VLE Transition feedback from Academic Partners

The information below can also be found in the document How to send sensitive data safely but has been edited slightly.

UHI Dropbox

UHI Dropbox is a file transfer system provided by UHI LIS Department. The service is not for creating back-ups but for exchanging sensitive data. It is available at: https://dropbox.uhi.ac.uk/.

1.1 It's not the same as dropbox.com.

UHI Dropbox is not the same as the online 'Dropbox' services (dropbox.com ; wetransfer.com) you may be aware of. **For GDPR reasons, you must not use either of these services (dropbox.com ; wetransfer.com).**

In addition, UHI Dropbox is a service provided by UHI LIS for transferring files only, and not for creating back-ups. Please create your own back-ups if necessary, as files in UHI Dropbox are automatically deleted after two weeks as a security measure.

1.2 Where can I get help?

If you're not familiar with using UHI Dropbox please review the UHI FAQs page at: https://dropbox.uhi.ac.uk/. If you would like some extra help understanding and using the service, please contact your local ICT team for assistance.

1.3 Log in to UHI Dropbox

Logging in to UHI Dropbox allows you to send files. It also allows you to see the files you have sent and received via UHI Dropbox and receive confirmation when recipients collect files you have sent. It also allows you to delete sent files from UHI Dropbox if there are any problems, so that they cannot be downloaded (note that deletion will not apply to any files already downloaded).

1.4 Verify email address and enter is correctly

Use the UHI Outlook system to make sure you are sending to the correct person. Be aware that many staff and students have the same, or similar names and email addresses. Use the Outlook address book function to make sure you are sending your files to the correct person.

If you cannot verify using the Outlook system you can ask the intended recipient to send you an email, to ensure that you have their correct email address.

UHI recommends copying and pasting the email address of the recipient from Outlook into UHI Dropbox when asked to enter the email address. This will help avoid misspelt names or other errors resulting in the file not sending or going to the wrong address.

1.5 Don't enter any sensitive data in the text box. Instead, put sensitive data into a file and send the file via UHI Dropbox

Recipients with access to the link will be able to see the contents of the text box without the password. For that reason, do not enter sensitive data in the text box, put the sensitive data in a document and send that document, encrypted (see next step), via UHI Dropbox.

1.6 Always click 'Encrypt every file' and create a strong password

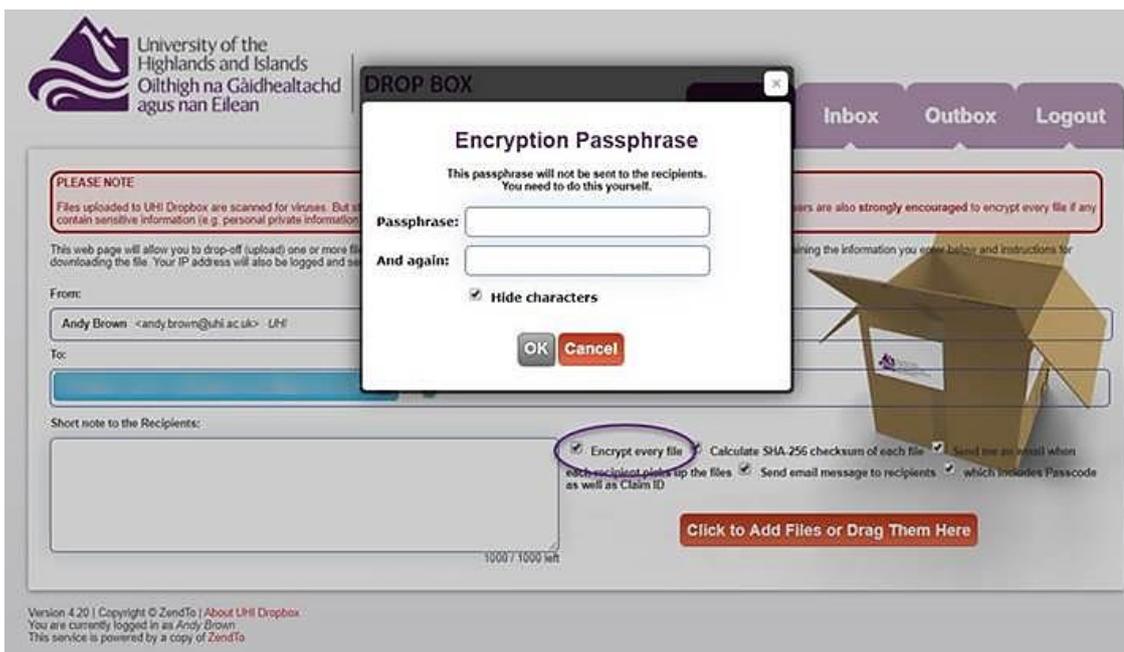The encrypt every file option is circled in the picture below.

Figure 1: Screenshot of the UHI Dropbox page with the Encryption pop-up window

Web: Educational Development Unit website   Email: Educational Development Unit Email Address

Create the password using the [LIS guidance for creating a password](): your password needs to be a minimum of 8 characters and contain at least 3 of the following 4 character sets:

1. **Numeric: 0 1 2 3 4 5 6 7 8 9**

2. **Lower Case: abcdefghijklmnopqrstuvwxyz**

3. **Upper Case: ABCDEFGHIJKLMNOPQRSTUVWXYZ**

4. **Special Characters: ~@#!"$%^&*()_+=\[]/{};,.?'**

Your password will not be sent to the recipients automatically.

1.7 Always communicate the password to the recipient via other means – telephone is best.

If an unauthorised party gained access to the Dropbox email, they would probably have access to other emails meaning that if you send the password via email the unauthorised party has both the link and the password. This risk is avoided by always communicating the password to the recipient via other means. Telephone is the best way of achieving this. Do not give the password to anybody but the intended recipient.

1.8 Remind recipients that the file will not be encrypted when they receive it.

UHI Dropbox encrypts files whilst they are in transit, but they are decrypted once they arrive with the recipient (once they have entered the password correctly).

If you wish to send a file that will remain encrypted after transfer, please contact your local ICT team.