Removable media such as memory sticks and cards, CDs, DVDs and other portable memory devices allow us to share and move information both inside and outside the SES Group, but they can easily be lost, stolen or damaged. We need safeguards in place to ensure sensitive and personal data is stored

Users should not put more information on removable media than they need to. Users can minimise risk by only storing the data they actually need on their removable media and deleting files as soon as they are finished with them.

Users should make sure they back-up anything put on removable media. Data held in only one place or one format is at much higher risk of being lost or corrupted than files that are regularly backed up.

If Users are transferring information from one computer or system to another via removable media, don't delete the original copy of the information from its original location until sure the data has been successfully saved to the new computer or system.

If Users need to share information with outside organisations or people, they should only use removable media if there isn't a more secure option available. Users must have the permission of the data owner to share the information, and must ensure the data and the removable media are stored securely.

Users should clearly label any data they store on removable media so that it is easy to identify the content and its version number or the date it was last updated. This will help ensure that they aren't using old versions of data.

Users should delete files stored on removable media once they have finished with them.

If Users are storing sensitive or personal data on removable media, they must ensure that it is encrypted so that it is protected if the device is lost or stolen.

Users should make sure the anti virus and malware checking software is working and up to date on any computers they plan to connect removable media to. If Users are transferring data from one computer to another, they must check the anti virus and malware checking software on both machines first.

Users must have permission from the Information Security Manager before using removable media to store, transfer, run or install any software or program.

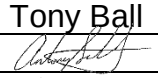
Users must securely store all removable media to ensure it is not lost, stolen or damaged. If Users are using removable media to transfer data, they must be able to show that they have taken reasonable care to avoid damage or loss when transporting the removable media. Users should keep a record of any data they put on removable media so that it can be traced.

Users should only transfer data which they are authorised to use to any removable media device.

Users should make sure data on removable media is stored and transported securely, in line with the type of data and its sensitivity.

If a User's removable media device is lost or stolen, they must report it as soon as possible to the Information Security Manager.

Any removable media device that is no longer needed should be securely destroyed.

Name:	Tony Ball
Signature:	
Date:	1st May 2017

1	AS	TB - MD	01/05/17	N/A First Issue
Revision	Prepared by	Approved by	Issue Date	Description of Modifications Made