

OCA Email Account

How do I enable 2-Step Verification (2FA)?

What is 2-Step Verification and why do I need to enable it?

2-Step Verification, or '2FA', adds an additional layer of security to your account to ensure that your personal information remains private and safe. Its use aims to prevent any unauthorised access to your account. Should you find it helpful, the following [Google Support Page](#) provides more information on the benefits of 2FA. As of February 29th 2024, 2FA was enforced for all OCA students.

How long will I have to enable 2-Step Verification?

If you are a new student enrolling from March 5th 2024, you will have thirty days from the first time you sign into your OCA Email Account to enable a **minimum of two authentication methods**. If you don't successfully enable a minimum of two authentication methods, you will be locked out of your account and will need to contact the IT Team (ithelpdesk@oca.ac.uk) to regain access.

Please note that if mitigating circumstances apply, you may opt out of enabling 2FA and will need to contact the IT Team (ithelpdesk@oca.ac.uk) to discuss your options further. Opting out will result in several restrictions being applied to your OCA Email Account; please refer to the What if I opt not to enable 2FA? section below for further details.

How do I enable 2FA and what are the authentication methods available?

Follow the steps below to enable 2FA on your OCA Email Account (you must be signed in via the Google homepage first – google.com – consult the [How do I sign into my OCA Email Account?](#) article for further guidance if required):

1. Navigate to the Google homepage – google.com.
2. Select the Google Account Profile Icon in the upper-right corner, followed by 'Manage your Google Account', or access the myaccount.google.com directly.
3. Select 'Security & sign-in' from the left-hand menu, and scroll down to select '2-Step Verification'. You will be prompted to enter your password to continue.
4. You must now enable a **minimum of two authentication methods** to ensure your account meets essential security requirements. See the information below on each authentication option.

Authentication Methods

- **Authenticator Application** – The Authenticator Application option will not be available the first time you set up 2FA. Instead, you will first need to select 2 of the other options below. See the [How do I set up an Authenticator Application as a 2FA method?](#) article for more information.
- **Google Prompt** – The Google Prompt option allows users to receive a notification to a Mobile or Tablet that will prompt you to accept or deny the sign in request using your preferred device(s). See the [How do I set up Google Prompt as a 2FA method?](#) article for more information.
- **SMS or Voice Verification Codes** – Setting up the SMS or Voice Verification Codes option will enable you to receive a verification code to your device via a text message or phone call. To set up this option, select 'Phone number' and follow the prompts on-screen.
- **Backup Codes** – Backup Codes are intended to act as an emergency authentication method and aren't recommended to be used as one of your two preferred methods where possible. To set up this option, select 'Backup codes' followed by 'Get backup codes'. You will then be issued with a series of 10, 8-digit codes. You must make a note of your codes; the option to print and

download is available, but you may wish to write them down or store them on another device, remembering to ensure that they are stored safely.

Backup codes can be refreshed at any time should you use all of your available codes, or your existing codes are no longer secure, by accessing the '2-Step Verification' page, selecting 'Backup codes', followed by the 'Refresh' icon to generate a series of new codes. You can also use the 'Delete' option to remove your codes and disable backup codes if desired.

What if I don't have a smartphone / want to provide my telephone number / can't install an Authenticator Application?

- If you don't have access to a smartphone, you may instead use SMS or Voice Verification Codes alongside Backup Codes as the second 2FA method.
- If you don't wish to provide your phone number, you should consider the use of the Authenticator Application alongside Backup Codes as the second 2FA method.
- Should mitigating circumstances apply, such as, but not limited to, not having access to a Mobile, you will need to contact the IT Team (ithelpdesk@oca.ac.uk) to discuss the option of alternatives and / or opting out of 2FA. Please note that restrictions will apply if opting out of 2FA; refer to the What if I opt not to enable 2FA? section below for further details.

What if I opt not to enable 2FA?

If you would prefer not to enable 2FA, your OCA Email Account will have restricted access to the OCA Directory which will revoke access to utilities such as the recipient auto-fill and suggestions feature available within Gmail. Access to Google Contacts is also restricted, so you will need to manually enter an intended recipient's known email address.