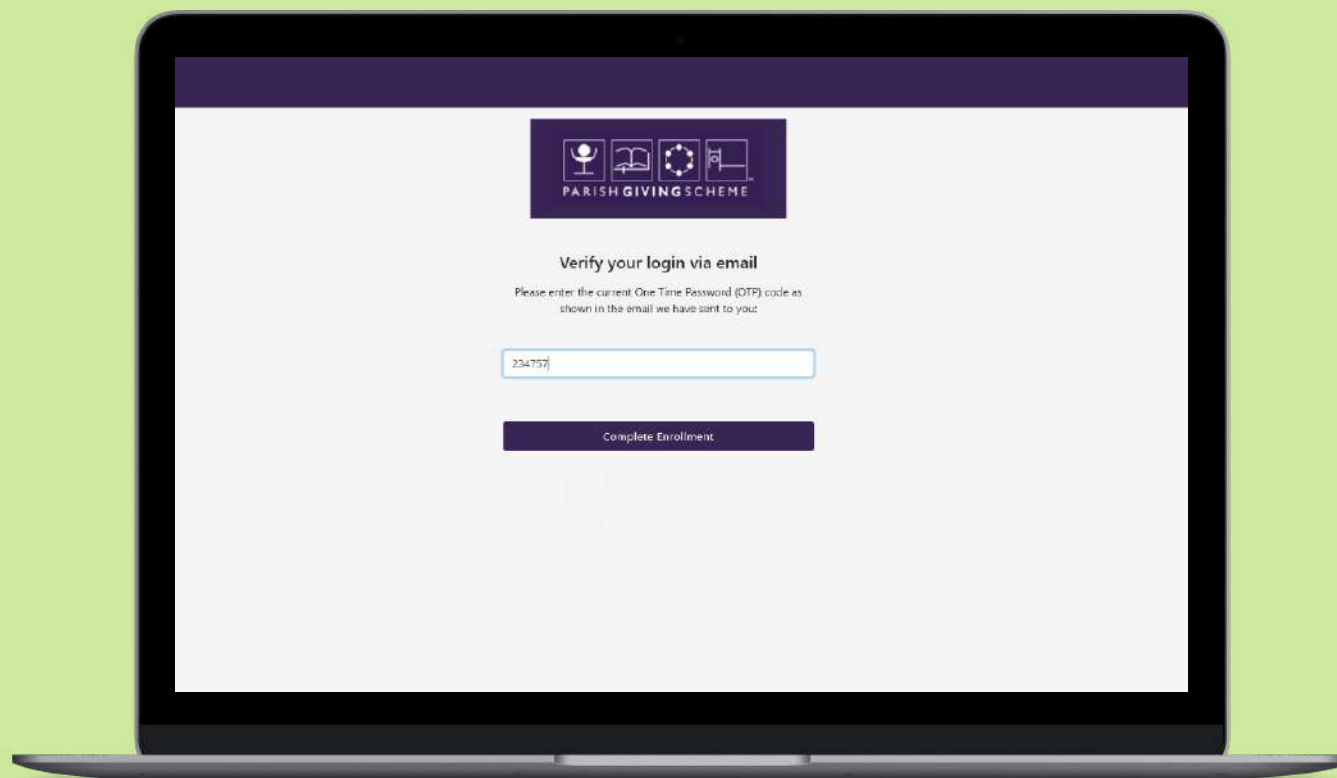




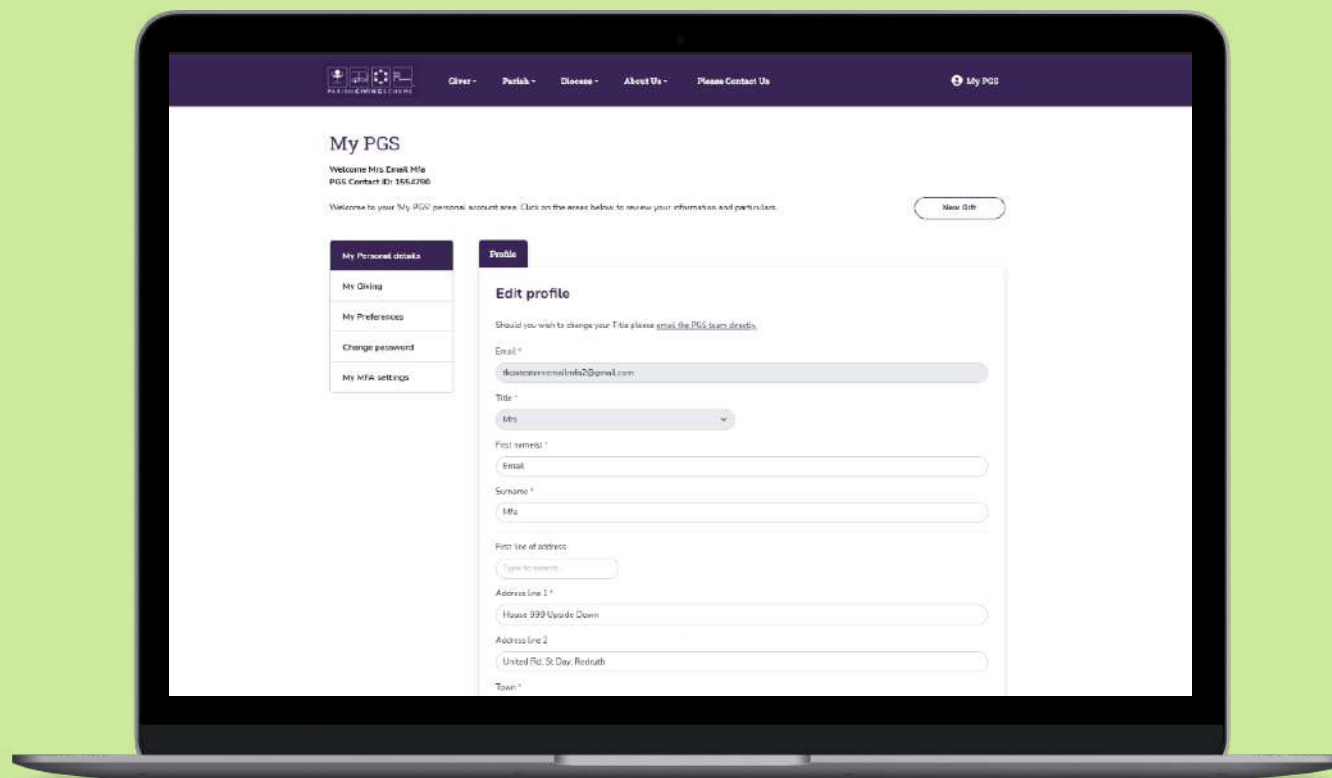
Follow the next few steps if you have chosen 'Email' as your validation method.



You will be asked to enter a one-time password, which has been sent to the email address associated with your PGS account.



Find the one-time password in your inbox, then enter the code and click 'Complete enrollment'.

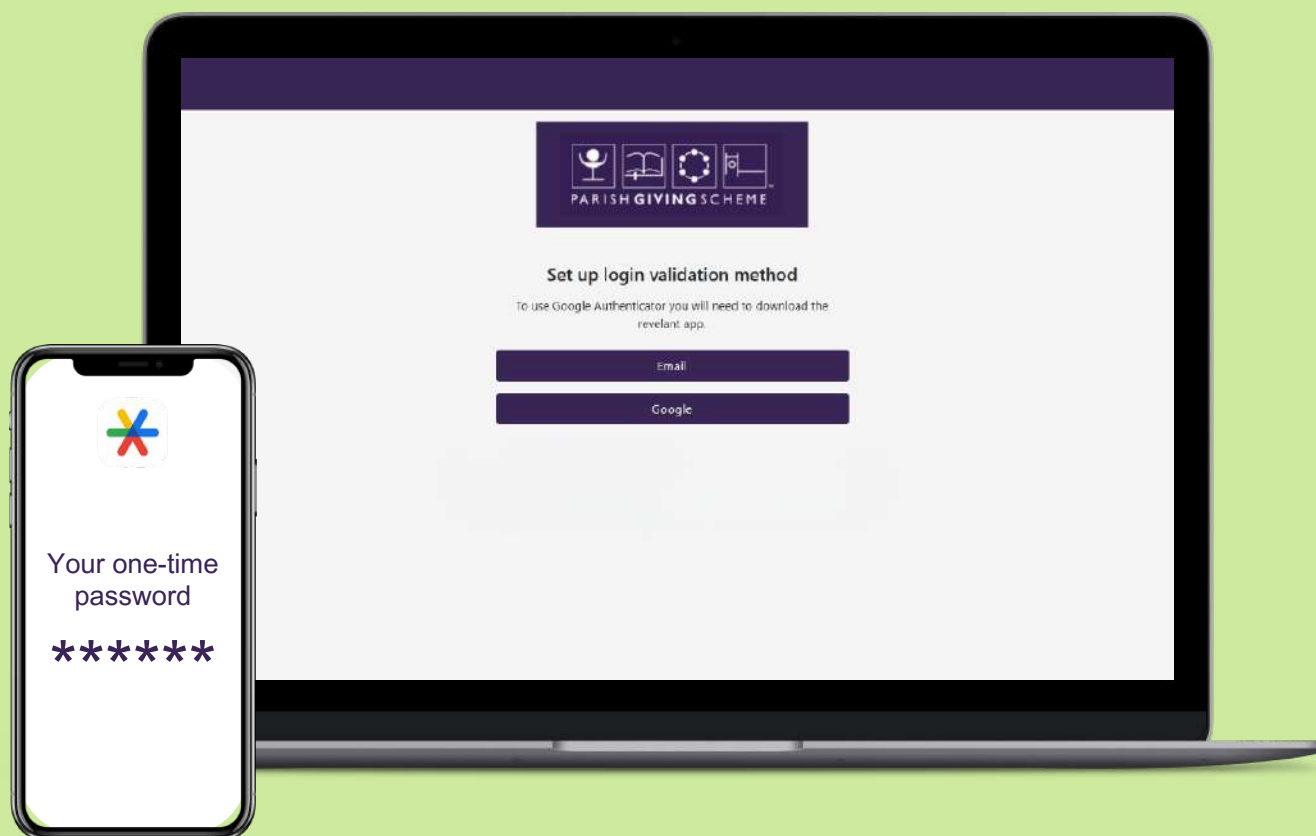


If you can see the portal homepage, you have successfully set up multi-factor authentication and you are now signed in to your PGS account.

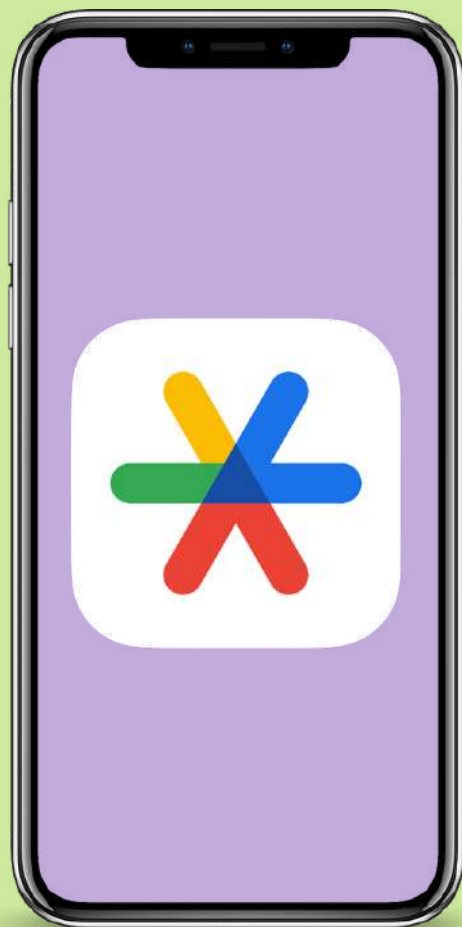


How to verify using Google

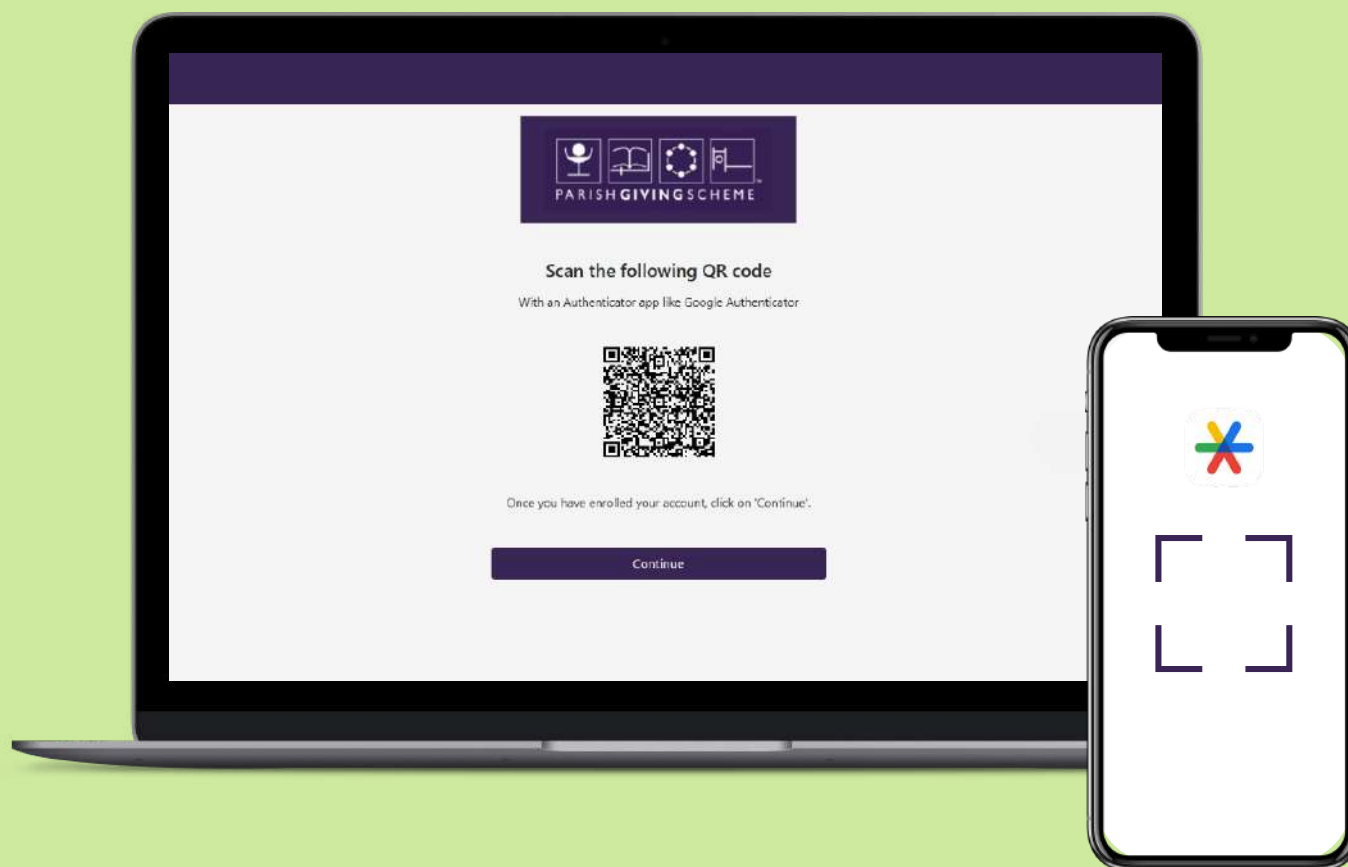




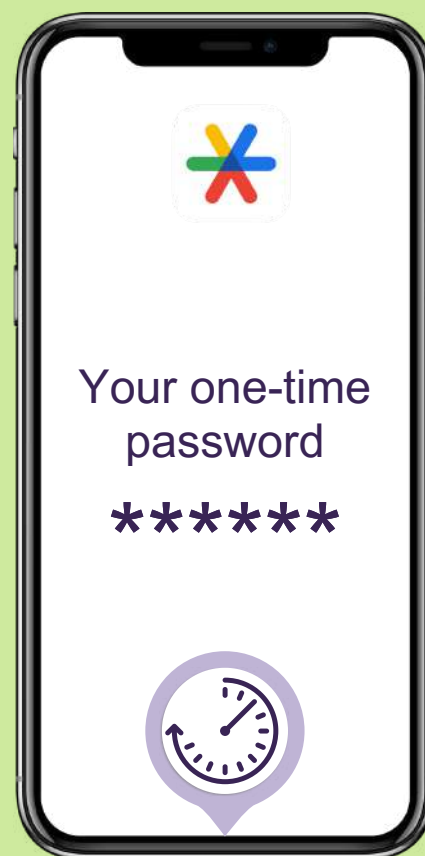
The next few steps only apply to users who have chosen 'Google' as their validation method.



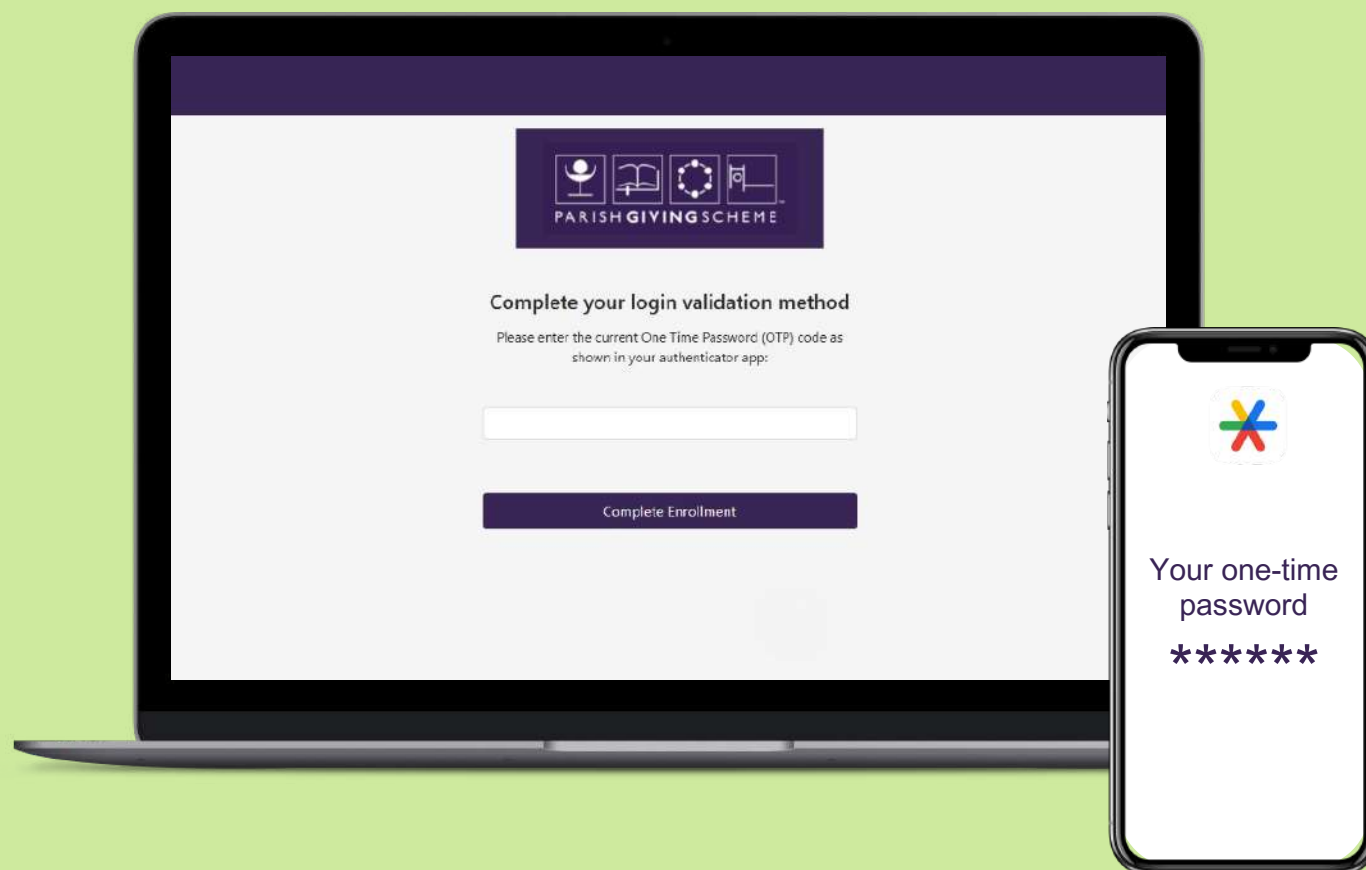
Use the app store on your smartphone to search for and download Google Authenticator. You're looking for the icon shown above.



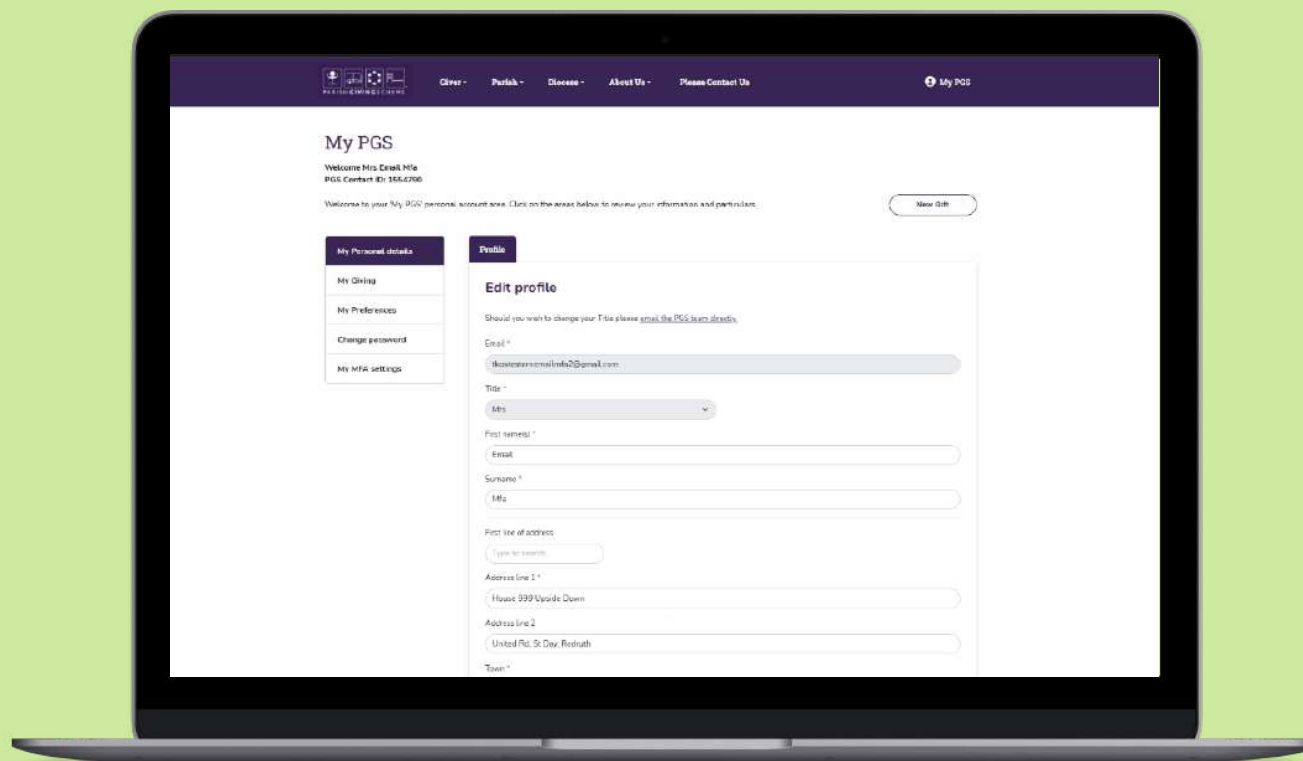
Once Google Authenticator has downloaded, open the app and scan the QR code shown on the PGS website.



Google Authenticator will produce a six-digit one-time password, which is valid for 30 seconds. Don't worry if you time out – a new code will generate automatically.



Enter the latest code on the PGS website, then click 'Complete enrollment'.

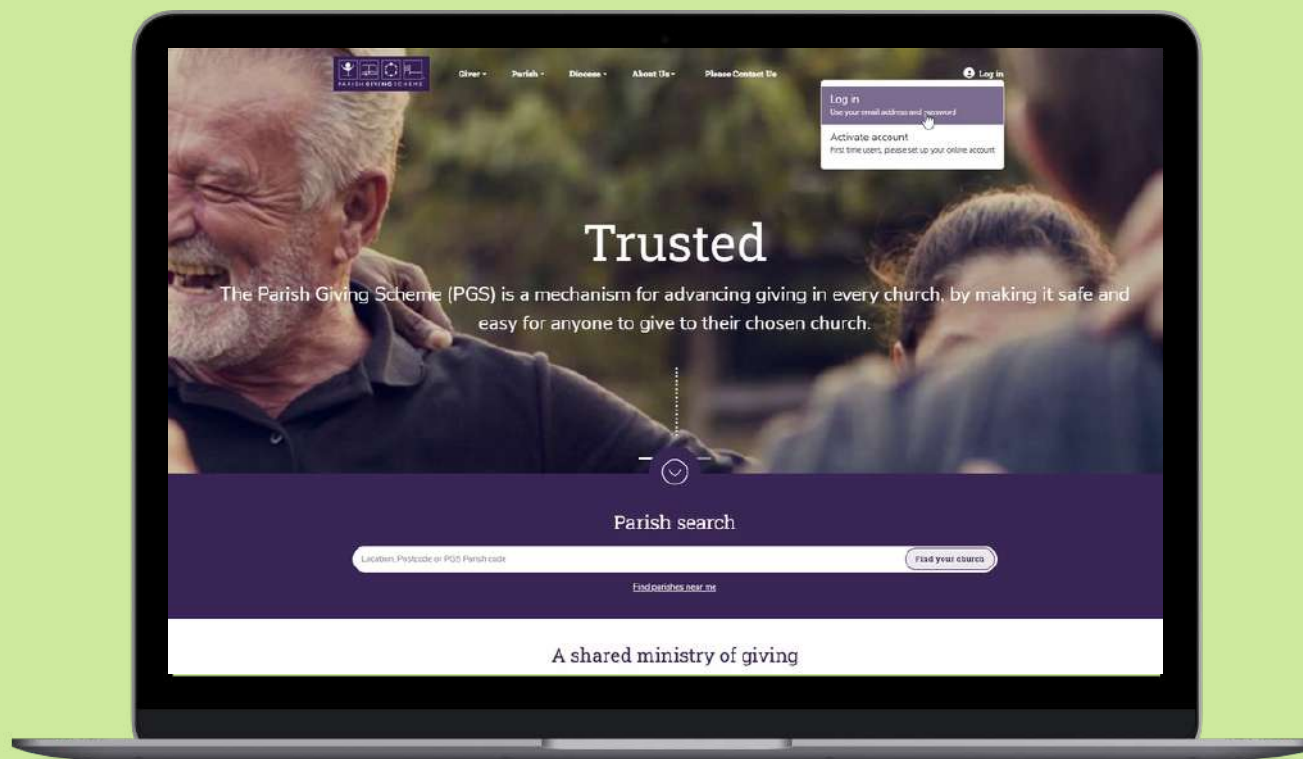


If you can see the portal homepage, you have successfully set up multi-factor authentication and you are now signed in to your PGS account.

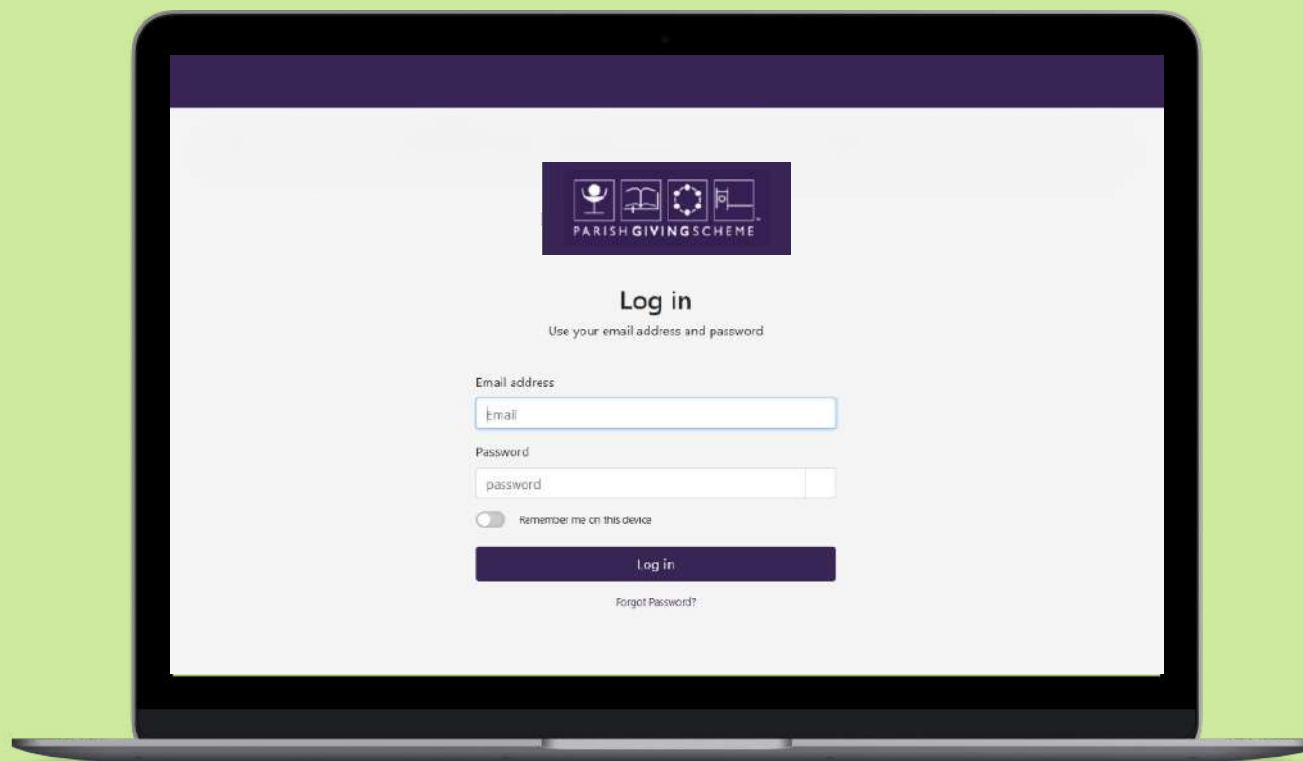


How to log in after setting up multi-factor authentication

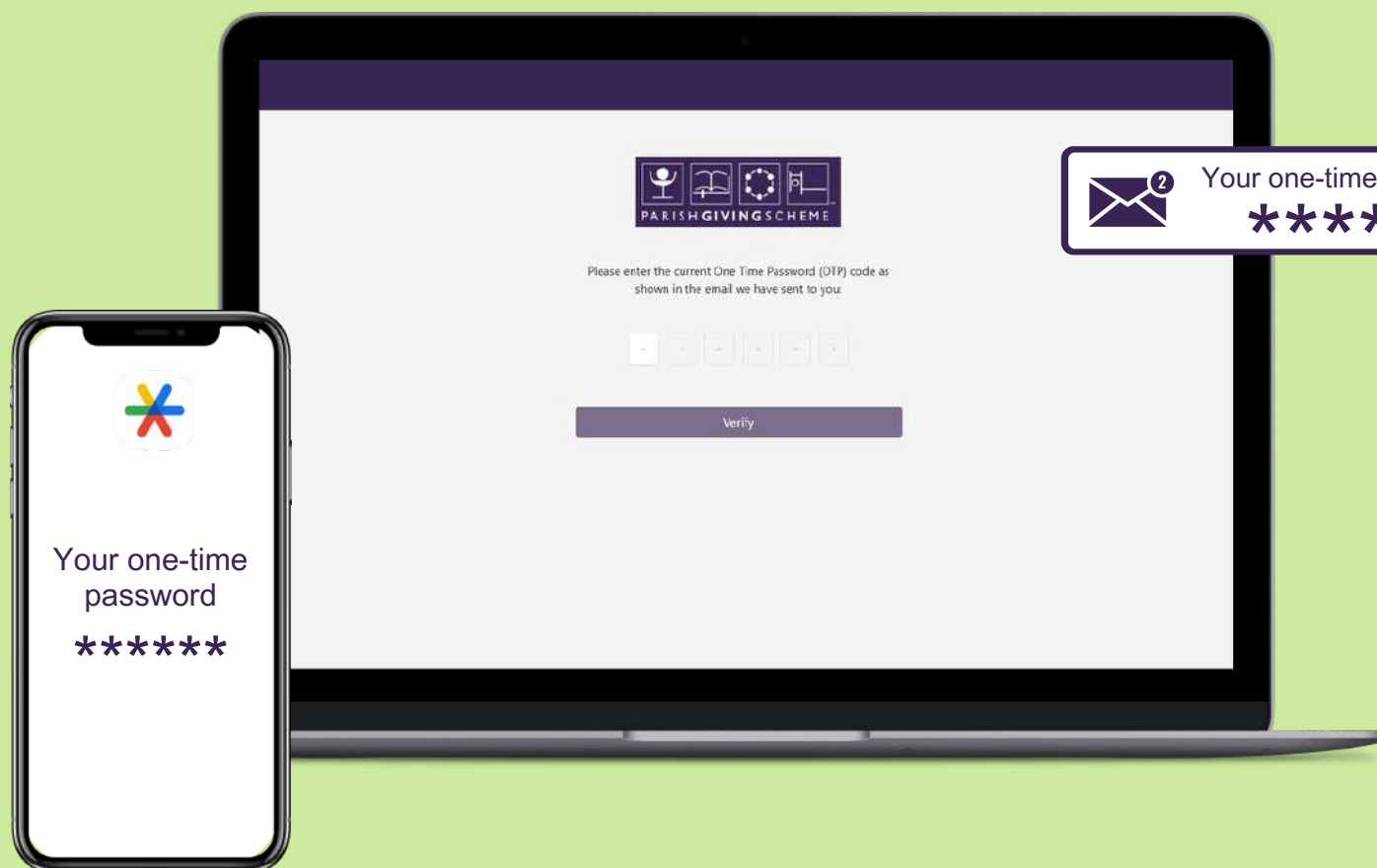




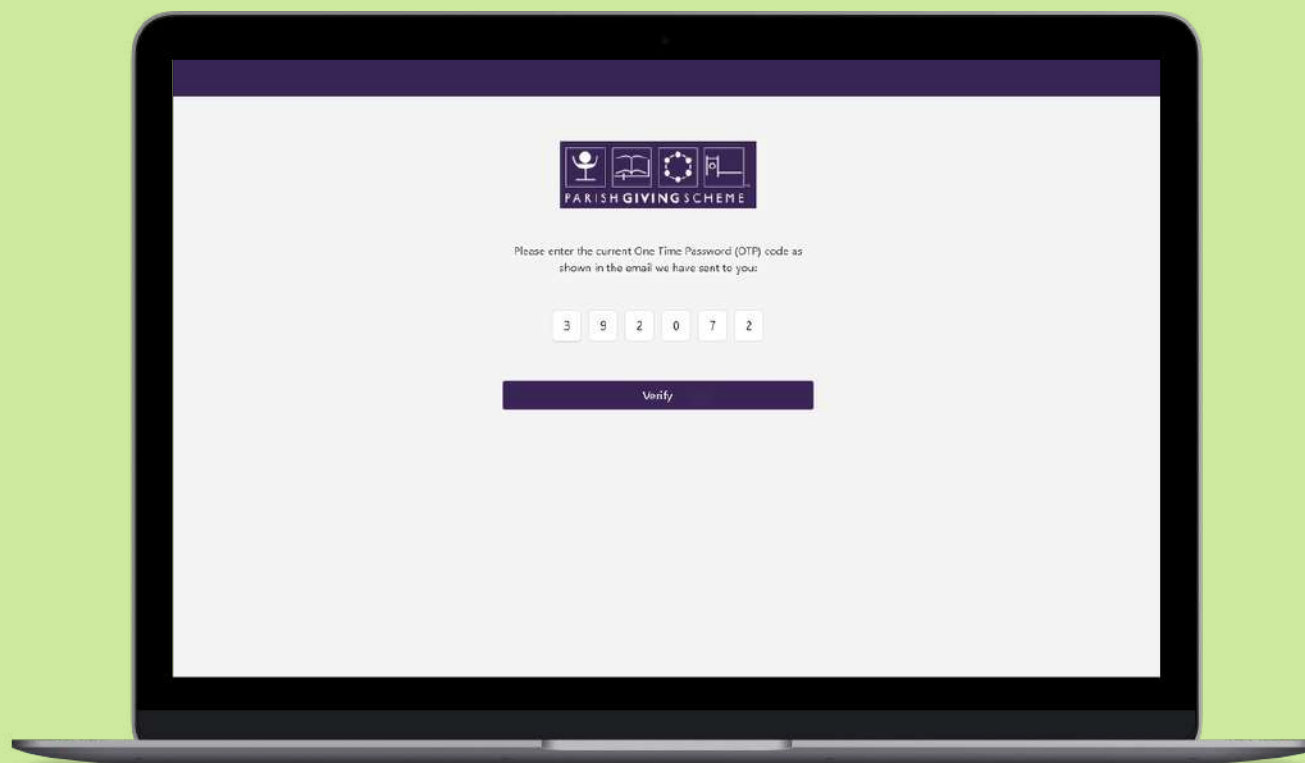
To sign in to your PGS account going forward, you'll need to use your chosen method to validate the login. Find the 'Log in' page to begin.



Enter your account details as normal, then click 'Log in'.



You'll be asked for a one-time password. If you set up multi-factor authentication with Google as your validation method, you'll find the code in the Google Authenticator app. If you chose to validate logins using an email address, your one-time password will be in your inbox.



Enter the code, then click 'Verify' to log in.

And that's it! With multi-factor authentication set up, your PGS account is now even more secure so you can continue to give with confidence.



We hope you found this guide helpful, but if you have any issues, please contact the PGS team on:



0333 002 1260