IDHS – Welcome Pack for Secure Data Handling

1. **Document Information**	
Document Name	IDHS-Welcome-Pack-for-Secure-Data-Handling-v2.5.docx
Service	Identifiable Data Handling Solution (IDHS)
Author	Bhavesh Varsani (BV)
Contributors	
Issue Date	27/07/2017

2. **Document History**

Version	**Date**	**Summary of change**
1.0	09/03/2013	First Draft (BV)
1.1	12/06/2013	Document amended and sections added (BV)
1.2	17/06/2013	Sections for Dual factor amended (BV)
1.3	18/06/2013	Dual Factor Mobile App section added (BV)
1.4	22/07/2013	Added Token Management section (BV)
1.5	24/07/2013	Document released (BV)
1.6	01/08/2013	Section 7 and 8 Updated (BV)
1.7	30/08/2013	ICE Steps updated for password forget/expired (BV)
1.8	18/10/2013	Incorporated “Auto generated password” for secure mail out (BV)
1.9	10/03/2014	Incorporated Password Forgotten / Expired process changes (BV)
2.0	15/05/2014	Updated password policies (BV)
2.1	27/09/2014	Secure Print Section added (BV)
2.2	20/10/2014	Presentation update to Password policies defining password polices as applied to relevant portals (BV)
2.3	27/11/2014	Updated the Secure Data out section (BV)
2.4	22/09/2015	Password Policy Updates (BV)
2.5	27/06/2017	Updated file transfer out section to indicate that transfers can be cancelled before a file is downloaded (AJP)

Contents

1. Document Information 1
2. Document History 1
3 Introduction 5
4 Apply for IDHS Service 5
5 Register with UCL IDHS 5
5.1 Password Policy – Data and Apps Portal 5
5.1.1 Password Strength 5
5.1.2 Password Age 5
5.1.3 Password History 5
5.1.4 Password Expiry Notification 5
5.2 Password Policy – File Transfer Portal 5
5.2.1 Username Policy – Applies only to external users to UCL who can only send data in 5
5.2.2 General password policies 5
5.2.3 Password Strength 6
5.2.4 Password Age 6
5.2.5 Password History 6
5.2.6 Password Expiry Notification 6
6 General Overview 6
7 IDHS Data Handling 7
7.1 Setting up and use of UCL Dual Factor Self Service Console 7
7.1.1 First time logon with soft token (software) 7
7.1.2 First time logon with hard token 8
7.1.3 Download and Install Token Auto Generator software 9
7.1.4 First time logon to the Self-service Portal 13
7.1.5 Configure Question and Answers (Q&As) for ICE logon 14
7.1.6 Changing your IDHS Password 15
7.1.7 Changing your PIN for your Token 15
7.1.8 Downloading a software Token 15
7.2 In case of Emergency (ICE) Logon 18
7.2.1 Logon to the UCL Dual Factor Self Service Portal using ICE Logon 18
7.2.2 Report a lost token 20

7.2.3 Generate an Emergency Token 21
7.3 Accessing the IDHS Data Handling Gateway 21
7.4 Accessing Data within the IDHS Environment 22
7.4.1 Using Remote Apps 22
7.4.2 Using Virtual Desktops 23
7.5 Research Shared Folder area 24
7.5.1 Launching Research Shared folder area 24
7.5.2 Research Shared Folder usage 25
7.5.3 When sending Data out 25
8 Secure Data out 26
8.1 Via File Transfer 26
8.2 Via FTP 28
9 Secure Printing from IDHS 29
9.1 Pre-requisites 29
9.2 Applying for Print Service 29
9.3 Printing 29
9.3.1 Print from application 29
9.3.2 Release print jobs 29
10 Registering an external user 30
10.1 Step 1: Send invite by UCL IDHS Research space owner 30
10.2 Step 2: Register by External collaborator 31

3 Introduction

Welcome to the UCL IDHS service, maintained by the IT for SLMS Infrastructure Team. This welcome pack will guide you on how to access the IDHS system and handle data.

4 Apply for IDHS Service

Before accessing the system, you will need to apply to register with the UCL IDHS system information available at https://www.ucl.ac.uk/aisc/services/handling-sens-data/tech-soln (use Mozilla Browser).

5 Register with UCL IDHS

A user name will be created for you, complying with the “Username” and “Password” policies as shown below

5.1 Password Policy – Data and Apps Portal

The Policy below applies only to the Data and Apps portal

5.1.1 Password Strength

```
Minimum Password Length: 7
Password must meet complexity requirements, i.e mixture or Upper
case, lower case, numbers and special characters.
```

5.1.2 Password Age

```
Password has to be changed every 90 days
```

5.1.3 Password History

```
You are not allowed to re-use any of your last 24 passwords
```

5.1.4 Password Expiry Notification

```
Password expiry notification emails are sent 20 days, 10 days, 5 days
and each day less than 5 days before expiry. If password is not
changed then passwords are automatically reset by the system, locking
user out of the system.
```

5.2 Password Policy – File Transfer Portal

The Policy below applies only to the File transfer portal

5.2.1 Username Policy – Applies only to external users to UCL who can only send data in

```
Minimum User Name Length: 6
Maximum User Name Length: 64
Prohibited Characters: /\:*?"<>|@_!#'&
```

5.2.2 General password policies

```
Disable File Transfer account after:
```

```
3 Invalid login attempts
90 Days of inactivity
```

5.2.3 Password Strength

```
Minimum Password Length: 7
Minimum Number of Upper Case Letters:  1
Minimum Number of Lower Case Letters: 1
Minimum Number of Digits: 1
Minimum Number of Special Characters: 1
Allowable Special Characters: ~@#$%^&*()-_=+<>?/\;:[]{},.
```

5.2.4 Password Age

```
Password has to be changed every 60 days
```

5.2.5 Password History

```
You are not allowed to re-use any of your last 24 passwords
```

5.2.6 Password Expiry Notification

```
Password expiry notification emails are sent 10 days, 5 days and 1
day before expiry. If password is not changed then passwords are
automatically reset by the system, locking user out of the system.
```

6 General Overview

IDHS provides three key functions as:

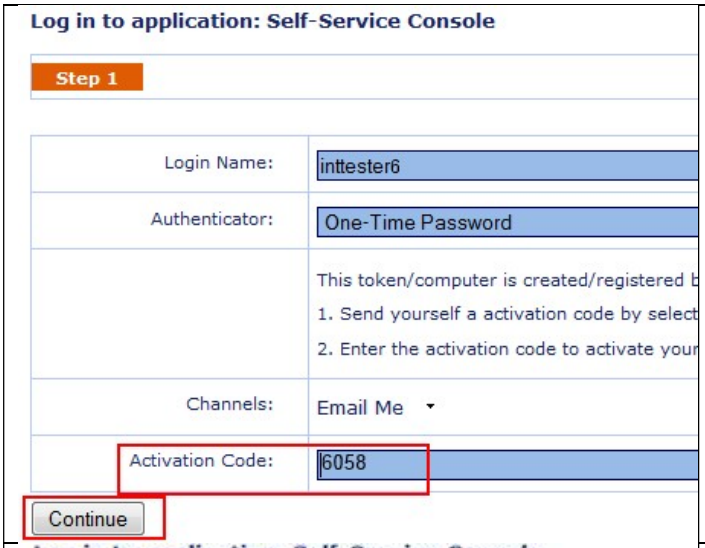
1. Data transfer in via https://filetransfer.idhs.ucl.ac.uk (File Transfer Portal). File transfer in can be done in two ways as described in the “Data Transfer In welcome pack”:
    a. Secure web for up to 5 individual files
    b. Secure FTP using for bulk file transfers
2. Data handling via https://accessgateway.idhs.ucl.ac.uk (Data and Apps Portal)
    a. User your IDHS username
    b. Use authentication combination as:
        i. Password for the IDHS account
        ii. Combination of **PIN** and Auto Generated **Token**
3. Dual Factor – Self service console: Portal to self-register, install auto token generating system and managing via https://registration.idhs.ucl.ac.uk/dss
4. Secure data transfer out via “File Transfer App” via the portal https://accessgateway.idhs.ucl.ac.uk

7 IDHS Data Handling

7.1 Setting up and use of UCL Dual Factor Self Service Console

7.1.1 First time logon with soft token (software)

https://registration.idhs.ucl.ac.uk/dss/	Navigate to the Dual Factor – Self Service Portal
	Enter your IDHS user account and click on continue
	Click on **Channels** and select you pre-registered email address Click continue
	Your email account should get two emails with subject lines **Your activation code &** **Your token**

	**Firstly**, open the email with the subject line **"Your activation code"** By doing this this step, we are activating your token for use. Use the activation code provided in the email. Go back to the Dual Factor Self-service Portal and enter it there. Click on **Continue**
	You will see a message that the token has successfully been activated
NEXT Steps	To download, install and configure the associated software that auto generates your token Section 7.14 of this document

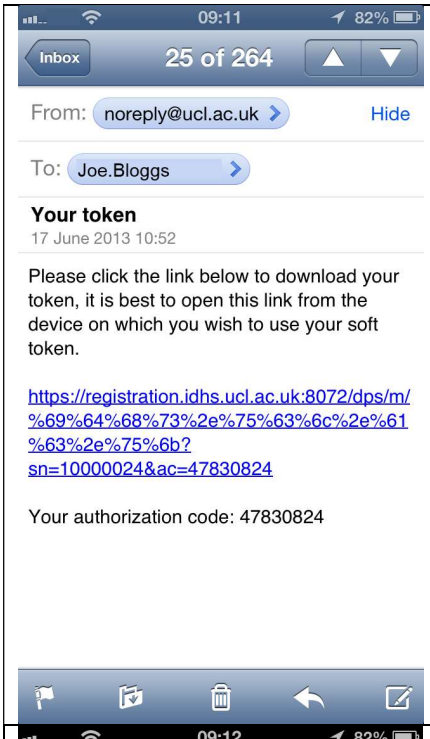
7.1.2 First time logon with hard token

	You have already been provide with a hard token as a new user
	Carry on with section7.1.3: First time logon to the Self-service Portal

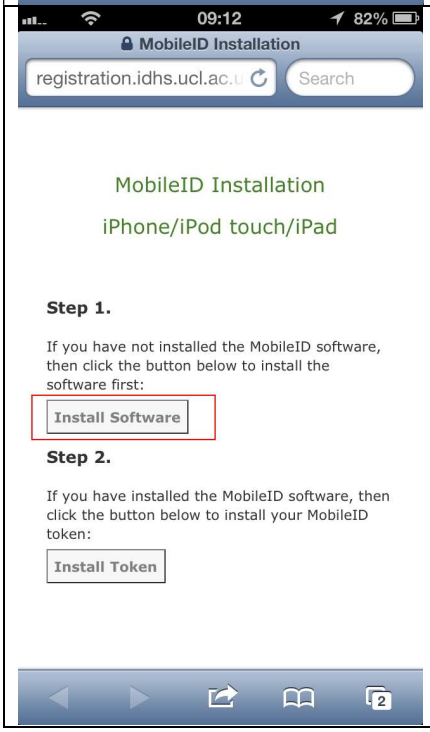
7.1.3 Download and Install Token Auto Generator software

7.1.3.1 Mobile App Instructions

7.1.3.1.1 iPhone, iPod touch and iPad

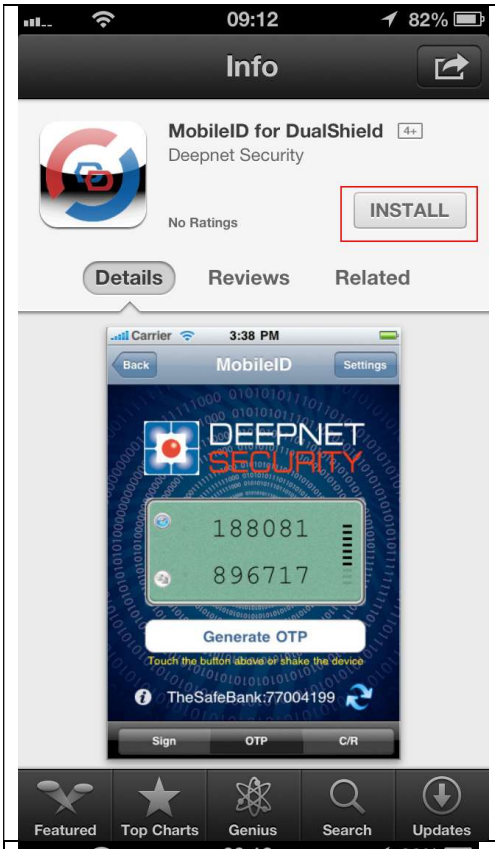
<table>
<tr>
<td> 
</td>
<td>Using your iPhone, iPod touch or iPad, Open the email with the subject line “Your token”

By doing this step you are downloading & installing the application that auto generates the token and installing the token on your device

Click on the link in the email</td>
</tr>
<tr>
<td> 
</td>
<td>A browser within your device will open up as shown in the screenshot.

Complete Step 1 by clicking on “Install Software”

This will launch the Apple Store where you can download and install the free app</td>
</tr>
</table>



Click on Install.

Note: If you have a password for your Apple App Store, please enter your own credentials to allow the install of the software.

Wait for the “MobileID for DualShield” app to install on your device.

Once successfully installed, carry on with the next step

Once your **App has installed**, Go back to the browser page and you will notice Step 1 as complete.

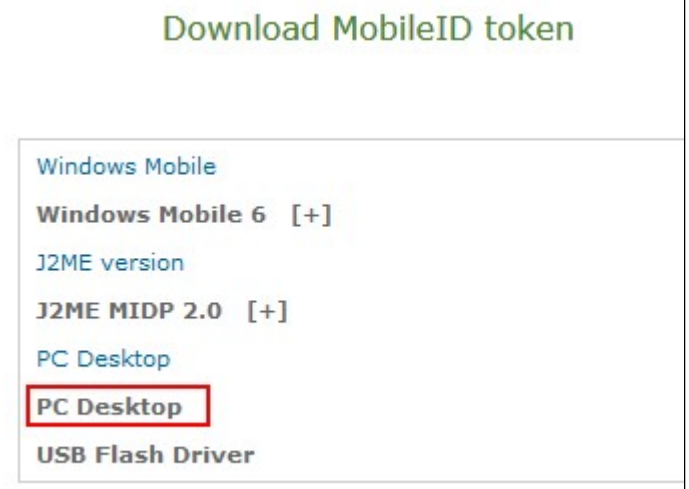
Carry on with **Step 2** to **Install Token** on your device

Click on **Install Token**

	Enter your **IDHS username** and **IDHS password** Click on **continue**
	The token is now available on your device. The token refreshes every 60 seconds. T Before using the token, click on **generate OTP** button to get the latest token
Next Step	Carry on with section [7.1.3 First time logon to the Self-service Portal] of this document

7.1.3.2 Desktop PC Instructions

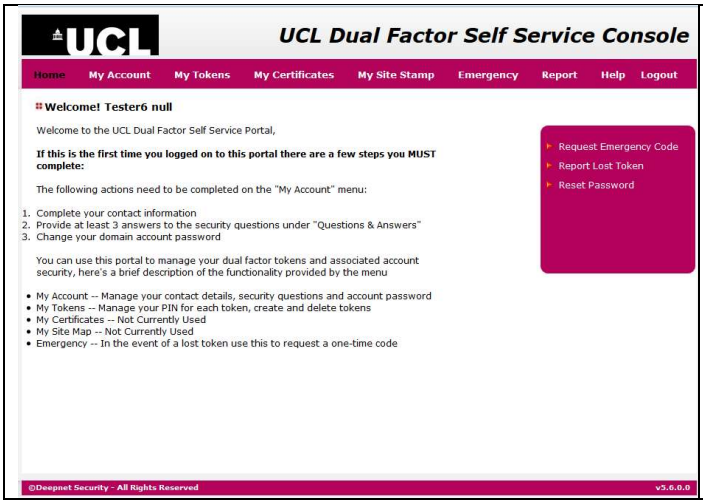
	Open the email with the subject line **"Your token"** By doing this step you are downloading and installing the application that auto generates the token Click on the link and enter your IDHS credentials

	Download the **PC Desktop** and install the software. This is a PC option. For Mobile devices, you will be presented with suitable options
	Click on Next → Agree T&Cs and finish installing

	Launch the installed software "**Deepnet MobileID**" from your PC Start → All Programs → Deepnet security → MobileID Enter your PIN: Default is 1234
	You will get an Auto generated Token that changes every 60 Seconds.
Next Step	Carry on with section 7.1.3 First time logon to the Self-service Portal of this document

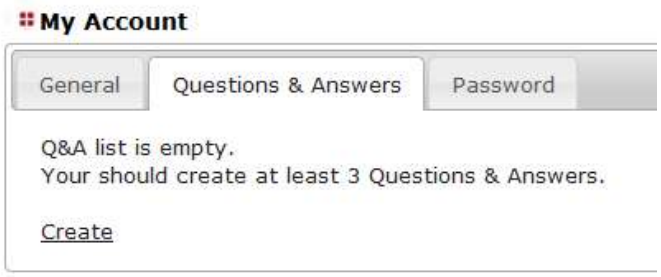
7.1.4 First time logon to the Self-service Portal

URL: https://registration.idhs.ucl.ac.uk/dss/	Go to the self-service portal
	Enter your **One-Time password** If your pin were 1111 and Auto generated token is 290541 One-Time Password = 1111290541
	This step only occurs the first time you log in. Change your pin here



Welcome to your self-service console

7.1.5 Configure Question and Answers (Q&As) for ICE logon



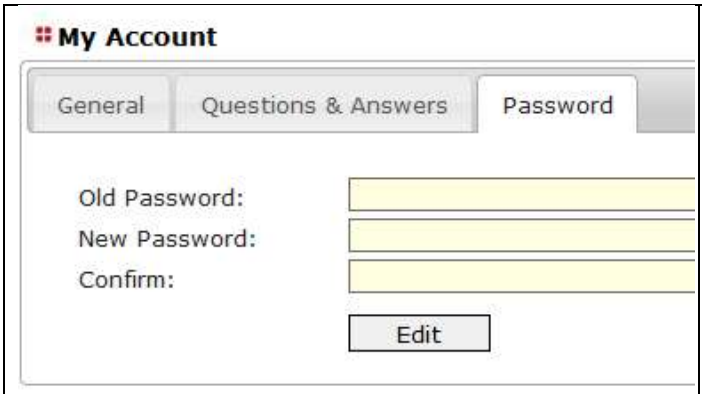
Click on My Account and navigate to the “Question and Answers” Tab

This set up is required to be configured to access the system **“In Case of and Emergency” (ICE Logon)**

Create at least 3 Q&As

These questions will be used to access the system and **generate emergency tokens**

7.1.6 Changing your IDHS Password



Click on **Password** tab to change your IDHS account password

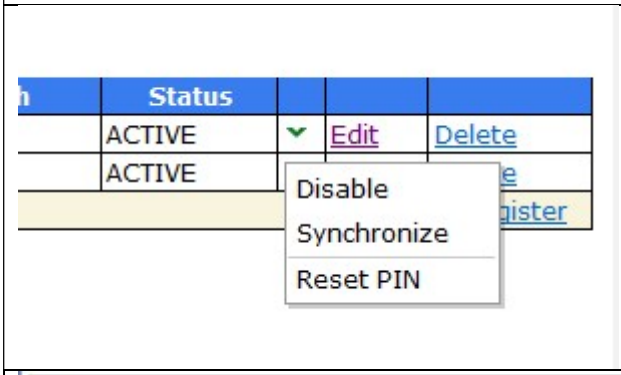
Click on **EDIT** to enable the fields

Then enter the passwords as prompted and click on **save**

7.1.7 Changing your PIN for your Token

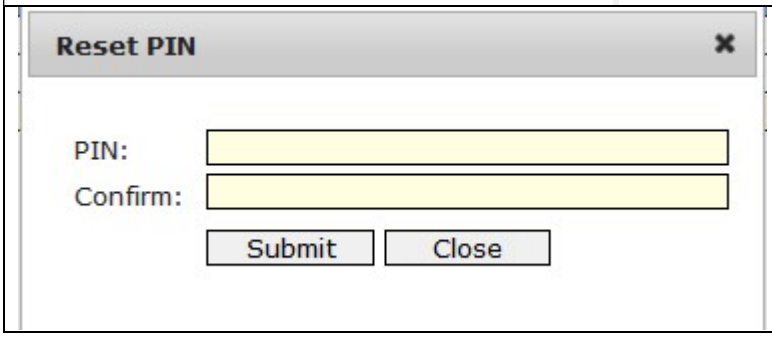
On the Security and Token Portal, click on “My Tokens”

MobileID/Time-Based = Soft Tokens
SafeID/Time-Based = Hard Tokens



Click on the ⌄ next to the token

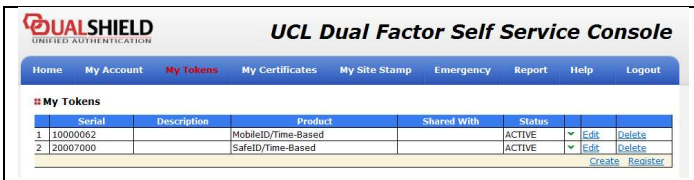
Click on **Reset PIN**



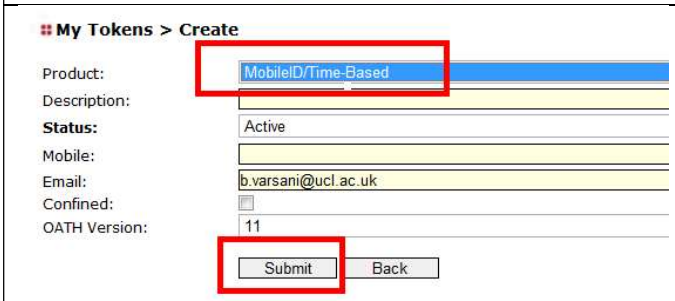
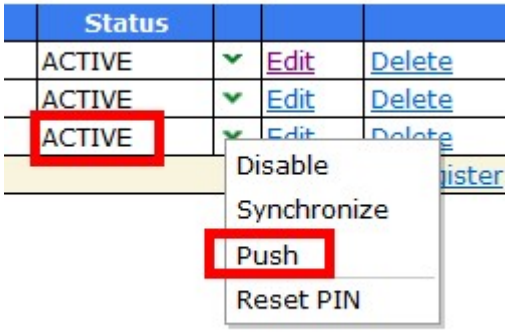
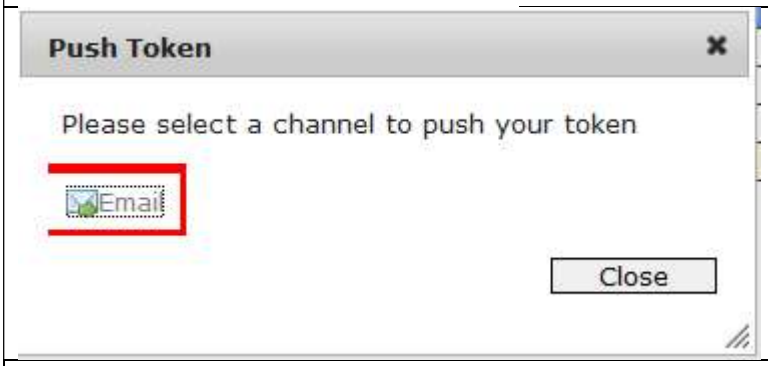
Enter the **NEW 4 digit PIN**

Note: you can only use a PIN once.

7.1.8 Downloading a software Token



On the Security and Token Portal, click on “My Tokens”

	Click on Create
	Ensure Product is : MobileID/Time-Based Click on **submit**
	Activate Token by clicking on email you have been sent to your IDHS registered email with subject line **Your Activation Code**
	Once yoken is activates, the status will be ACTIVE Click on the ⌄ next to the token Click on **push**
	Click on email
Next Steps	Carry on with steps as per section 7.1.3 Download and Install Token Auto Generator software

7.2 In case of Emergency (ICE) Logon

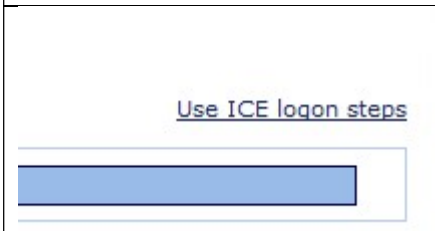
This is a three step process as follows:

7.2.1 Logon to the UCL Dual Factor Self Service Portal using ICE Logon

This process can only be used if you have set up the Q&As as per section 7.1.4 Configure Question and Answers (Q&As) of this document.

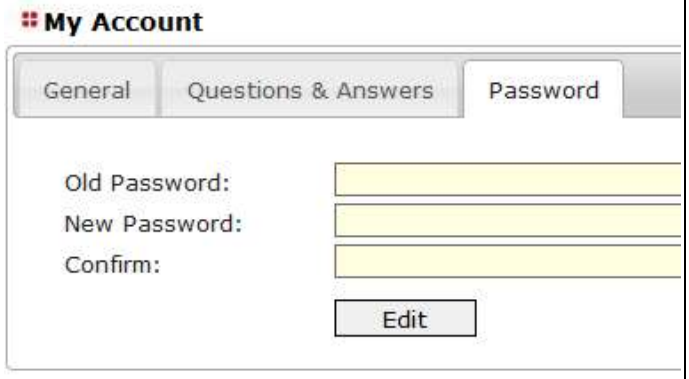
7.2.1.1 Password Forgotten / Expired process

**** For this method you will require setting up a remote session with IT for SLMS Infrastructure team so they can view you go this stage and help you reset your password. They will need to enter your old password for you****

https://registration.idhs.ucl.ac.uk/dss	Logging into self service to generate emergency tokens. Go to the Self service portal **Note**: This will only work if you have created these Q&As during the self service set up as defined in
	Click on **"Use ICE logon steps"** on top of the login name on the right Enter your IDHS username
	Select the **Authenticator** as **One-Time Password** Enter the One-Time Password (PIN+Token)

Enter the **answers to the Questions** previosly set up

Click one Continue



Change Password

Click Myaccount → Password

Click on **EDIT** to enable the fields

Then enter the passwords as prompted and click on **save**

7.2.1.2 Token Lost / not working

https://registration.idhs.ucl.ac.uk/dss

Logging into self service to generate emergency tokens. Go to the Self service portal

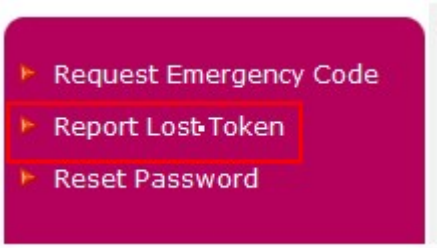
Note: This will only work if you have created these Q&As during the self service set up as defined in

Click on **"Use ICE logon steps"** on top of the login name on the right

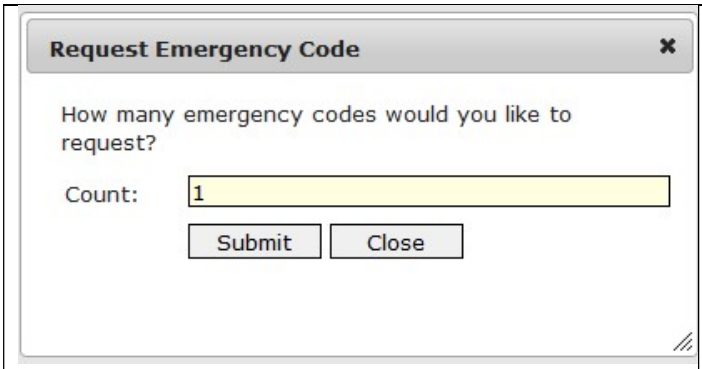
Enter your IDHS username

	Select the **Authenticator** as **Static Password** Enter the IDHS Password
	Enter the **answers to the Questions** previosly set up Click one Continue
	Continue with section 7.2.2 Report a lost token of this document

7.2.2 Report a lost token

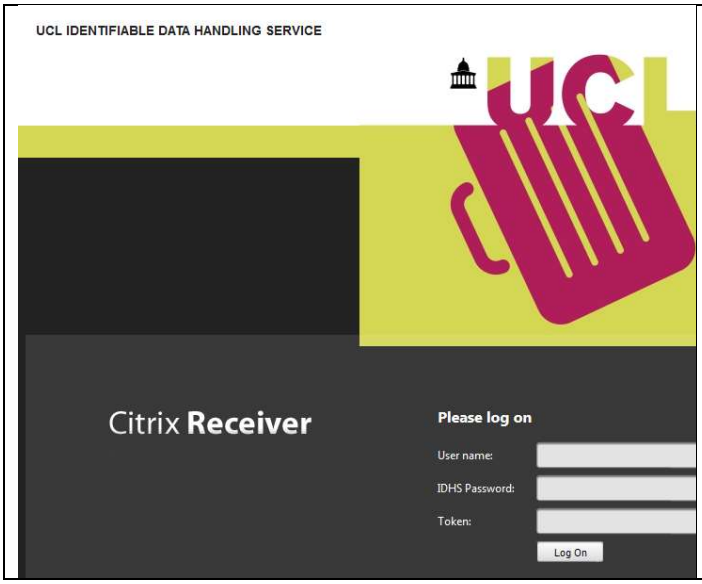
	Click on **Report** or **Report Lost Token** This will notify the IDHS Service service desk with the problem you have occurred by logging a Service Desk Ticket on your behalf.
	Continue with section 7.2.3 Generate an Emergency Token of this document

7.2.3 Generate an Emergency Token

	Click on Emergency to create emergency tokens → select number and click on **submit** The emergency tokens are used to access the IDHS service when you don't have access to the DeepNet Auto token generator or lost your token **You can ONLY use this token ONCE** You can then use this token to login to the IDHS access gateway service (for data handling) and the Dual factor self service portal with your IDHS credentials
	Generate emergency token **Select the Token** by ticking the check box You can either **EMAIL** it to your IDHS registered email address OR **use it to access the gateway** You can ONLY use this token ONCE
	Use this Emergency token as a one time login to access the UCL IDHS Secure Data Handling Gateway
Next Steps	Section 7.3 Access the IDHS Data Handling Gateway

7.3 Accessing the IDHS Data Handling Gateway

URL =	https://accessgateway.idhs.ucl.ac.uk



Login using registered **IDHS Username.**

With dual authentication as:

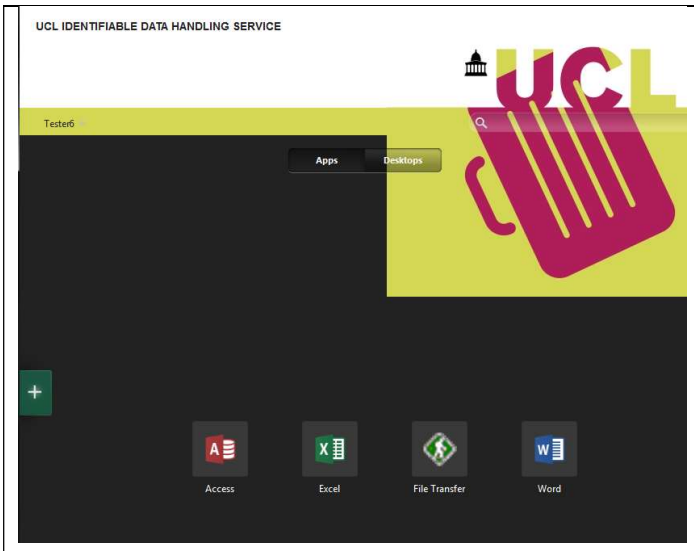
IDHS Password AND

TOKEN (PIN+TOKEN)
If your pin were 1111 and Auto generated token is 29054, then your token will be 111129054

If using emergency token then TOKEN= the emergency token by itself (without the PIN)

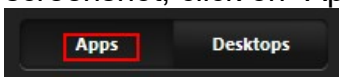
7.4 Accessing Data within the IDHS Environment

7.4.1 Using Remote Apps



Once successfully logging in, you will receive “app” options as shown.

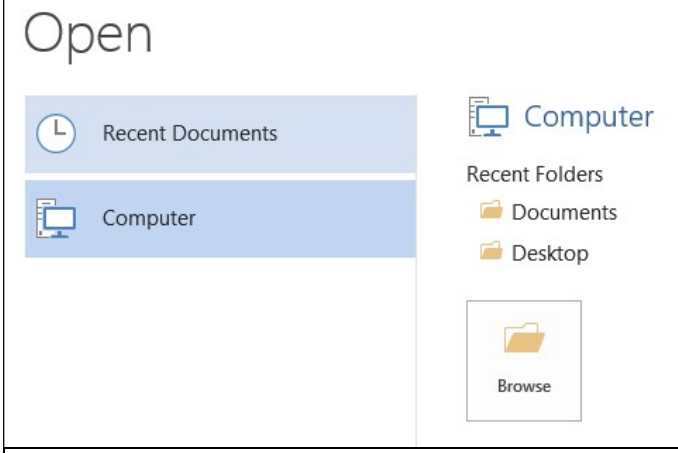
If options not available as screenshot, click on “Apps”



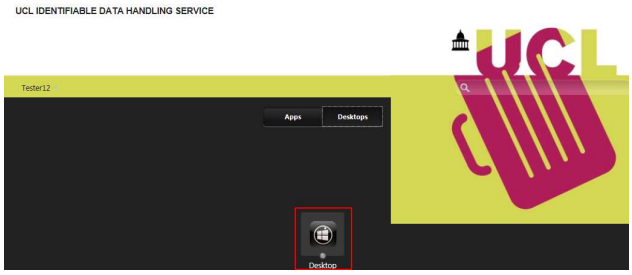
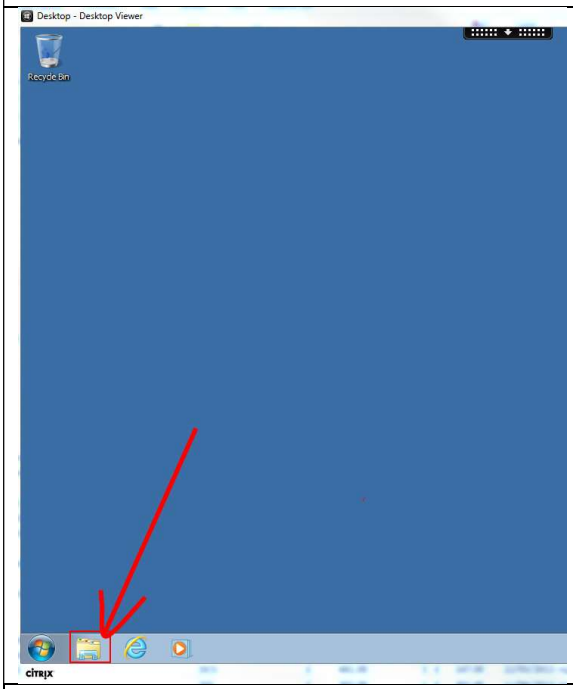
Word – is to launch the word app
Excel – is to launch the excel app
Access – is to launch the access app.
File Transfer – is the link to the IDHS transfer in portal as https://filetransfer.idhs.ucl.ac.uk
Click this link to send data out securely.

Click on app. Word as shown in this example.

Once the app launches, click on open other documents

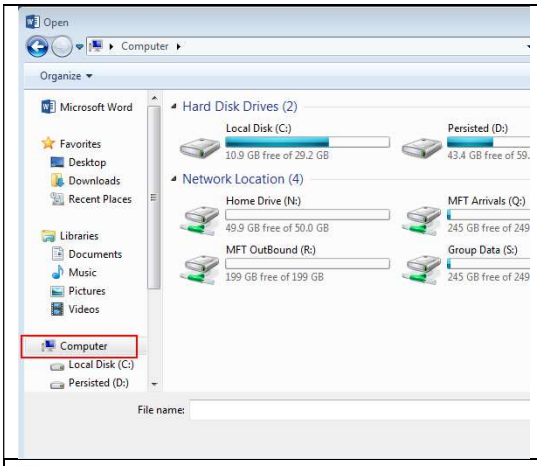
	Click on **Computer → Browse → Computer**.
Next Step	Section 7.5.1 "Launching Research Shared Folder area" of this document

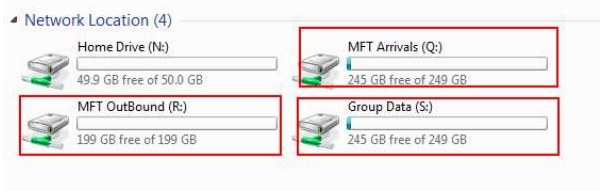
7.4.2 Using Virtual Desktops

	Once logged in, to use a Desktop to access the data, click on **"Desktops"** Then click on Desktop icon as squared on the screenshot on the left. This will launch a virtual desktop.
	A new window citric session will open. To view the data click on the Windows Explorer icon as shown
Next Step	Section 7.5.1 "Launching Research Shared Folder area" of this document

7.5 Research Shared Folder area

7.5.1 Launching Research Shared folder area

<table>
<tr>
<td> 
</td>
<td>Click on Computer on the left hand Menu</td>
</tr>
<tr>
<td>There are three possible locations where data exists:
MFT arrivals, Group Data and MFT Outbound

Both MFT arrivals and Group Data will have a folder within it for each Research space that a user will have access to.
 
</td>
<td>MFT Arrivals* is where the encrypted data arrives when sent in.

Group Data is where data needs to be decrypted and stored. This is the location where the data should be transferred too.

MFT Outbound is where data you want to send out should be copied to before sending the data out. Then follow <a>section 8 “ sending data out” of this document

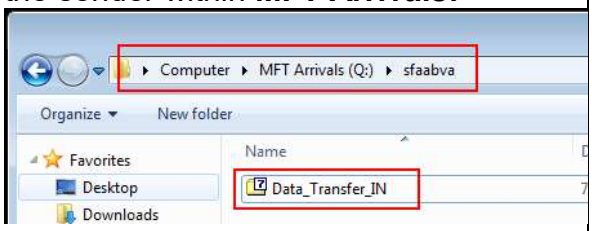
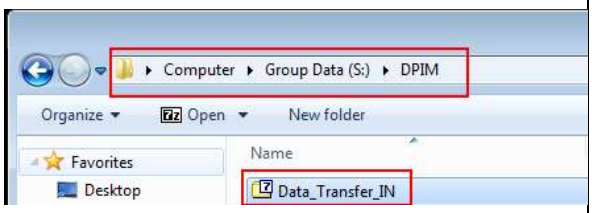
All three folders except MFT Arrivals* should have the same Research space name.

MFT Arrivals* will have the usernames of the sender as the folder name.

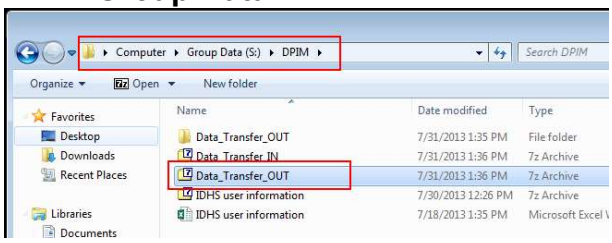
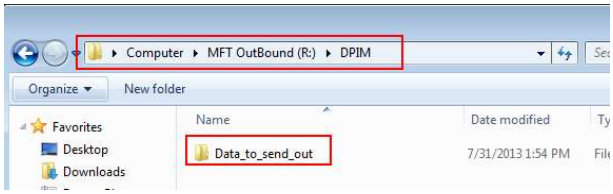
*Data that a user sends into the IDHS system will be under their own username within the MFT Arrivals</td>
</tr>
</table>

7.5.2 Research Shared Folder usage

7.5.2.1 When receiving data

Transfer data from the "**Username"** of the sender within **MFT Arrivals:**  To the same **research space** within **Group Data**  For the purpose of this document, the sender of data is **sfaabva**	Data should be transferred from **MFT arrivals** to the relevant **Group Data** folder then decrypt the data to complete the process. MFT arrivals should NOT be used for storing data. ***MFT arrivals folder should have encrypted documents sent in. Once you move the data to Group Data folder Decrypt the data. The password for decryption should be provided to you by the sender of the data*** As a guide please view the IDHS encryption document On how to decrypt the data. https://www.ucl.ac.uk/isd/itforslms/services/handling-sens-data/tech-soln/IDHS-Service-Quick-Links

7.5.3 When sending Data out

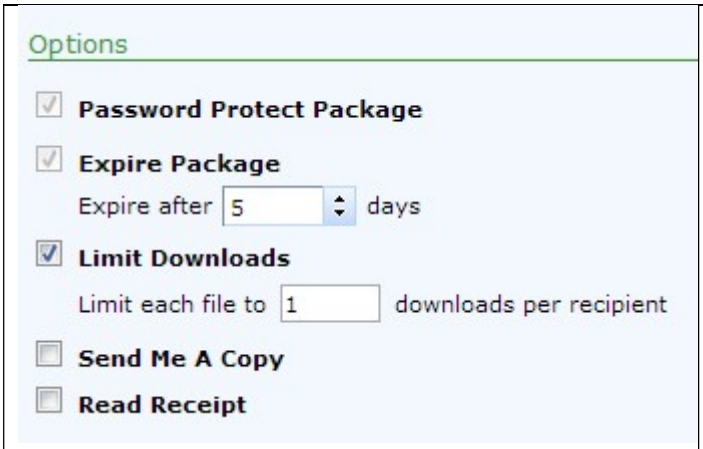
Transfer data from the **Research space** within **Group Data:**  To the same **research space** within **MFT Outbound**  For the purpose of this document, Research space name is "DPIM"	Data should be transferred from **MFT outbound** to the relevant **Research Group Name** folder. MFT Outbound should NOT be used for storing data. ***MFT Outbound folder should have encrypted documents ready to send out. Once you move the data to MFT Outbound folder, follow section 8 "Send Data out" of this document***

8 Secure Data out

Before using this section, ensure that you have copied the data you want to send out to the folder for your relevant research group name under **MFT Outbound using the Data and applications portal** https://accessgateway.idhs.ucl.ac.uk

8.1 Via File Transfer

https://filetransfer.idhs.ucl.ac.uk	File Transfer Portal
	Login to the File Transfer portal
	Click on secure mail
	Click on new message
	Fill in the To field, subject and message



Under options, note a password for the secure email is ticked. **This password will be auto generated and Encrypts the data**

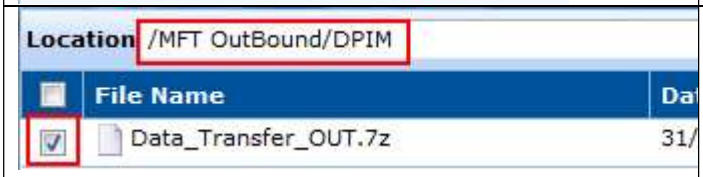
When you send the package this password will be displayed to you

Enter days of expiry

Enter download limits

Attach file or files you want to send out.

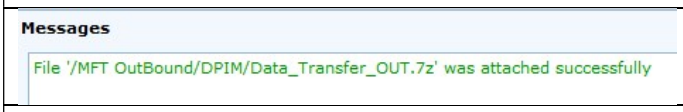
Click on Attach a file from my workspace



Browse to Location (Research Group Folder) under the MFT Outbound folder

Select the file to send

Click attach file



View successful attached message and click on **close**

Click on send.

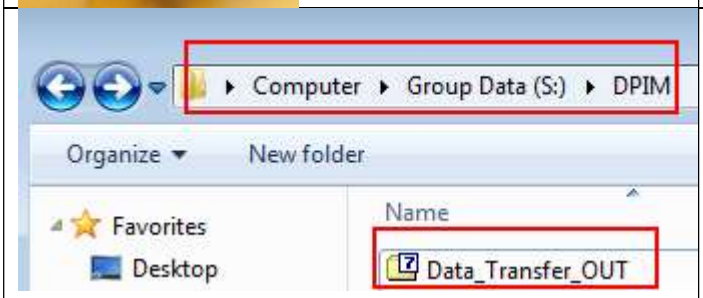
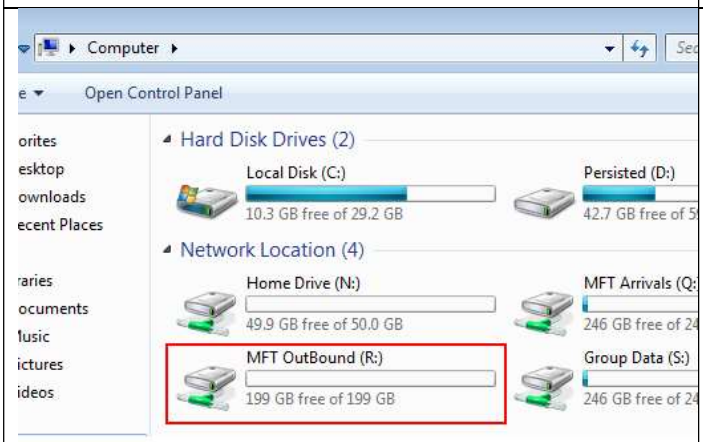
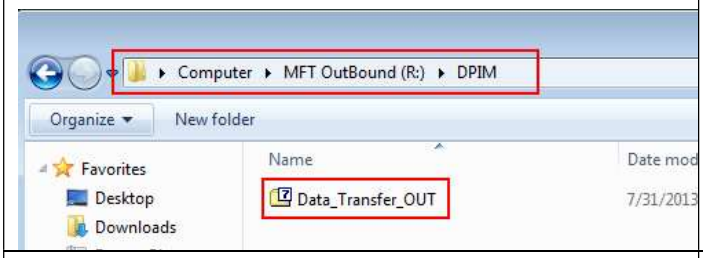
Note the password "auto generated" by system

This password will be required by end user to download the package

Notify user the password to download package.

NB: In the case that you want to cancel a transfer, the Data Safe Haven support team can remove the file before it is downloaded. Contact your usual support channels for help.

8.2 Via FTP

	Encrypt the folder first. Using the “Desktop” version of IDHS
	Locate the files to be transferred from the “**Group Data**” Drive and respective research folder. In this case from research folder “**DPIM**” Folder to transfer is the encrypted folder as “**Data_Transfer_OUT”**
 Browse to Copy the folder to the respective Research folder (DPIM in this case)under “**MFT OutBound**” 	Copy the folder to send out to location as shown
	Ask user to make an FTP connection and download the files from the MFT Outbound Folder.
	Provide the receiver the password to decrypt.

9 Secure Printing from IDHS

9.1 Pre-requisites

- Completed physical risk assessment and part of an audit programme. If studies have a current successful IG Toolkit submission (via the UCL Information Governance Advisory service) then the Information Asset Owner (usually the PI) can apply for secure printing service

Note: if studies have NOT completed a physical risk assessment and not part of an Information Governance Audit programme, then the Information Asset Owner should request a physical risk assessment by emailing slms.pid@ucl.ac.uk

9.2 Applying for Print Service

- Complete the form as http://www.ucl.ac.uk/isd/itforslms/services/handling-sens-data/tech-soln/docs/using-IDHS/application-forms/IDHS-New-Service-Request-Form.
    - Service name – state as “Secure Print Service”
    - Project Name – Your study name (same name as the share already on IDHS)
    - Notes / Further info: Printer Make, Model and IP address
    - Add members to access the “Services”: Add users name, username and service that they require access to
    - Where it asks for the Information Asset Owners signature, this is the data owners signature (usually the PI)
    - Send a completed and signed form as below to your usual IDHS route channels. If not sure visit http://www.ucl.ac.uk/isd/itforslms/about/contact

9.3 Printing

Once secure printing has been set up, log on to the “Data Safe Heaven” (aka IDHS) https://accessgateway.idhs.ucl.ac.uk and open your document that you would like to print.

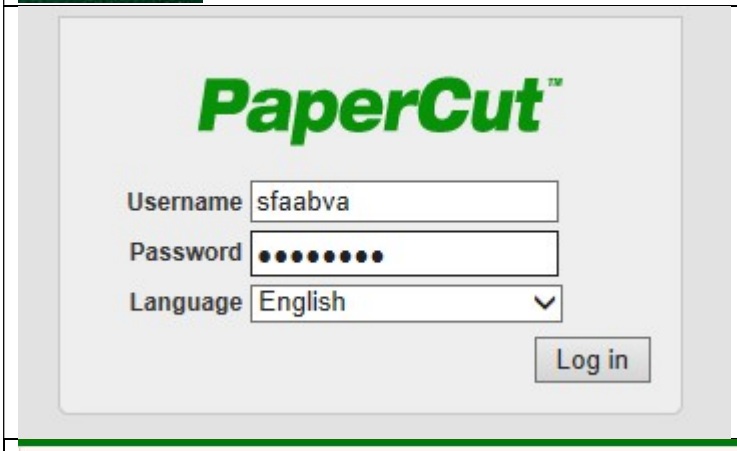
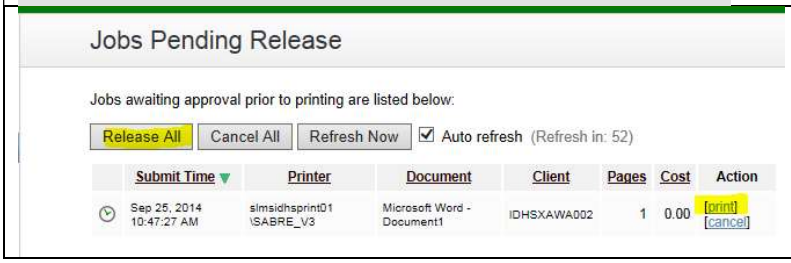
Printing is a two stage process as below:

9.3.1 Print from application

Print the document to the preferred printer. If you have rights to print to more than one printer, ensure you are selecting the printer that you want to print to.

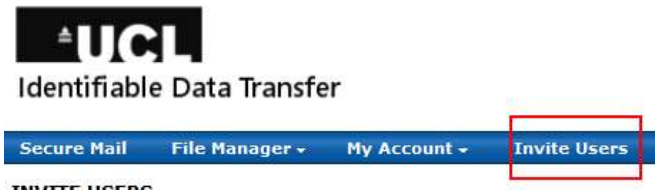
9.3.2 Release print jobs

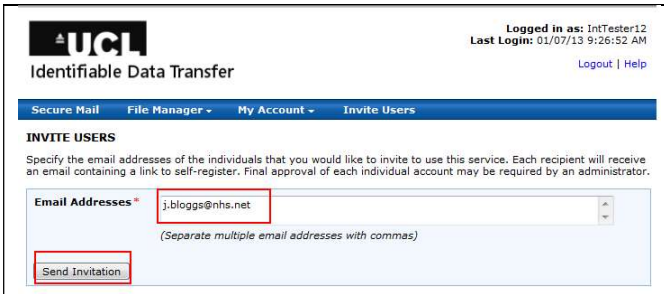
This feature has been added as a queue management allowing users to queue up jobs till they are ready to release them and collect them.

	Launch “Secure Printing” Application Either as an “app” or within “Secure Desktop”
	Login using your UCL IDHS credentials
	Release Print job to printer

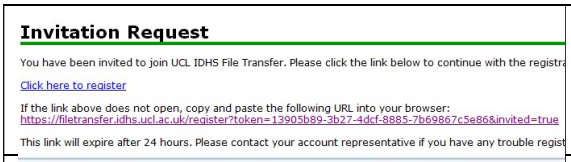
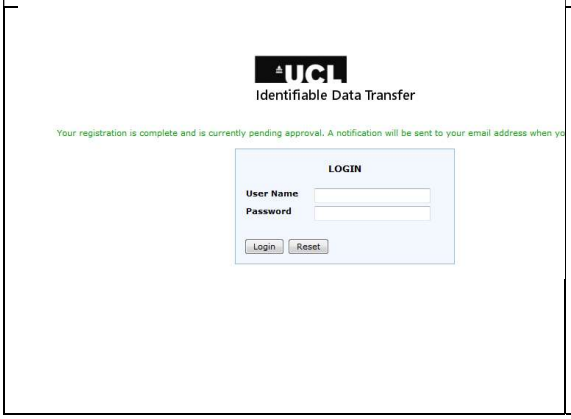
10 Registering an external user

10.1 Step 1: Send invite by UCL IDHS Research space owner

https://filetransfer.idhs.ucl.ac.uk	Browse to the **filetransfer** portal
	Login using your UCL IDHS credentials
	Click on Invite Users from the menu **Note**: This will only show on the menu if you have specific permissions to invite users

	Type the email address of external collaborator to send and invite to. Click on Send invitation
	Confirmation message that the invite has been sent

10.2 Step 2: Register by External collaborator

	The external collaborator now registers by clicking on the email they receive. **Note: This link expires after 24 hours**
	External user will register with fields as shown. Click on Submit
	External users can now automatically log in. Please provide them with the “Welcome Pack for Data Transfer IN” Available at: https://www.ucl.ac.uk/isd/itforslms/services/handling-sens-data/tech-soln/welcome-packs

End of Document