This safeguarding data section focuses on the accessing data on the staff network from other networks and from off campus.

More comprehensive instructions for using TrueCrypt are in the Remote Access Guide.

After this introduction, you could use the guide to

-    demonstrate accessing the staff network through the student network .

-    assist the audience in setting up emails on their mobile devices, laptops etc. that they have brought with them to the session.

Focus: Two networks at UH

Main points:
-    access to core services is restricted to staff so unless they're on the staff network, they are considered off-site.

Highlight that they can still access these services using network connect and Novell.

Focus: Network Connect online

Main points:
-    log into the UH VPN – the virtual portal.

Highlight from this site you can access the staff store and email, but it can be a little clunky. We recommend getting access from your machine.

Focus: Network connect on your machine

Main points:
-    Once downloaded, can be run from the start menu

Highlight that this gives access to the online services, outlook, and engage.

Focus: Novell

Main points:
- Install the package with the UH settings in place.
- Must login to view the drives

Highlight that the other options are all set in the package that is downloaded so don't play around with the settings as this will damage the connection.

Focus: Email

Main points:
- Outlook exchange is available on the net, on your machine off campus, on your mobile and your tablet.

Highlight that instruction and settings for the domain etc. are available in the Remote Access Guide.