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.

Before you start

In order to use the service, you will first need to have set up Multi-Factor authentication (MFA). You may have already done this when you accessed your University email for the first time. If you have not, you should set this up now by going to https://aka.ms/setupsecurityinfo. You will need to know your existing password. If you have forgotten your password, please contact the IT Service Desk.

Reset your password

Once you have set up Multi-Factor authentication, 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 – and prove you aren’t a robot by entering the validation characters you see. Then 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 set up Multi-factor authentication.

   **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.

   Make sure your new password conforms to our password rules – see page 4 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 I change my phone, or phone number?

If you change the phone or phone number that you used when setting up Multi-factor authentication, 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 University 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

Find out more about IT Account Security in Toolkit.

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.