*Use this guide to inform your users about the upcoming sign in changes. Edit as necessary to suit your organisation’s processes. Red text highlights particular text you may wish to edit/delete as applicable for your organisation.*

# [System name] sign-in user guidance for email and password sign-in users

When you first sign in there are some initial tasks to get you set up:

1. **Email-based sign-in:** No need to remember a separate username, just use your system email address.
2. **Enhanced security:** You’ll set up Two-Factor Authentication (2FA) for an added layer of protection.
3. **Password reset:** For your first sign-in, you’ll need to reset your password.

## Password reset

A screenshot of a login page

Description automatically generatedFirstly, you’ll receive a welcome email to confirm your account has been activated and prompting you to set your password.

It will confirm the email address you will use as your login ID.

Click **set your password**.

|  |
| --- |
| **Note:** Your activation email is only valid for 24 hours, so if you click the link after this period, you’ll see this message below:    Click **Reset password** and you’ll receive a new email with updated link: |

A screenshot of a login page

Description automatically generatedYou will be directed to the [system name] sign-in page and asked to set a password.

Enter a password which must meet the **minimum** requirements as explained on screen.

Click **Set password.**

A screenshot of a login screen

Description automatically generatedYou’ll then receive a confirmation email to confirm you’ve successfully set your new password.

# Initial Sign-in

A screenshot of a computer

Description automatically generatedOnce you have set your password, go to sign in and you will need to configure your **Two-Factor Authentication (2FA)** settings.

2FA is an extra layer of security used to verify your identity when accessing [system name]. Instead of relying solely on a password, 2FA requires you to provide two different types of verification, making it difficult for unauthorised users to gain access.

Choose your preferred second method of verification (app or email) and follow the set up instructions:

|  |  |
| --- | --- |
| **App** | **Email** |
| A qr code on a screen  Description automatically generated | A screenshot of a form  Description automatically generated |
| Scan the QR code and enter the code generated in your authenticator app  A screenshot of a login box  Description automatically generated | Enter the email address you would like your 2FA code to go to. You will receive an email containing a time sensitive code  A screenshot of a cellphone  Description automatically generated |

Once you have entered your 2FA code you will access [system name].

## Subsequent Sign-in

Once you’ve completed the initial sign in process and set up your 2FA, each time you sign in you’ll see the box below.

A screenshot of a login form

Description automatically generated

If signing in on your own device, be sure to tick the **Remember my email on this device** box to save you typing it in each time.

|  |
| --- |
| **Note: Please don’t tick the box if using a shared device.** |

Click **Next** to continue.

A screenshot of a login page

Description automatically generatedYou’ll be taken to the **Sign in** screen to enter your password.

Click **Log in** then complete the 2FA process you set up initially to access [system name].