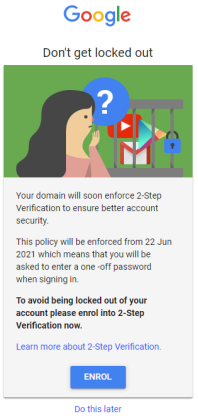
Using Enforced 2-Factor Authentication 2026

2-Factor Authentication for Your Brigshaw Trust Email

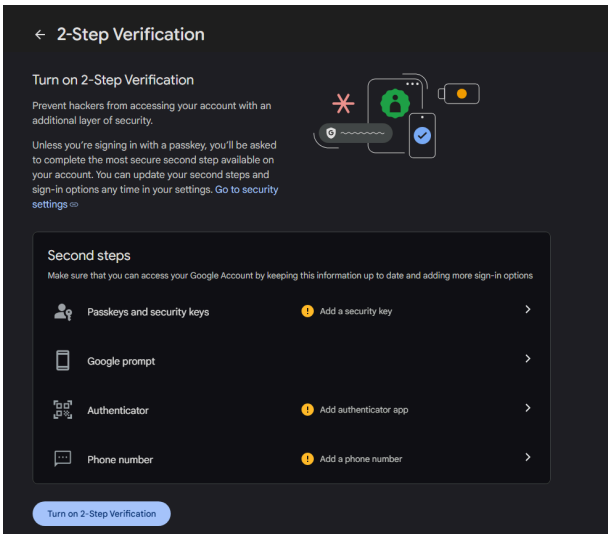
All staff email accounts now have 2-factor authentication enabled by default and can not be disabled. There are several different authentication methods available. We recommend you activate at least two methods, but in order to do so you must first set up text or voice authentication.

Getting Started with 2-FA

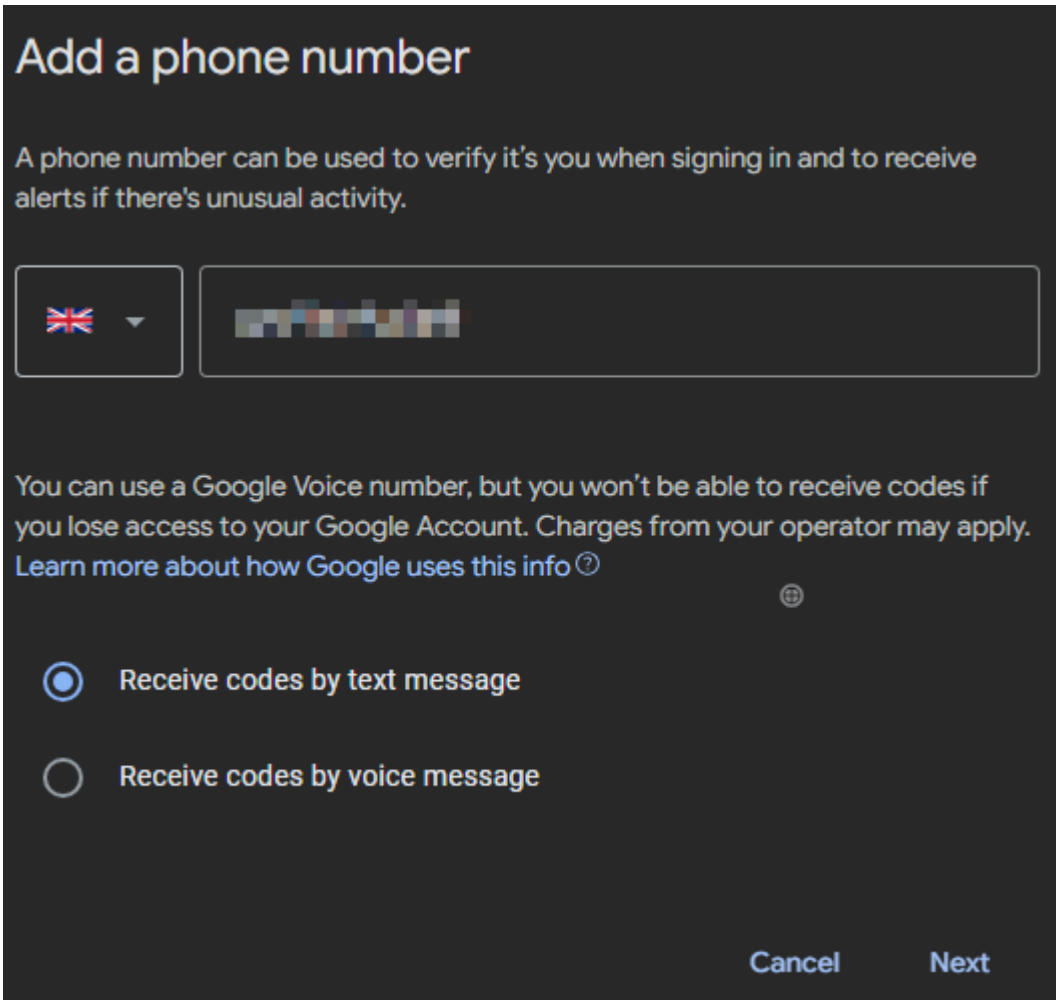
1. When you sign in to your Brigshaw Trust email account you will be presented with the following prompt. If this is a new account you will have already accepted the terms and changed your password to something only you know, and something you will remember.



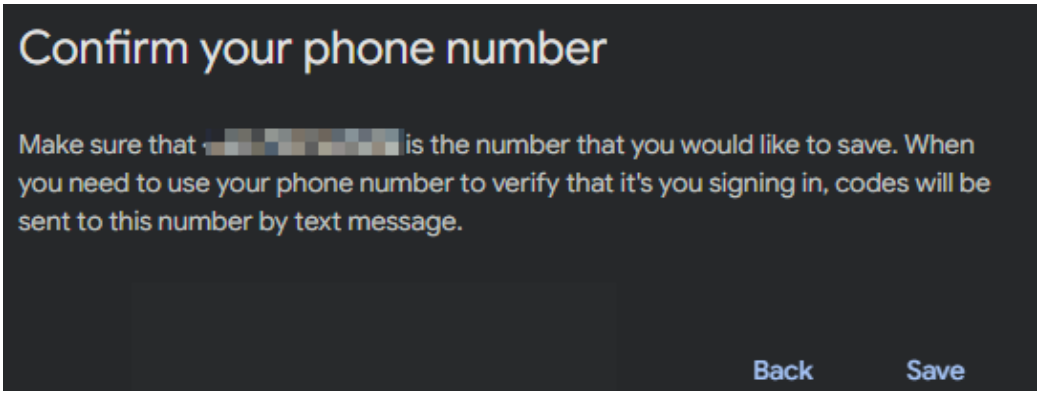
2. Click “Enrol”, then click “Turn on 2-Step Verification” You will be asked to input your mobile phone number, and select whether you’d rather receive a text or a phone call with a confirmation code. It is recommended that you select a text message.



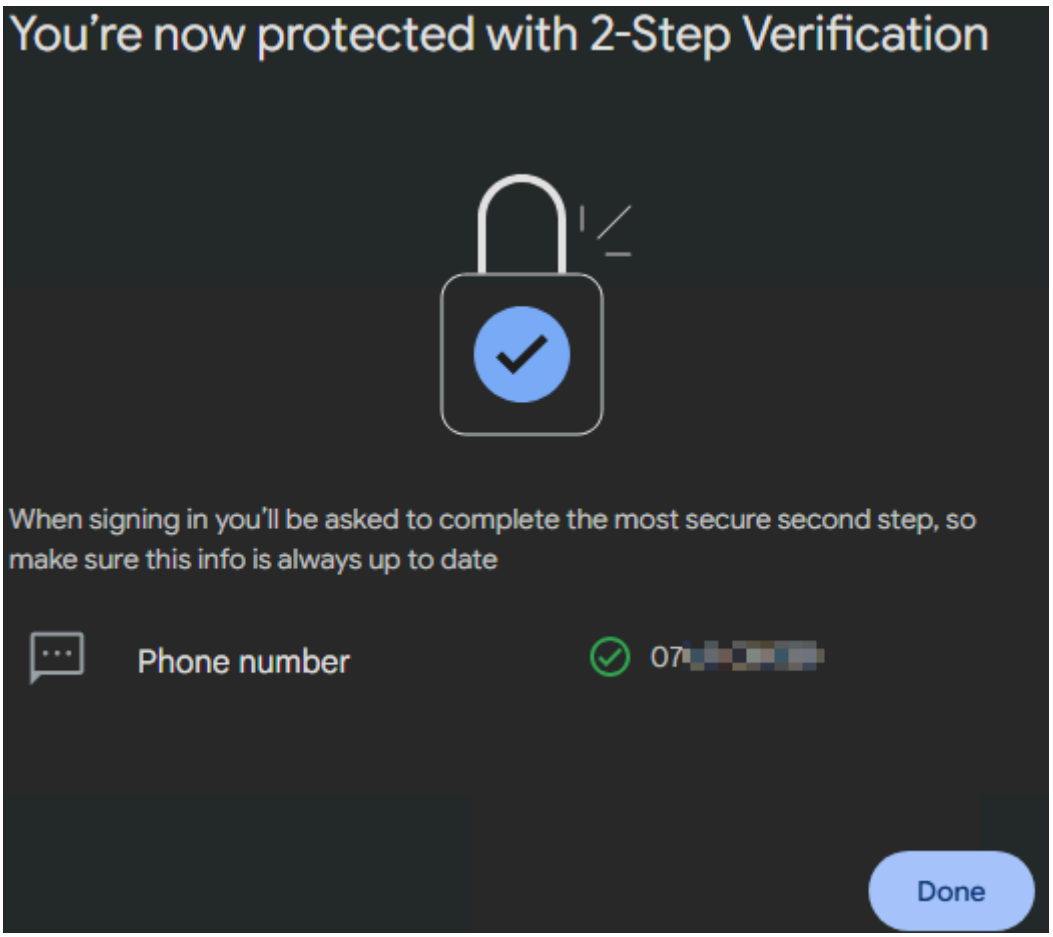
3. Then click “Next”



4. Followed by Save



5. You should now see the following message please click “Done”



From now on, you’ll receive a text message whenever you try to sign in with a 6-digit code. You’ll need to enter this in order to log in.

If you ever lose your phone or are unable to log in, please contact the IT Team as we can provide a single-use code to log in. It is also important to be vigilant for incoming codes when you haven’t requested one. If this happens to you, your password may be compromised. Please let the IT Team know immediately if you suspect such activity.

As this method can be cumbersome or require a phone signal, we **highly** recommend setting up one or more of the other methods **in addition** to this, these are detailed on the next pages.

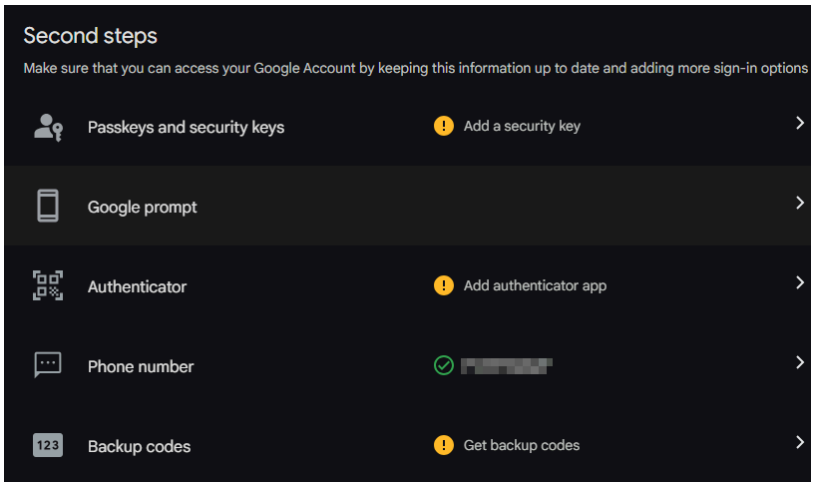
Additional 2-FA Methods

We recommend you set the Authenticator App up

Authenticator App

Each time you sign in, you'll be asked for a randomly generated code within an app, which changes every 30 seconds. There are multiple apps available but this guide will use Google's Authenticator App. It doesn't rely on any connection at all once set up. This app can also be used for 2-Factor Authentication for many other services.

1. Click on the "Authenticator" "Set Up" option, then select which model of phone you have and press "Next".



2. You will be shown a QR Code. Keep this on your screen, and download the Authenticator App to your phone or tablet. Once it has finished, you can set it up. Follow the instructions on your device's screen to scan the barcode and confirm the process has worked.
    a. If you already use authenticator, tap on the plus in the bottom-right corner, then select "Scan barcode". Align the box on your phone with the displayed QR code on your desktop pc's screen. This should automatically add the account to your app.

    b. If you encounter issues with scanning a barcode, click "can't scan it" on your pc to get a code and select "Manual entry" on the device. Follow the on-screen prompts on both devices.
3. Press "Next" on your desktop pc, then enter the code displayed on your phone. If the text is red it indicates your code is about to expire, so it's best to wait a moment for a new one.

If you have any issues or questions please speak with the IT Support team who will be more than happy to help and advise.

The Google Authenticator app can be downloaded here for IOS and here for Android/Google Play