Equally Safe in Higher Education

Data Operation Procedures

Authorised by	
Date	
Version	
Next review date	

Contents

Introduction

Equally Safe in Higher Education (ESHE) works with extremely sensitive personal data, or "special categories of personal data" as described by GDPR. It is therefore imperative that everyone that works with the data ensures they comply with the procedures to keep this data as safe and secure as possible.

Basically speaking, we are looking to ensure a high confidence that only the right people have the right level of access to the right data.

USER

Policies

1. The ESHE folder in Strathcloud will be the location to store all ESHE files.
2. Files must not be shared with users out with Strathcloud.
3. Specifically, the "share -> get a link" functionality of Strathcloud should not be used.
4. Specifically, ESHE files must not be emailed, they must only be accessed via Strathcloud.
5. Strathcloud allows access from any device from any location. You must only access from a device that you are confident is secure.
6. The Strathcloud sync app must not be used to sync ESHE data to your local device.
7. ESHE files must only be downloaded or checkout to university owned domain connected devices and if the device is portable it must have encryption enabled.
8. Reduce the amount of time and number of ESHE files that are held on your local device.
9. All files created must be tagged and categorised as "ESHE".

Procedures

Create a file

When created a Microsoft Office file on your device, for a ESHE case, tag and categorise the file:
Right click file and select "Properties"
Select "details" tab
Double click next to "Tags"
Type "ESHE"
Double click next to "Categories"
Type "ESHE"
Click "OK"
By tagging a file it makes it easier to identify if these files turn up somewhere they should not be.

Upload a file

To store and share your file upload it to Strathcloud – it will automatically be shared with those that the folder administrator has given access to:
Navigate your browser to https://strathcloud.sharefile.eu
Login with DS account
Go to "Folders - >Shared with me"
Select the folder "ESHE"
Select the corresponding folder to upload your file to
Click the + and select upload
Navigate to your file and click upload
Your file is now accessible by anyone that has access to that folder (as set up by the administrator)
Delete the version of the file on your local device and delete from recycle bin

View a file

From a device you trust
Navigate your browser to https://strathcloud.sharefile.eu
Login with DS account
Go to “Folders - >Shared with me”
Select the folder “ESHE”
Select the corresponding folder
Click the file to view securely on line

Update a file

On a university owned device (and one with encryption enabled for portable devices)
Navigate your browser to https://strathcloud.sharefile.eu
Login with DS account
Go to “Folders - >Shared with me”
Select the folder “ESHE”
Select the corresponding folder
Check the file you want to update
Select “…More” and click Checkout
Select “download”
Edit your file
Check in your file – you will be asked to upload it
Delete the version of the file on your local device and delete from recycle bin

Request 3rd party Access

If you wish to have someone else added to a folder, contact an administrator of the folder.

ADMINISTRATORS

Policies

1. The ESHE folder in Strathcloud will be the location to store all ESHE files.
2. Files must not be shared with users out with Strathcloud.
3. Specifically, the “share -> get a link” functionality of Strathcloud should not be used.
4. Specifically, ESHE files must not be emailed, they must only be shared via Strathcloud.
5. Strathcloud allows access from any device from any location. You must only access from a device that you are confident is secure.
6. The Strathcloud sync app must not be used to sync ESHE data to your local device.
7. ESHE files must only be downloaded or checkout to university owned domain connected devices and if the device is portable it must have encryption enabled.
8. Reduce the amount of time and number of ESHE files that are held on your local device.
9. All files created must be tagged and categorised as “ESHE”.
10. Administrator must ensure access only provided to correct contacts.
11. Administrator must maintain audit records.

Procedures

Create a new folder

When you create a new folder, decide on the access requirements:
Who should have access
What access should they have
Should this folder be deleted on a certain date
Record the details in your audit spreadsheet

Add a contact to a folder

If you have been asked to add access for an existing contact, to gain access to a folder:

Verify that this contact should have access
From a device you trust
Navigate your browser to https://strathcloud.sharefile.eu
Login with DS account
Select the folder “ESHE” (it may be a personal folder or it may be under “shared with me”)
Select the corresponding folder
Select “people on this folder”
Click “add people to this folder”
Select the contact and select the desired access level
Record the access in your audit spreadsheet
If using a honey trap add download user access (see later)

Create a new 3rd party contact

If you have been asked to add access for a new 3rd party organisation, to gain access to a folder:
Verify that this contact should have access
Ensure there is a GDPR data sharing agreement in place with the organisation
Ensure that this is for a named individual at the organisation and not for a shared account
Request a Temp IT account from ISD (they will provide a DS username password for the new contact)
From a device you trust
Navigate your browser to https://strathcloud.sharefile.eu
Login with DS account

Select the folder “ESHE” (it may be a personal folder or it may be under “shared with me”)
Select the corresponding folder
Select “people on this folder”
Click “add people to this folder”
Select the contact and select the desired access level.
Record the access in your audit spreadsheet
If using a honey trap add download user access (see later)

Create a Honey Trap

A honey trap is an enticing location (folder and files) that no normal user should need to access. It is designed to help identify if a malicious actor has access to a legitimate account. If these folders and files are accessed it is an indication of a possible breached account.
In the ESHE folder create a folder called “Accounts”
Check the box “email me when a file is downloaded from this folder”
In the Accounts folder upload a file called “bank details.zip” with fake details in it
Ensure users know not to access this file

Receive a Honey Trap email notification

Contact the user to see if it was them by mistake, if it wasn’t, contact helpdesk and raise a “cyber-security – compromised account incident”

Audit Check

At least every 3 months, download the audit files, store with your audit spreadsheet and look for anomalies.
From a device you trust
Navigate your browser to https://strathcloud.sharefile.eu
Login with DS account
Select the folder “ESHE” (it may be a personal folder or it may be under “shared with me”)
Select “… more options -> View activity log”
Select all users
Tick all activities
Select the data range as last 3 months
Click “Export to Excel”

- Look for anything where the user is noreply@sf-notifications.com – this means policy has been broken and a file has been shared without login
- Look for anything where the username is an email address – this means policy has been broken and a file has been shared without login
- Look for anything interacting with the honeypot
- Look for anything suspicious (such as a large amount of files downloaded by a user, or access at strange times)

Record your audit findings in your audit spreadsheet and contact cyber security for anything strange

Annual Audit

Check that accounts still need access to the folders:
Ensure any data no longer required to be kept is removed
Ensure that any access no longer required is removed (especially 3rd party)
Record findings in your audit spreadsheet