Laptop Advice – Home Working Options and Encryption Advice

1. Background

   When you log on to the University ISAD several valuable changes are made to the way you work with your computer. First your username and password are checked, then you are given access to all the right resources, such as network printers, a shared drive (N:) for collaborative file storage, and most importantly a user drive (U:) for your personal 20 Gb of file storage. Using some technical magic the My Documents folder on your computer is relocated to become your U: drive and your Desktop folder is relocated and stored within your U: drive. This means that, unlike on non University owned laptop, your files are safely stored on secure, reliable and backed up network storage instead of a computer hard drive that is vulnerable to failure or theft.

2. Getting Started

   To prepare a new laptop for home you must connect it to the University network and log on to ISAD. Then you should follow the steps in Section 3 to "Make Available Offline" all of the folders that you would like to see when NOT connected to the University network. This will include the Desktop folder and any other folders in your U: drive that you want to work on.

3. To Make Files or Folders Available Offline (also referred to as Synchronizing)

   - In your U: drive, right-click the file or folder, and then click **Make Available Offline**. (Put files in a folder than sync them individually). The Offline Files Wizard starts. Click **Next** to continue.
   - Check box to **Automatically synchronise the Offline Files when I log on and log off my computer** and then click **Next**.
   - Do not select **Create a shortcut to the Offline Files folder on my desktop**. Click **Finish**.
   - Choose whether or not to make the entire contents of the folder available offline. The files are then copied to your computer.

4. Working Offline

   - You now have copies of chosen files on your laptop and can update them or write new documents when you have no network connection, (off line). When you next connect to the University network and log on, windows updates the out of date copies that are stored on your U: drive, hence the term synchronisation.
   - If you disconnect from the University network whilst working on a document you "go offline" and are notified by an icon that appears at the bottom right hand corner of your screen. This means that when you save the document it will be an offline copy to be synchronized when you next connect to the network.

5. Controlling Synchronisation

   - From the Tools menu in My Computer, choose Folder Options, then Offline Files
   - Choose when to synchronise by checking the "at log on" or "at log off" boxes. It is recommended that work carried out on off-line files is synchronised as often as possible on campus to avoid the possibility of loss of work.
   - To stop a file/folder being synchronised: right click on the file/folder and un-tick the **Make Available Offline** option.

6. Manual Synchronisation

   To synchronise files or folders manually, right click on the desired file or folder and choose "synchronise". If necessary, you can right click on the U: drive using the same method

7. Alternative to Working Offline

   You can access your U: drive from off campus by making a Virtual Private Network (VPN) connection. This is a secure connection that will allow you to view all your files/folders as if you were in the office. Files that are saved whilst connected over a VPN are saved directly to the U: drive. Hence when you disconnect the VPN you will no longer see them. NB This method of working requires a fast network connection to work smoothly.

True Crypt Encryption

All new University laptops will be encrypted with True Crypt full drive encryption to protect a user's files/folders in the event of the laptop being lost or stolen.
When you turn on an encrypted laptop you will be prompted for your True Crypt password before the machine will start up. If you forget your password or suspect your laptop might have been compromised please contact the University IT Help Desk for further advice on 01392 263934. **Do not attempt to fix it yourself**. DO NOT write down your password and keep it in the bag with the laptop as in the event of the loss of the system this will render the encryption in-effective.

Please go to the link below for more information on Encryption – it's very important you understand the implications of why University laptops are encrypted, as well as your related responsibilities.

http://as.exeter.ac.uk/it/regulations/infosec/encryptionforlaptops/