

Bring Your Own Device **Policy**

Roselyn House School

2026 – 2027



Approved by:	Rachel Smith	Date: 01/09/2026
Last reviewed on:	September 2026	
Next review due by:	September 2027	

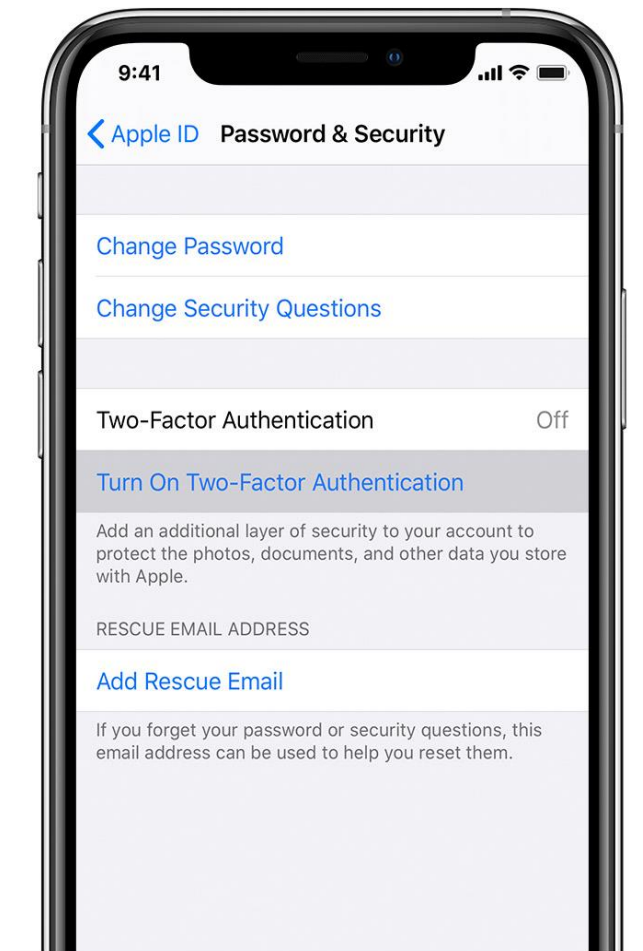
BRING YOUR OWN DEVICE POLICY ANNEX 1

Set up two-factor authentication for your Apple ID

You can follow these steps to turn on two-factor authentication on your device. [Find out more about the availability of two-factor authentication.](#)

Turn on two-factor authentication on your iPhone, iPad or iPod touch

1. Go to Settings > [your name] > Password & Security.
2. Tap Turn On Two-Factor Authentication.

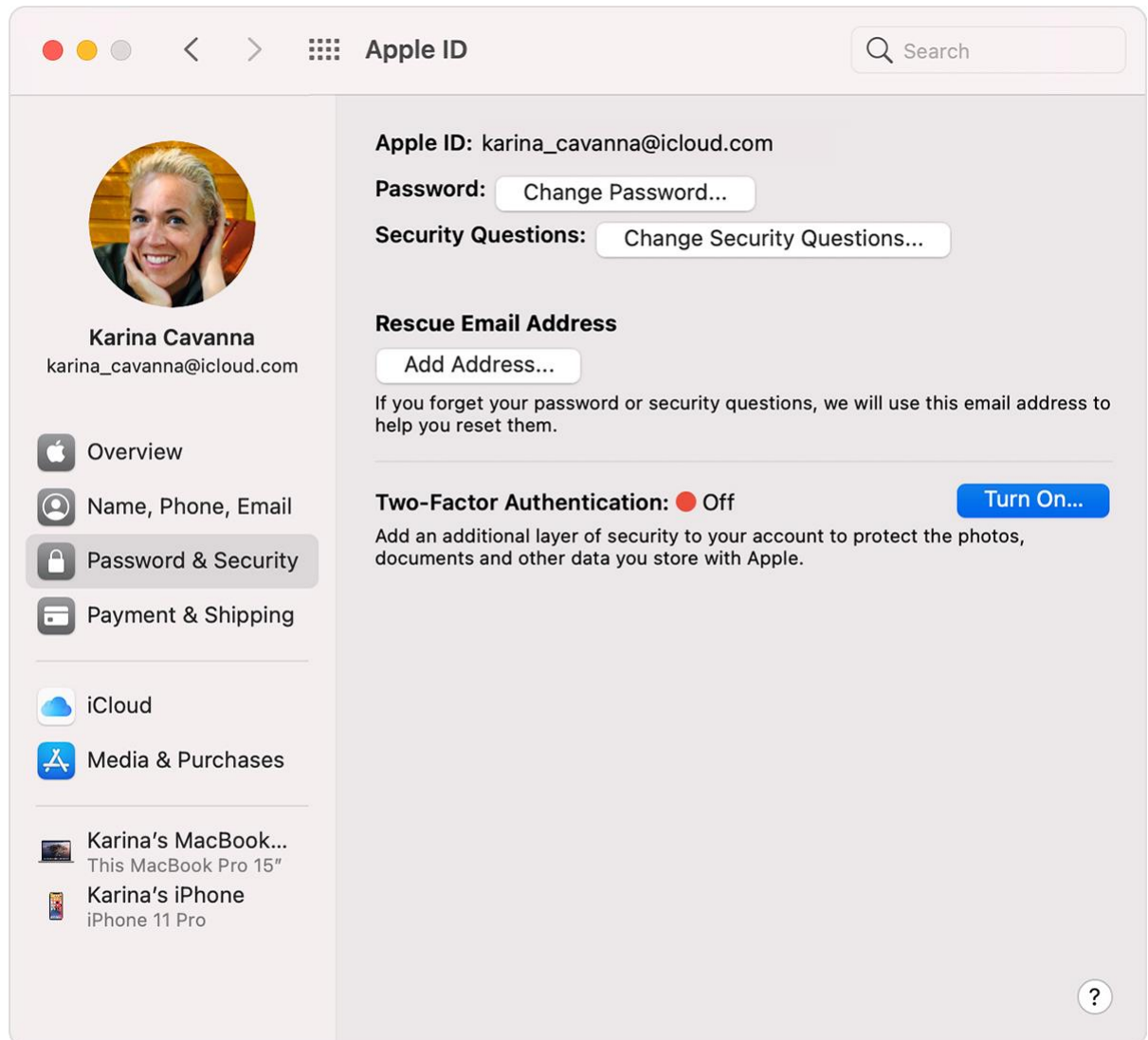


3. Tap Continue.
4. Enter the phone number you want to receive verification codes on when you sign in. You can choose to receive the codes by text message or via an automated phone call.
5. Tap Next.
6. Enter the verification code to verify your phone number and turn on two-factor authentication.

You may be asked to answer your Apple ID security questions.

Turn on two-factor authentication on your Mac

1. Choose Apple menu  > System Preferences, then click Apple ID.
2. Click Password & Security under your name.
3. Next to Two-Factor Authentication, click Turn On.



If you're using macOS Mojave or earlier:

1. Choose Apple menu  > System Preferences, then click iCloud and select Account Details.
2. Click Security.
3. Click Turn On Two-Factor Authentication.

Some Apple IDs created in iOS 10.3 or macOS 10.12.4 and later are protected with two-factor authentication by default. In this case, you will see that two-factor authentication has already been turned on.

Upgrade to two-factor authentication on the web

1. Go to appleid.apple.com/uk, then sign in with your Apple ID.
2. Answer your security questions, then tap Continue.
3. You'll see a prompt to upgrade your account security. Tap Continue.
4. Click Upgrade Account Security.
5. Enter the phone number you want to receive verification codes on when you sign in. You can choose to receive the codes by text message or via an automated phone call.
6. Click Continue.
7. Enter the verification code to verify your phone number and turn on two-factor authentication.

If you have an Apple ID that's not protected by two-factor authentication, some Apple websites may ask you to update your account.

What to remember when you're using two-factor authentication

Two-factor authentication significantly improves the security of your Apple ID. After you have turned it on, signing in to your account will require both your password and access to your trusted devices or trusted phone number. To keep your account as secure as possible and help ensure you never lose access, there are a few simple guidelines you should follow:

- Remember your Apple ID password.
- Use a device passcode on all your devices.
- Keep your trusted phone number(s) up to date.
- Keep your trusted devices physically secure.

Manage your account

You can manage your trusted phone numbers, trusted devices and other account information from your [Apple ID account page](#).

Manage your trusted phone numbers

To use two-factor authentication, you need to provide at least one trusted phone number that you can receive verification codes on. Consider verifying an additional trusted phone number other than your own phone number. If your iPhone is your only trusted device and it is missing or damaged, you will be unable to receive the necessary verification code to access your account.

Update your trusted phone number on your Apple ID account page

1. Go to appleid.apple.com/uk.
2. Sign in with your Apple ID.
3. Go to the Security section and click Edit.

If you want to add a phone number, click Add a Trusted Phone Number and enter the phone number. Choose to verify the number with a text message or an automated phone call, and click Continue. To remove a trusted phone number, click ✕ next to the phone number you want to remove.

Update your trusted phone number by using account recovery

1. Go to appleid.apple.com/uk.
2. Sign in with your Apple ID.
3. Select “Didn’t get a verification code?”, then select More Options.
4. You’ll be redirected to iforgot.apple.com/uk.
5. Complete your account recovery request. [Find out more about account recovery](#).

View and manage your trusted devices

You can view and manage a list of your trusted devices on iOS, macOS and in the Devices section of your [Apple ID account page](#).

On iOS:

1. Go to Settings > [your name].
2. Select a device from the list.

On macOS Catalina or later:

1. Choose Apple menu  > System Preferences.
2. Select Apple ID.
3. Select a device from the sidebar.

On macOS Mojave or earlier:

1. Choose Apple menu  > System Preferences.
2. Select iCloud, then click Account Details.
3. Click the Devices tab.
4. Select a device from the list.

On the web:

1. Go to your [Apple ID account page](#).
2. Sign in with your Apple ID.
3. Go to the Devices section.

[The device list shows the devices that you're currently signed in to with your Apple ID.](#)

Select a device to view device info, such as the model and serial number. Below that, you can see other useful information, including whether or not the device is trusted and can be used to receive Apple ID verification codes.

You can also remove a trusted device by selecting Remove from Account from the device list. Removing a trusted device will ensure it can no longer display verification codes and that access to iCloud, and other Apple services on the device, will be blocked until you sign in again with two-factor authentication. If you need to find or erase your device before you've removed it from your trusted device list, you can [use Find My iPhone](#).

Generate app-specific passwords

With two-factor authentication, you need an [app-specific password](#) to sign in to your account using third-party apps or services, such as email, contacts or calendar apps not provided by Apple. Follow these steps to generate an app-specific password:

1. Sign in to your [Apple ID account page](#).
2. Click Generate Password, below App-Specific Passwords.
3. Follow the steps on your screen.

After you have generated your app-specific password, enter or paste it into the password field of the app as you normally would.

Frequently asked questions

Need help? You may find the answer to your question below.

What if I've forgotten my password?

You can reset or change your password from your trusted device or browser by following these steps.

On your iPhone, iPad or iPod touch

1. Go to Settings > [your name].
2. Tap Password & Security > Change Password.
3. Enter a new password.

On your Mac

1. Choose Apple menu  > System Preferences, then click Apple ID.
2. Click Password & Security, then click Change Password.

If you're using macOS Mojave or earlier:

1. Choose Apple menu  > System Preferences, then click iCloud.
2. Choose Account Details. If you're asked to enter your Apple ID password, click Forgotten Apple ID or password and follow the on-screen instructions. You can skip the steps below.
3. Click Security > Reset Password. Before you can reset your Apple ID password, enter the password used to unlock your Mac.

On the web

If you don't have access to an iPhone, iPad, iPod touch or Mac, you can reset or change your password from iforgot.apple.com/uk.

What if I can't access a trusted device or haven't received a verification code?

If you're signing in and don't have a trusted device to hand that can display verification codes, you can get a code sent to your trusted phone number via text message or an automated phone call instead. Click Didn't Get a Code on the sign-in screen and choose to send a code to your trusted phone number. You can also get a code directly from Settings on a trusted device. [Find out how to get a verification code](#).

If you're using iOS 11.3 or later on your iPhone, you may not need to enter a verification code. In some cases, your trusted phone number can be verified automatically in the background on your iPhone. It's one less thing to do, and your account will still be protected with two-factor authentication.

If I can't sign in, how do I regain access to my account?

If you can't sign in, access a trusted device, reset your password or receive verification codes, you can [request an account recovery to regain access to your account](#). Account recovery is an automatic process designed to get you back in to your account as quickly as possible, while also denying access to anyone who may be pretending to be you. It may take a few days – or longer – depending on what specific account information you can provide to verify your identity.

If you've generated a recovery key, you can use your recovery key to regain access to your account instead. [Find out more about using a recovery key](#).

Do I still need to remember any security questions?

No. With two-factor authentication, you don't need to remember any security questions. We verify your identity using your password and verification codes sent to your trusted devices and phone numbers. When you enrol in two-factor authentication, we keep your old security questions on file for two weeks in case you need to return your account to its previous security settings. After that, they're deleted.

Can Apple Support help me regain access to my account?

Apple Support can answer your questions about the account recovery process, but can't verify your identity or expedite the process in any way.

What are the system requirements for two-factor authentication?

For the best experience, make sure you meet these system requirements on all of the devices you use with your Apple ID:

- iPhone, iPad or iPod touch with iOS 9 and later
- Mac with OS X El Capitan and iTunes 12.3 and later

- Apple Watch with watchOS 2 and later
- Apple TV HD with tvOS
- Windows PC with iCloud for Windows 5 and iTunes 12.3.3 and later

Can Apple IDs created for children use two-factor authentication?

Yes. Any Apple ID that meets the basic system requirements can enrol in two-factor authentication. Find out more about [who can use two-factor authentication](#).

What if I don't recognise the location shown in my sign-in notification?

When you sign in on a new device, you'll get a notification on your other trusted devices that includes a map showing the approximate location of the new device. This is an approximate location based on the IP address the device is currently using, rather than the exact location of the device. The location shown may reflect the network you're connected to, and not your physical location.

If you know you're the person trying to sign in but don't recognise the location shown, you can still tap Allow and continue signing in. However, if you ever see a notification that your Apple ID is being used to sign in on a new device and you're not the one signing in, tap Don't Allow to block the sign-in attempt.

What if I use two-factor authentication on a device running older software?

If you use two-factor authentication with devices running older OS versions – [such as an Apple TV \(2nd or 3rd generation\)](#) – you may be asked to add your six-digit verification code to the end of your password when signing in. [Get your verification code](#) from a trusted device running iOS 9 and later or OS X El Capitan and later, or have it sent to your trusted phone number. Then type your password followed by the six-digit verification code directly into the password field.

Can I turn off two-factor authentication after I've turned it on?

If you are already using two-factor authentication, you can no longer turn it off. Certain features in the latest versions of iOS and macOS require this extra level of security, which is designed to protect your information. If you have recently updated your account, you can unenrol within two weeks of enrolment. Just open your enrolment confirmation email and click the link to return to your previous security settings. Bear in mind that this makes your account less secure and means you can't use features that require higher security.

Is this different from Apple's older two-step verification feature?

Yes. Two-factor authentication is built directly into iOS, macOS, tvOS, watchOS and Apple's websites. It uses different methods to trust devices and deliver verification codes, and offers a more streamlined user experience. You need two-factor authentication to use certain features that require improved security.

If you're already using two-step verification and want to update to two-factor authentication, [find out how to switch to two-factor authentication](#). If your account isn't

eligible for two-factor authentication, you can still use [two-step verification](#) to protect your information.

Information about products not manufactured by Apple, or independent websites not controlled or tested by Apple, is provided without recommendation or endorsement. Apple assumes no responsibility with regard to the selection, performance or use of third-party websites or products. Apple makes no representations regarding third-party website accuracy or reliability. [Contact the vendor](#) for additional information.

Android Phone/Tablet Two Factor Authentication

Turn on 2-Step Verification

With 2-Step Verification (also known as two-factor authentication), you add an extra layer of security to your account in case your password is stolen. After you set up 2-Step Verification, you'll sign into your account in two steps using:

- Something you know, like your password
- Something you have, like your phone

Turn on 2-Step Verification

1. Open your [Google Account](#). (Or Samsung Account if you use their own authentication service)
2. In the navigation panel, select **Security**.
3. Under "Signing into Google," select **2-Step Verification** > **Get started**.
4. Follow the on-screen steps.
5. **Verify it's you with a second step**
6. After you turn on 2-Step Verification, you'll need to complete a second step to verify it's you when you sign in. To help protect your account, Google/Samsung will request that you complete a specific second step.