



## Use of Flash Drives (Memory Sticks) Policy

### Arrangements for Review:

**Jim Duncan** is responsible for the implementation of this policy and conducting regular reviews. This policy was adopted in July 2010 and will be **reviewed in May 2011**.

## **Background**

Portable data holding devices such as flash drives are vulnerable to being lost if great care is not taken to ensure that they are kept safe and secure. Flash drives can hold any kind of electronic data some of which could be sensitive regarding individuals and Seashells or its partners. If a flash drive is lost or stolen there is a risk that such data could be accessed by unauthorised individuals. Under these circumstances we could be found to be breaching our common law and statutory duties to protect the confidentiality of such information.

## **Aim**

The aim of this policy is to safeguard data that may be stored on portable data devices to help ensure that we comply with our legal responsibilities.

## **Procedure**

With regard to all data belonging to Seashells:

- If data needs to be held on a flash drive then it must only be held on an encrypted, password protected device belonging to Seashells;
- Personal or any other flash drive not belonging to Seashells must not be used to store data;
- Staff needing to use a flash drive will be issued with one by Seashells;
- All staff issued with a flash drive must take all reasonable steps to ensure that the device is not lost or stolen and has a secure password;
- All staff issued with a flash drive must not reveal the password of the device to anyone not employed by Seashells and only to fellow employees where it is necessary and justifiable given the nature of the data and need for access to it;
- Any member of staff issued with a memory stick/flash drive must change the password on the device if they believe that someone else may have learnt the password and/or after it has been shared with another member of staff and their need to access that data has ceased;
- The password may be shared with the Data Controller\* or his delegate on an ongoing basis, for password retrieval purposes;
- Any member of staff leaving the employment of Seashells will be required to ensure that they return any memory stick/flash drive that they have been issued with.

This policy will be updated and reviewed in the light of changing legislation and circumstances.

\*At the time of the creation of this policy, the Data Controller is the Director of Seashells.

JD 2/5/10