Password Reset

This guide relates to personal IT accounts, not secondary accounts such as guest, external, project, or resource. To change the password on a secondary IT account, use the password change utility. If you have forgotten the password for a secondary account, and need to reset it, please contact servicedesk@abdn.ac.uk.

Password Reset is a feature of Microsoft Authentication. It allows you to reset or change your personal University IT account password yourself – for example if you forget it, or if you think your IT account has been compromised. You can do so at any time and from anywhere. All you need is an internet connection.

In order to use the service, you will first need to complete a simple registration process.

Note: If you have already registered for Multi-factor Authentication (MFA) you do not need to register again and can skip to the section Reset your Password, below.

Registration

You will need to know your existing password in order to access the registration page. If you have forgotten your password, please contact the IT Service Desk.

Until you complete registration, you will be prompted to do so each time you sign into an Office 365 application, e.g. Outlook on the Web (OWA), OneDrive for Business, etc.

When you click Next you will be asked to set up a method of proving who you are. To go ahead with registration at this point follow guidance from step 3 below.

If it is not convenient for you to register you can click Skip setup at that point to bypass registration but note that you will be prompted to register each time you sign into an Office 365 application until you complete registration.

To register

1. On a laptop or desktop computer, go to https://aka.ms/setupsecurityinfo
2. Sign in using your username@abdn.ac.uk and password.
3. You will be asked to set up a method of proving who you are.
   The default method suggested is the Microsoft Authenticator app which you install on your smartphone. We recommend you use this method.
   If you prefer, you can select I want to set up a different method, and then choose phone as your method of proving who you are.
4. We recommend that you **set up two** authentication methods – however:

   ![Warning Icon]
   You should not choose Email as one of your methods as this is not a strong method of authentication and cannot be used when your account is enabled for MFA.

   Once you have successfully set up one method of authentication, you can go back to [https://aka.ms/setupsecurityinfo](https://aka.ms/setupsecurityinfo) and set up an alternative.

**To set up the Microsoft Authenticator app:**

- Download the [Microsoft Authenticator app](https://aka.ms/setupsecurityinfo) to your smartphone, from your App store. If prompted allow access to your camera.
- On your laptop or desktop computer, in the Microsoft Authenticator window, click **Next**.
- Follow the on-screen instructions to **add your University Office 365 account** to the Microsoft Authenticator app on your smartphone.
  - This involves scanning a QR code. If that is not possible, click **Can’t scan image?** and follow the instructions.
- The Microsoft Authenticator app will then generate **6-digit codes** as it finalises the set up.
- On your laptop or desktop computer, you will be prompted either to enter one of the 6-digit codes from the app, or to click **Approve** on your smartphone.
- You will see confirmation when you have successfully set up this method of authentication.

**To set up a phone:**

- You’ll be prompted to select your country or region from a drop-down menu, and to enter your mobile phone number in the box provided
- You can then opt to receive your verification code number by text (click **Text me a code**) or by phone call (click **Call me**)
- Click **Next**
- Once you receive the verification code, type it into the text box provided and click **Next**
  
  **Note:** If you chose **Call me**, you will receive a phone message asking you to press the # key instead.
- You will see confirmation when you have successfully set up this method of authentication.
Sign-in methods:

Note whichever method you set up first will become your default sign-in method.

- To add an alternative method of authentication, or to change any details, go to setup Security Info
- Sign in using your username@abdn.ac.uk and password
- You will be asked to verify your account using the default method you set up, e.g. by entering a code from the Microsoft Authenticator app.
- The method(s) you have already set up are listed

- To add another method of authentication, click on + Add Method and follow the on-screen instructions. Options you can use are: Authenticator app, Phone, and Alternate phone.
  
  Note: You can only receive calls to an Alternate phone

- To change a method that is listed, click delete beside it. Then choose + Add Method, as above, to add new details.

- To change the default sign-in method click change and choose your preferred option.

Reset your password

Once you have registered authentication methods, you can reset your password at any time.

1. Go to https://www.abdn.ac.uk/password-reset/

   Alternatively, on Outlook Web App’s Sign in screen:
   - Enter your username@abdn.ac.uk, then Next.
   - At the Enter password dialog, click Forgotten my password

   Or, on a classroom or staff PC, click Reset password on the sign in screen.

2. The Microsoft password reset window opens in your web browser.

   Type your University username@abdn.ac.uk in the User ID text box – this may already be populated – prove you aren’t a robot by entering the validation characters you see, click Next
3. Choose whether you want your verification code to be received in the Microsoft Authenticator app, or by Text, or Call.

4. You’ll find a verification code in your Microsoft Authenticator app (if you set that up), or it will be sent to the mobile phone number that you provided when you registered.

   **Note:** If you selected Call my mobile phone number, you will receive a phone message asking you to press the # key instead of a verification code.

5. Type in the verification code and click Next
6. Type in your new password, then confirm your new password

Get back into your account

* Enter new password:

* Confirm new password:

Finish  Cancel

Make sure your new password conforms to our password rules – see page 6 below.

7. Click Finish.

If your password reset was successful, you will receive an onscreen confirmation and an email notification.

Once you have changed your password, you will need to update wireless and email settings on all your devices (phones, tablets and PCs) with your new password in order to receive email and connect to the University wireless network.

Please allow up to 30 minutes for your password change to synchronise across all the University IT systems.

What happens if my details change after registering?

If you change the phone or phone number that you used when registering, that method of authentication will no longer work.

You must remove it from your list of methods and register your new details. To do this:

1. On a laptop or desktop computer, go to https://aka.ms/setupsecurityinfo
2. Sign in using your username@abdn.ac.uk and password.
3. Follow the onscreen instructions to add a new authentication method or to delete a method that you can no longer use.

Further information and help

If you need help setting up or changing authentication methods please contact the Service Desk.
Password Rules

When trying to set a new password, you might see the message “This password does not meet the length, complexity, age, or history requirements of your corporate password policy.” Or “We’ve seen that password too many times before. Choose something harder to guess.”

To make sure your account stays safe, your password must conform to the following rules:

- Must not be a previously used password
- Must contain at least 8 characters
- Must not contain your IT account username
- Must not contain your first or last name
- Must contain characters from at least three of the following four character classes:
  - Uppercase English characters (e.g. A-Z)
  - Lowercase English characters (e.g. a-z)
  - Numeric characters (e.g. 0-9)
  - Special characters – choose from: ! # $ % & ( ) * + , - . : ; < = > ? @ [ ] ^ _ ` { } | ~

**Note:** The following symbols are not valid: £ \ " '

**Tip!**

Use three or more random words together. By using a mix of upper and lowercase letters and substituting some letters with numbers and special characters, you can make your password even harder to guess.

Password Security

- IT Services will never ask you for your password.
- Never share your password. Keep it secret, keep it safe.

Watch out for phishing emails. For guidance on how to protect yourself from phishing scams see our [Toolkit guide](#).