NHS
Shared Business Services

ISFE Supplier Drop In Session

J.Murphy 21st October 2025

Shared vision. **Better together**

Introduction

NHS Shared Business Services

- John Murphy , Head of Customer Service Centre (CSC).
  - Responsible for the team of 63 providing the 1st line help desk service from source to settle
  - Capacity has been expanded by 40% to support the supplier on boarding exercise from validation to onboarding
  - The Supplier Portal (SDM) has been live since 2nd October 2025 to enable new suppliers to register to provide service to NHSE
  - Around 2000 suppliers are running through the of which 400+ are now fully registered and using the portal.
  - Over 5000 suppliers have successfully completed the validation process.
  - There will be further waves of suppliers invited once the previous waves have settled.
  - We plan to start to release the registration links via e-mail to the validated administrators on Wednesday, it could take a few days to issue all the invitees.
  - Today's session is to talk through the process so that the onboarding exercise is as smooth as possible
  - Please raise questions in the chat so we can make sure all content is covered during the allocated time.
  - The process can be found on the Supplier section of the corporate website, and a link is provided in your login e-mail

Data Security

NHS
Shared Business Services

- Your data security is at the heart of the new portal, so we have introduced. Multi Factor Authentication (MFA)
- This requires an App to be downloaded and installed on a mobile phone.
- The App is required each time you log in to the portal, so please do not delete the App after initial log in.
- The App itself and MFA process is well established but there are occasional problems which I will cover at the end of the presentation
- Reminder:-

Data Theft/Exfiltration: The attacker could access and download sensitive commercial data from Salesforce for that Supplier, which could include pricing, invoicing and some personal data such as contact details.

Data Tampering/Manipulation: The attacker may be able to maliciously modify or request modification to data relevant to the Supplier, leading to operational disruption or financial damage or lock a legitimate supplier out of their account.

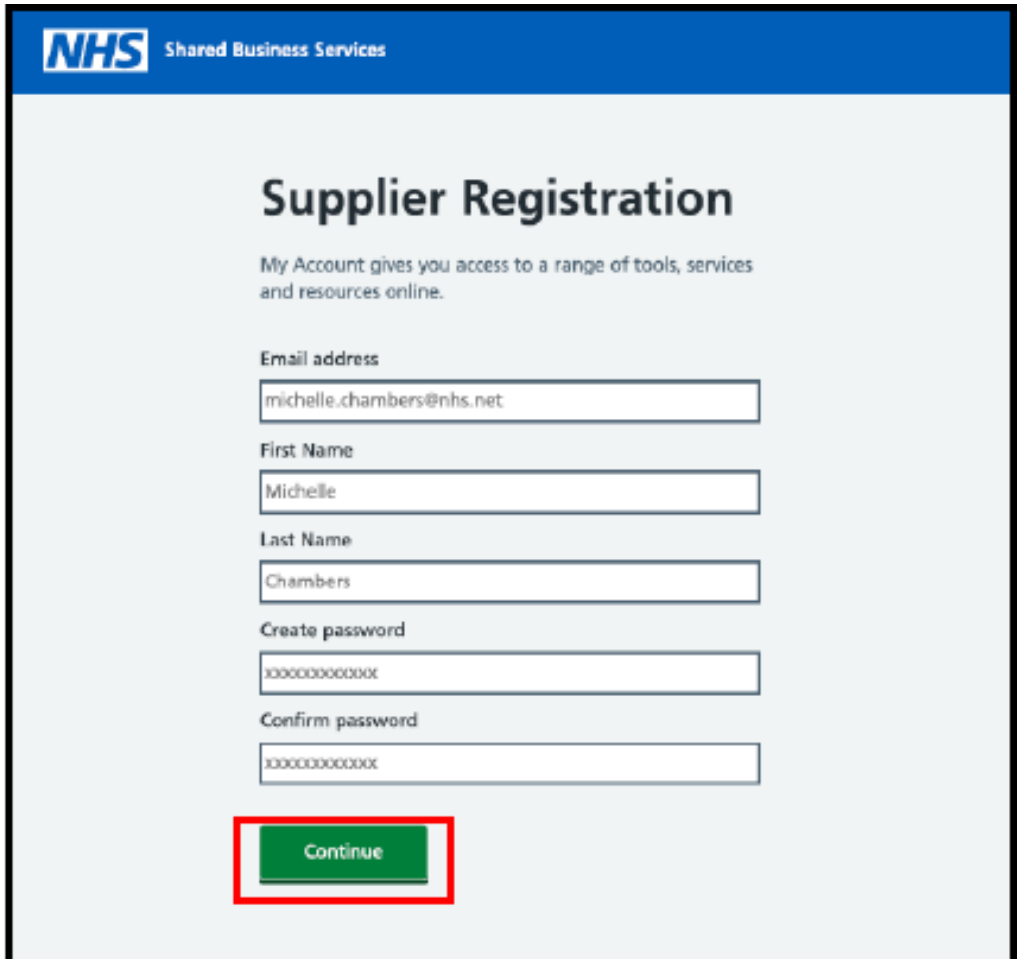
Payment Fraud: The attacker may be able to request a change to banking details (although they are not able to manually change these via the Supplier Portal directly) to divert future payments to an account controlled by the fraudster although there are other measures in place to guard against this activity.

System Compromise & Lateral Movement: The attacker could use the access token and exploit improperly configured permissions to move laterally into other connected systems or gain higher privileges within the Salesforce org. Although independent security penetration testing has been performed on this solution and will be retested at least annually.

Reputation Damage: A data breach involving supplier data, directly resulting from a security control failure (MFA reset fraud), may leads to a significant loss of trust with the supplier community and Clients.
Compliance and Regulatory Fines: A breach can result in non-compliance with regulations like GDPR leading to legal action and financial penalties.

The Process One

NHS
Shared Business Services

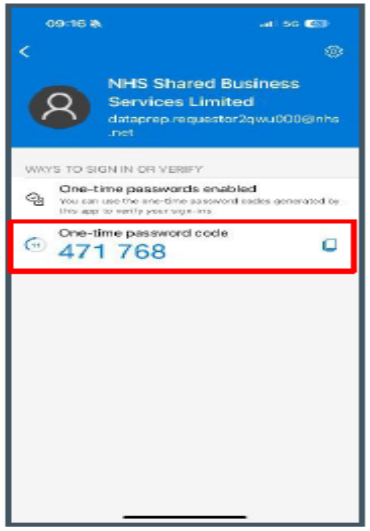


The Process Two

Shared Business Services

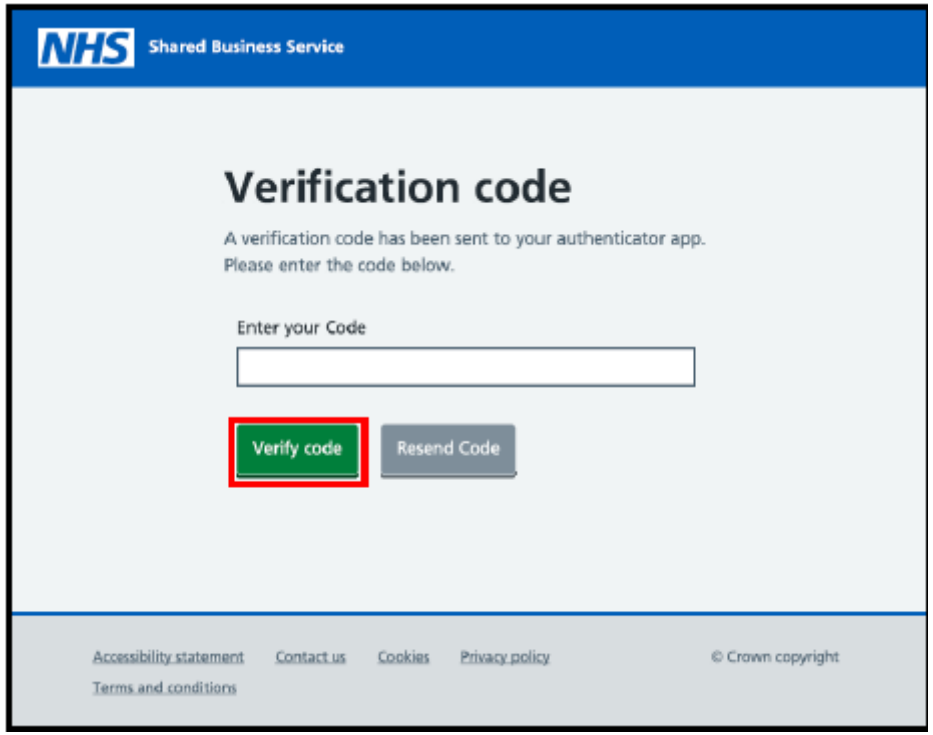
Once you have installed the **Authenticator App** on your smart device, open the app and select the QR code icon to access the QR code scanner, as shown in the screenshots below:

On your smart device, type in your credentials in the **Authenticator App** to generate a **One Time Passcode**, as shown in the screenshot below:



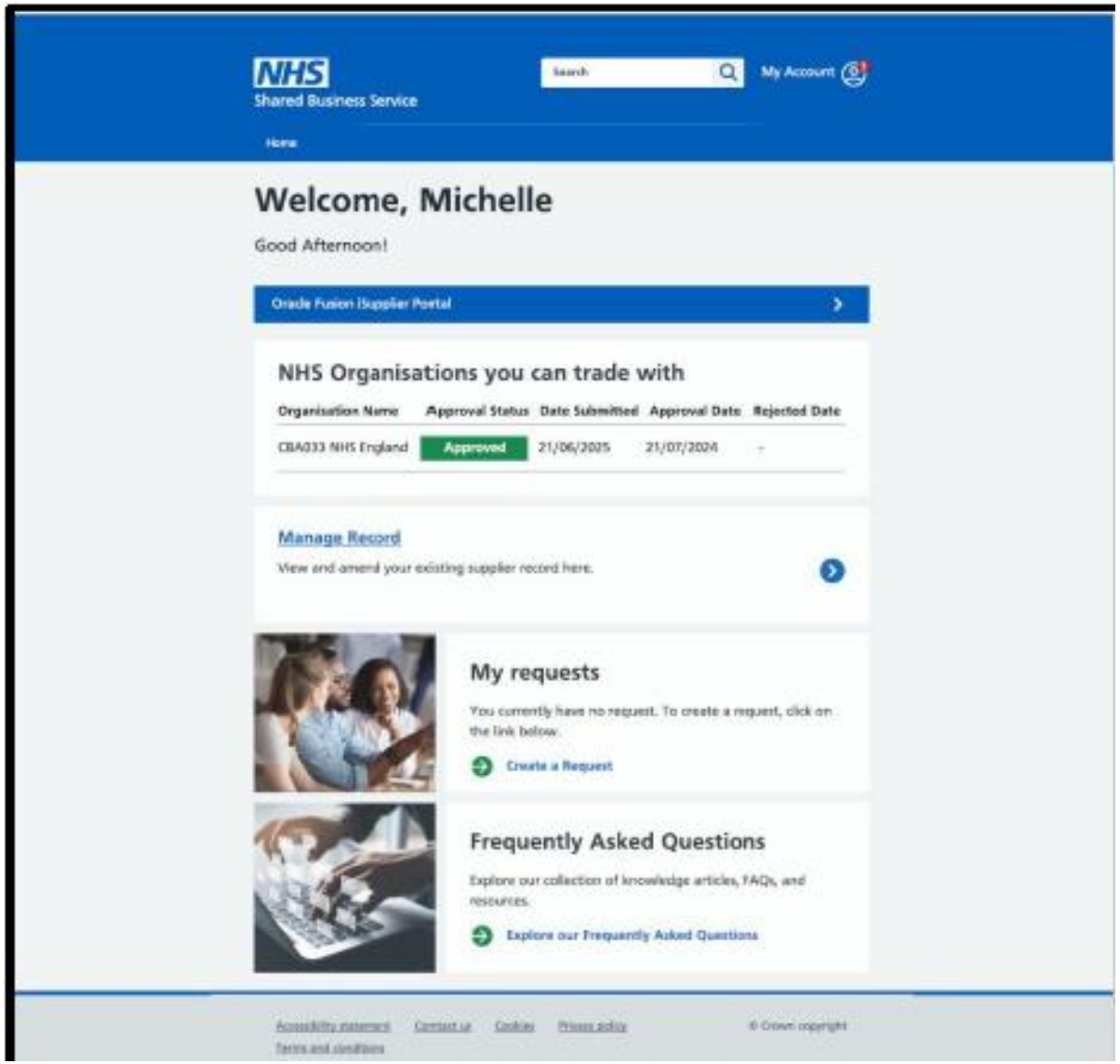
The Process Three

NHS
Shared Business Services



The Process Four

NHS
Shared Business Services



- Note T&C's will pop up the 1st time you log in.
- These will only appear again if they are updated.

Resolving Issues.

NHS
Shared Business Services

- Issues can arise which require the MFA App to be reset.
  - User deletes app after initial log in
  - Potential conflict with CFAP log in if already using MFA
  - Shared e-mail box (How this will work to be explained)
  - Change of e-mail
  - It simply didn't work
  - I already have MFA for another system
- The Help Centre is unable to resolve these issue and will need to triage to a separate team.
- Log in issues must be e-mailed to sbs.suppliers@nhs.net.
- We can not accept via phone or via the current web form.
- The reasons for this are on the next slide.

Issue Resolution.

NHS
Shared Business Services

- To protect your data, we need to verify that an individual requesting an MFA reset is a genuine request.
- Once we have verified the case is passed over to the IT team to reset and send out a new link.
- For more complex cases they may need to contact you for more information. Attaching screen shots can help accelerate the resolution.
- Please note depending on demand this may take up to 10 days.
- As an Administrator, once we receive your e-mail, we will be in touch by making a phone call to you on your registered landline number. You will be asked some validation questions to verify that you are indeed the correct person. We then pass your details as a validate person to the IT team to issue the MFA reset.
- If as Administrator, you have used the option to provide access to others in the organisation and their MFA process has failed, you will need to raise a service request in the portal help centre , naming the individual, their e-mail details and contact number. As you have verified the individual, we will then transfer the case to our IT team to resolve. Your case notes will be update with an incident number for future reference.

Getting the best from Support.

NHS Shared Business Services

- The Portal Introduces a new help centre in addition to data management and invoice status check.
- The new help centre replaces the exiting webform process and gives end to end transparency of where a case is up to and action's we have taken to support resolution.
- Phone calls and e-mails will all be logged on the platform, so the platform becomes your single point of reference for all your cases.
- This will include cases that are logged by the catch and dispatch team when call demand is such that the overflow functionality kick in
- To support the SLA with NHSE to resolve cases with 5 working days we have introduced omni channel workflow which queues inbound cases in the order received and then allocates to the next available agent with the required skill set.
- The summary dashboard on you landing page will provide an instant update of progress with your case.
- Once we have been through the ISFE go –live hyper care period we will be working to bring out case resolution times back down to the levels experienced earlier in 2025.

The End

NHS
Shared Business Services

- Thank You