XOSERVE

<u>**Proposed IAD Password Reset Functionality.**</u>

Security Questions Enabling Password Reset:

When an existing user logs into the IAD application for the first time following implementation of the password reset functionality, the system will directly take them to the 'CREATE PROFILE' screen where the user must set their eight security information answers and reset the password.

Figure 1 – Create profile screen

Once the user has created their profile, the system will display the message informing them to re-login with their new password; on clicking OK the system will redirect them to the login page.
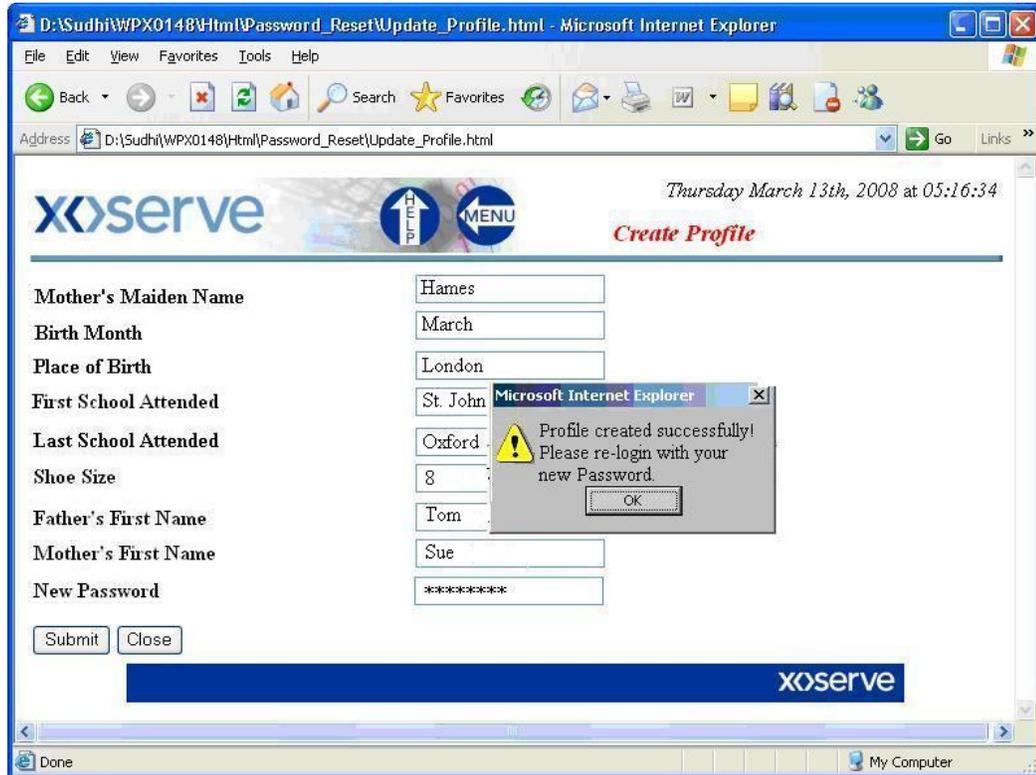
Figure 2 – Profile when created successfully.

The password created by the user will be live for 28 days by default. The expiry date will be reset for the passwords every time the user creates a new password or modifies the existing password. A prompt to change the password is given prior to the 28 day expiry.

At any point that the user wishes to change their password, they can use the MODIFY PASSWORD link in the IAD Main Menu.
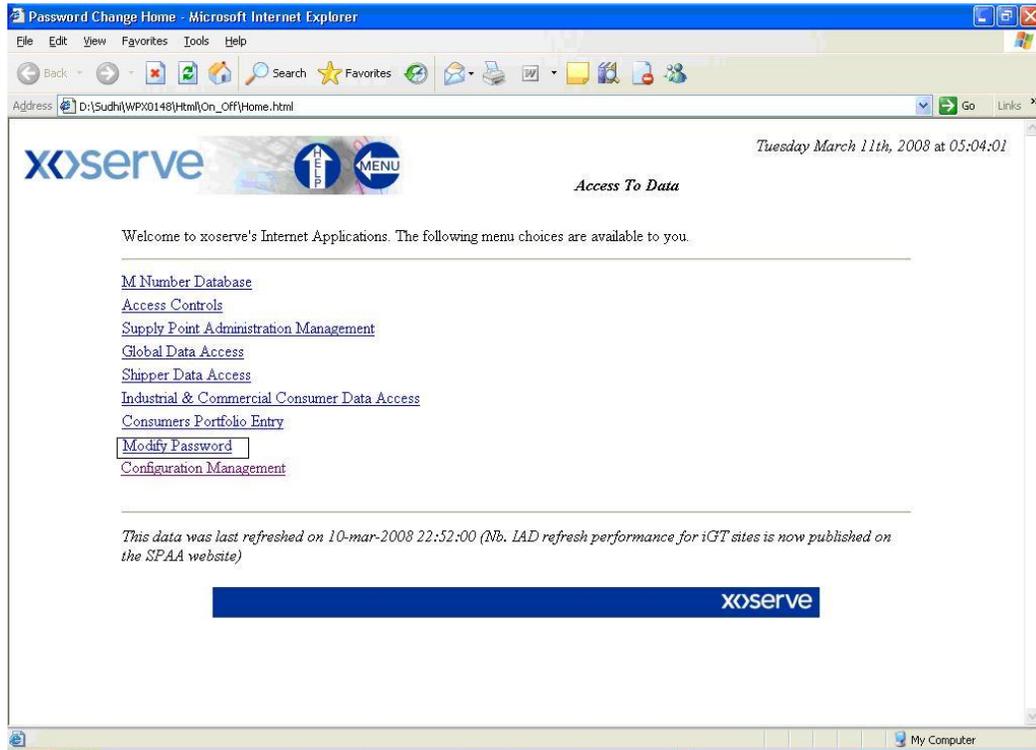
Figure 3 – Modify Link present in IAD Main Menu

When identifying the password, no security questions are asked and it will directly take the user to the 'MODIFY PASSWORD' screen where the user can set their 'New Password'. If the new password and the 'Confirm Password' fields do not match, the message 'New and Confirm Passwords do not match, please retry or type the new password again' is displayed.
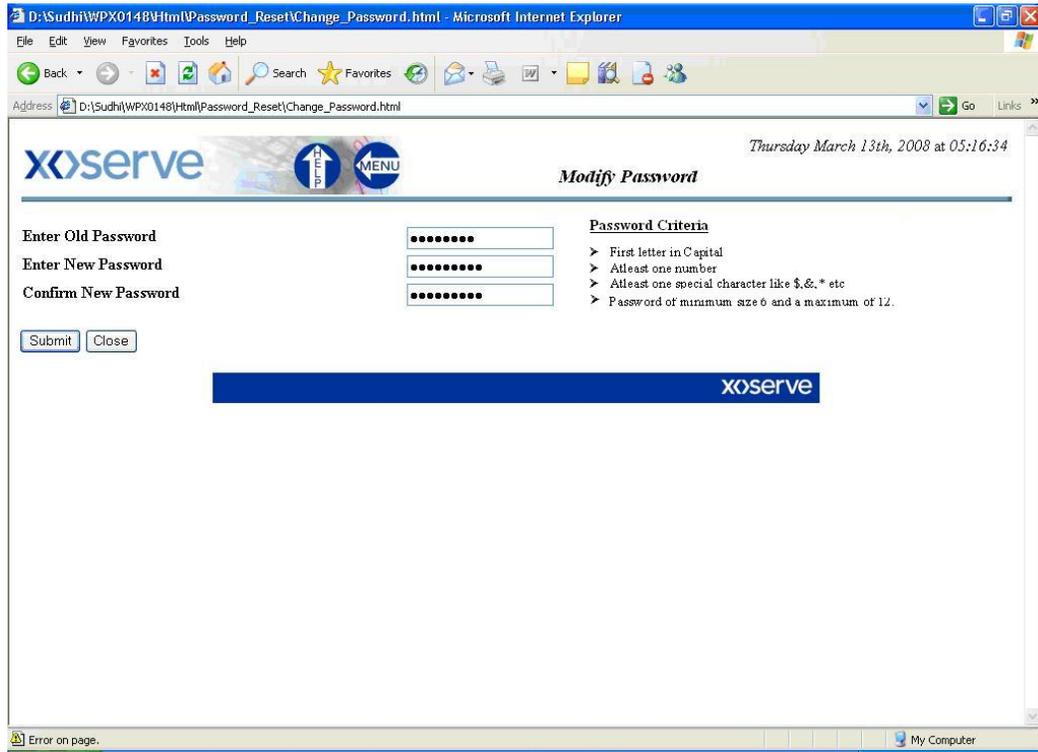
Figure 4 – Modify password screen with Password criteria.

The following sample screens display errors that users may encounter:

Case1: When the password is modified successfully.
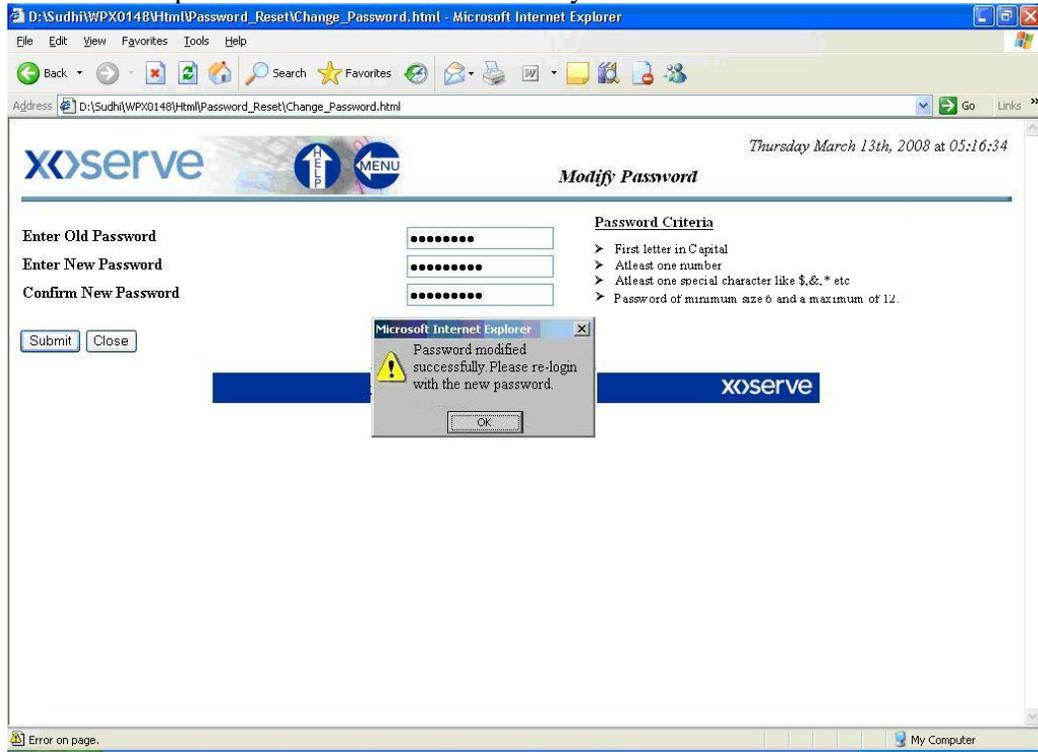
Figure 5 – Password when modified successfully.

Case2: When New Password and Confirm Password do not match.
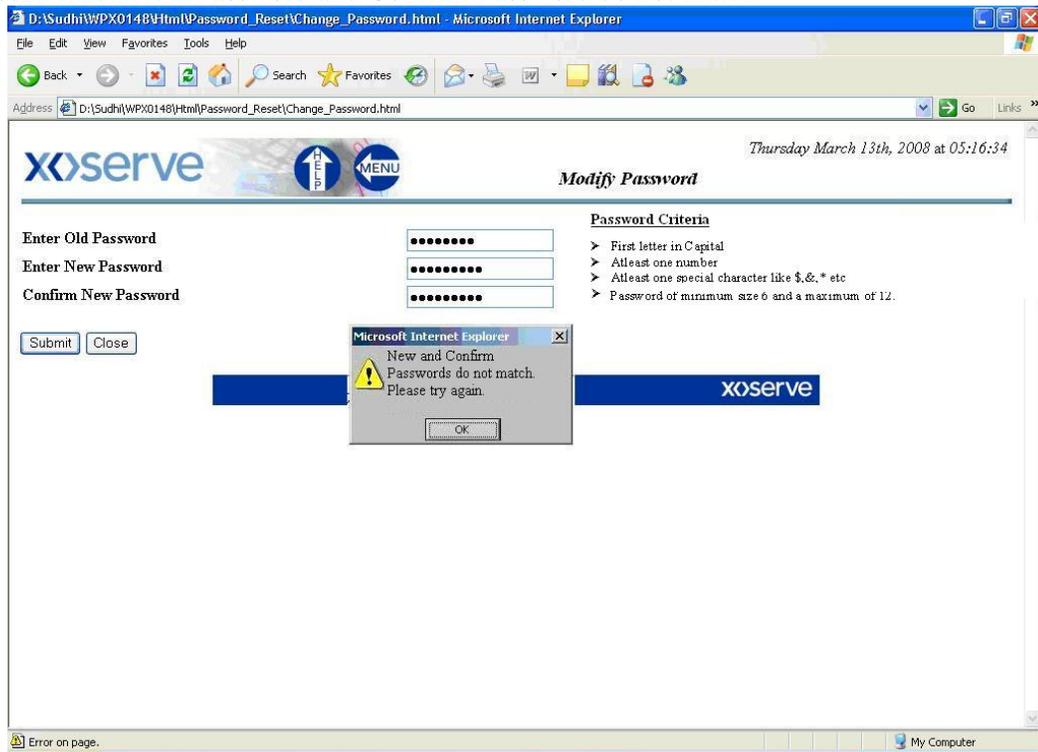
Figure 6 – Mismatch in new and Confirm Password.

Case 3: When the password criteria is not met.
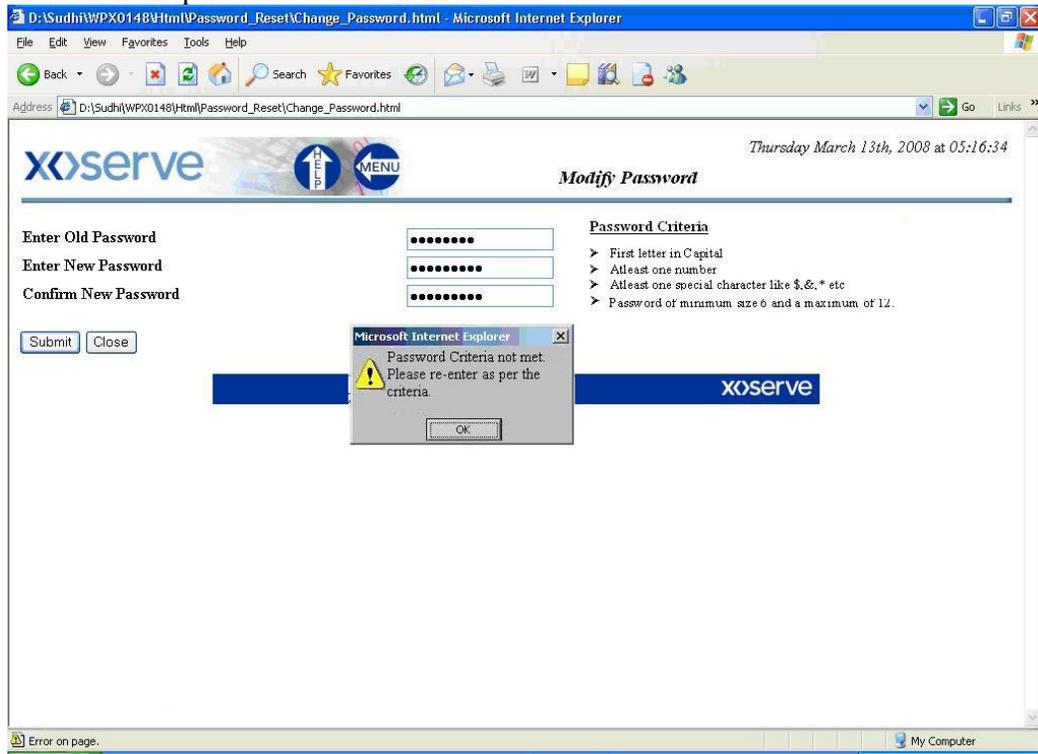
Figure 7 – Retrieve Password Link in the Login Failure screen

User Password Reset Using Security Questions:

If the user inputs the wrong password after three attempts, the system will take the user to the 'LOGIN FAILURE' screen where they can click on the link 'Retrieve Password' which will launch the 'RETRIEVE PASSWORD' screen where they can answer the three randomly selected security questions.
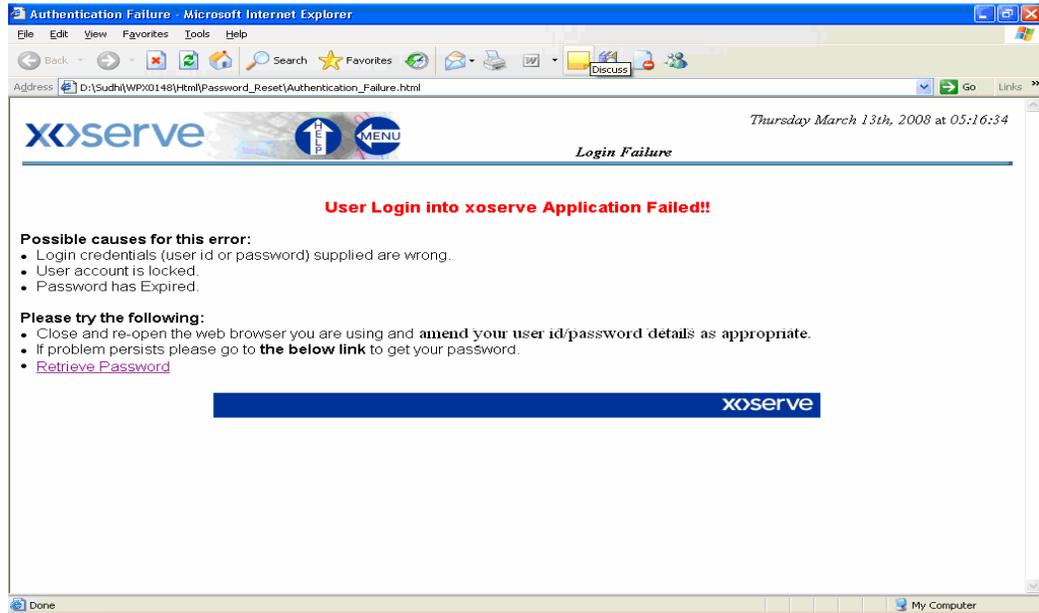
Figure 8 – Login failure screen.
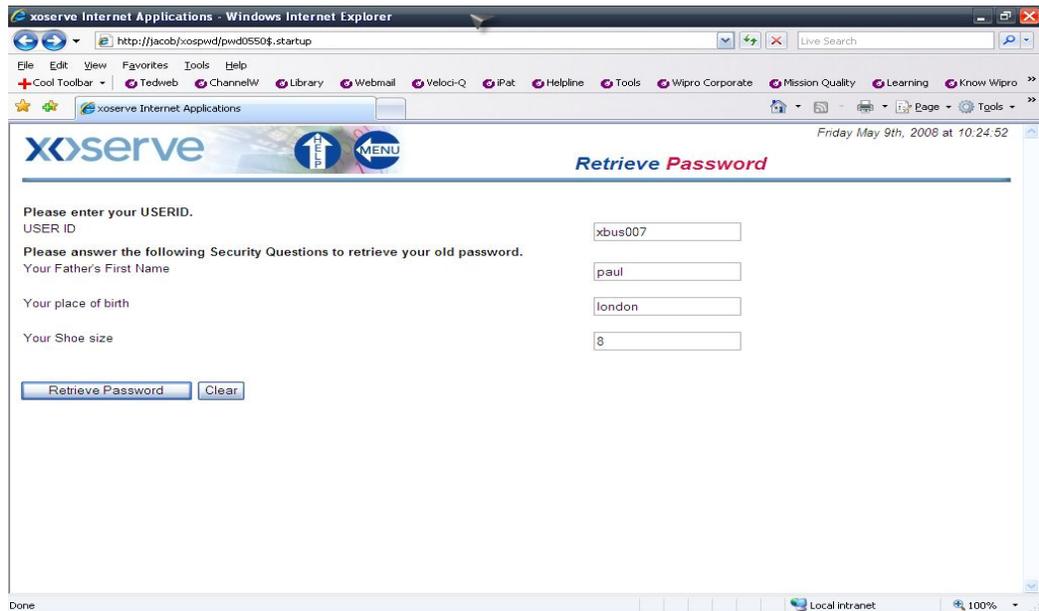
Figure 9 – Retrieve Password Screen.

The security information is then validated by the system and displays the user's password on the screen. The system will then display a message informing the user to re-login with their password and once the user clicks on 'OK' the system will direct the user to the login page.
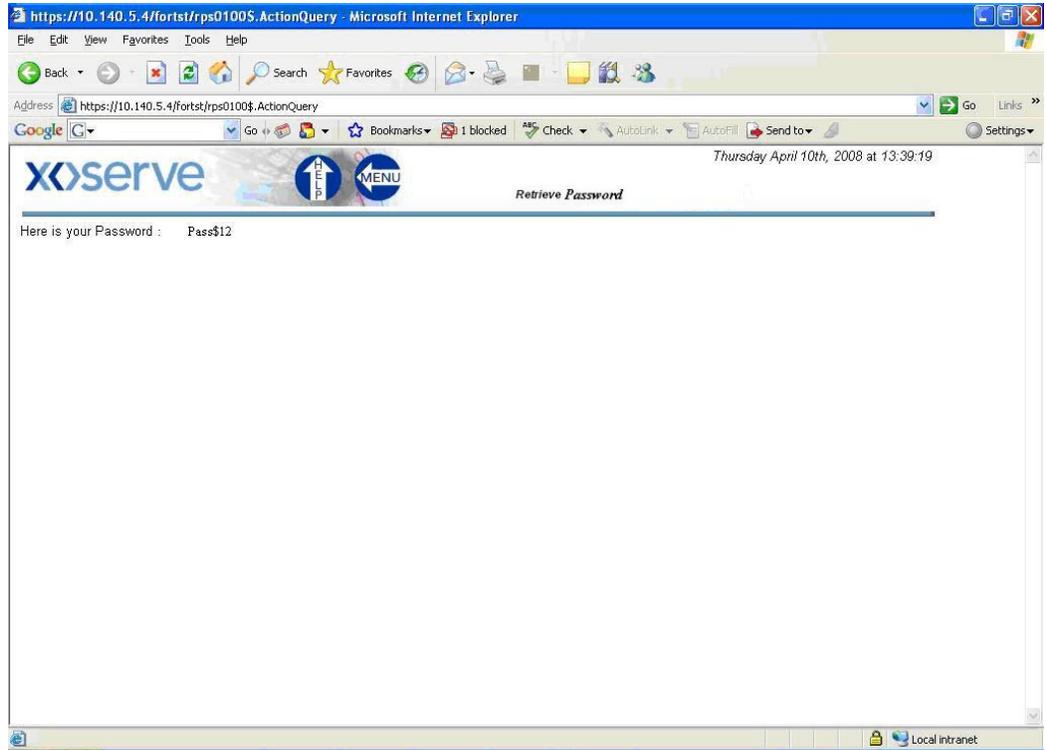
Figure 10 – Password retrieved.

There will be 3 attempts for the user to answer the randomly generated security questions. If the security questions are answered incorrectly after the third attempt the IAD system will display the message "Security credentials provided are incorrect, please contact your LSO to reset your Password". On contacting the LSO, they will then raise a call to the helpdesk to reset the password.
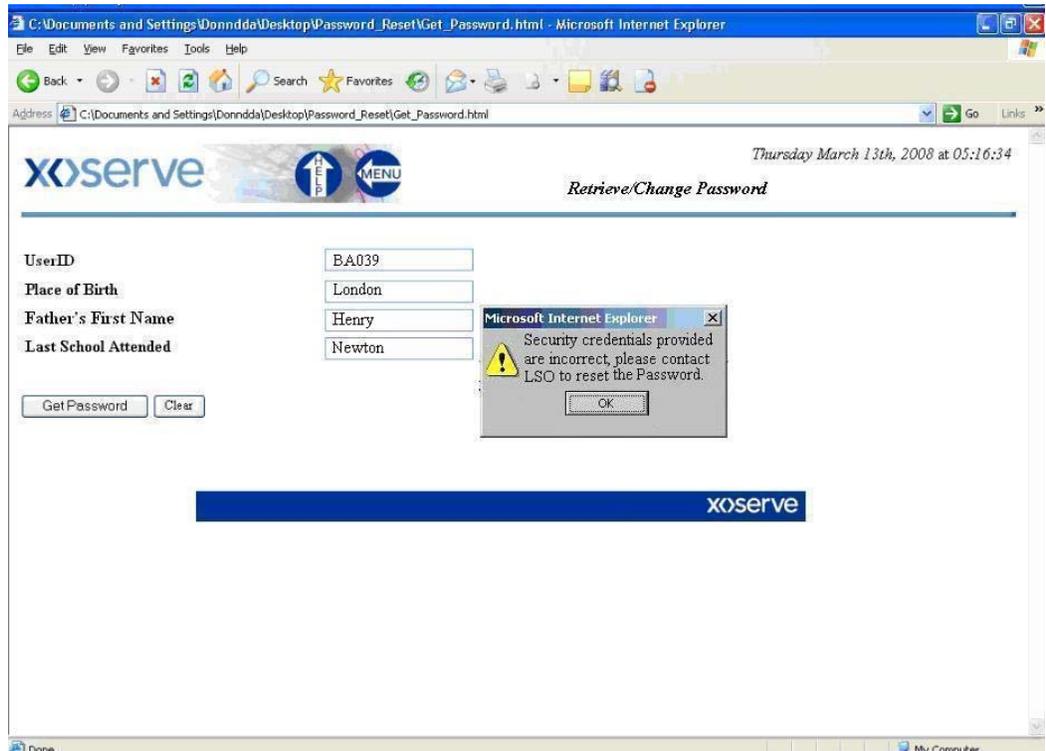
Figure 11 – Retrieve screen when user fails to answer the security questions.