



How to use your new Encrypted USB Pen Drive



Introduction

With the increasing need to have access to data at any time it has never been more important to secure that data on mobile devices.

Advances in technology bring new threats that need addressing and USB Pen Drives, while extremely useful and versatile, have always had the issue of how you protect the data you store on them.

Information Security have conducted extensive research into this issue and have come up with the solution in the form of a USB Pen Drive with high-level encryption built in.

What needs to be stored on the drive?

Any information classified as “Protect” or “Restricted” needs to be protected while off site and must be stored on the encrypted USB Pen Drive.

For an explanation of these classifications, please refer to the “Protective Marking, Handling and Disposal Policy” which is available from the “Information Management” area on the Intranet, under “Advice and Guidance”.

How to use your new drive

When you first plug the drive in, Windows will install the drivers needed to use the device – don’t worry if you see some messages appear in the bottom right hand corner; this is normal. Depending on how you have Windows configured (i.e, whether you have enabled the ‘Autorun’ feature), one of two things will happen next:

1. The install screen will appear and will begin the process needed to set up a password on the device **OR**,
2. **You will have to manually start the device:** Go to “My Computer” or a location where you can see all your drive letters (C:, D:, etc) and look for the following:

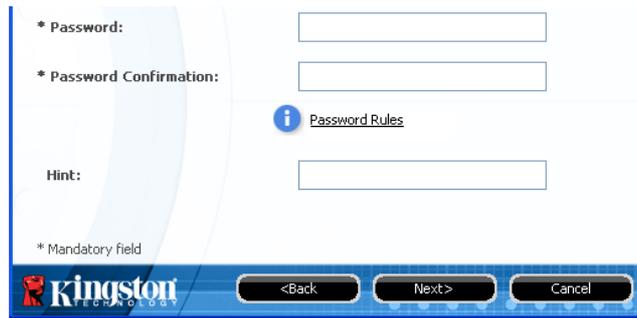


Click on the drive with the title “DTSP Launcher” and then on “DTSP_Launcher.exe” file contained within.

(Note: you may have to do this everytime you plug in the drive – it all depends on how your copy of Windows is set up. The “Autorun” feature allows new devices to be seen and connected and this may be disabled on your machine)

Tip: You may find that creating a shortcut to this file, on your Windows Desktop, enables you to locate this file a lot quicker.

The install process will then start. Follow all the on screen prompts until you get to the screen below.

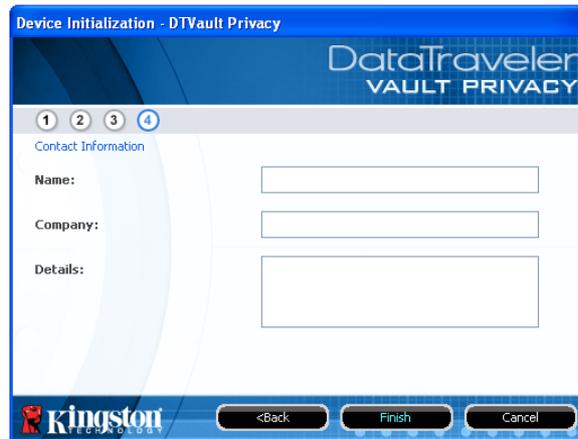


Password Choice

Choose a strong password and one not easily guessed. Should you require any direction on this, then please contact Information Security and we will be happy to assist you with advice on selecting a strong password.

Note: there is an option to type a password hint. Please try and be as deliberately ambiguous as you can, for instance – “The name of the street I live on” would be a bad choice, whereas “Where is H?” would be a great choice as H could stand for Home and only you would know that!

Continue to this screen:



Please fill in your name and put “Warwickshire County Council” in the “Company” field.

What next?

Please transfer any files from your old USB Pen Drive to the encrypted one you have just configured.

Important – If enter the wrong password in 10 times in a row, then the device will automatically wipe itself. You should never store information that you haven’t got a master copy of in your WCC Network folder and be sure to replace your information with your current copy on regular intervals.