Information Security Do's and Don'ts

- **Do not** disclose, discuss or share any confidential information which has been shared with you as a member of the LSCB with anyone outside of the LSCB without the express permission of the Independent Chair.
- **Do not** store LSCB confidential information on your personal computer, personal device or USB unless your equipment has been authorised by your employing organisation as a 'Bring Your Own Device'.
- **Do not** use personal email accounts i.e. Hotmail, Gmail, Yahoo to send or receive LSCB papers, unless it is sent or received via Egress Switch (the secure email encryption service provided by the Council).
- **Do not** share confidential information provided to you as a member of the LSCB via social media.
- **Do not** print any confidential reports or papers in relation to the LSCB. Keep all printing to an absolute minimum for security and environmental purposes.
- **Do not** leave confidential information provided to you by the LSCB unattended.
- **Do not** share your computer or email password with anyone or leave it written where others may see it.
- **Do not** open any email attachments or links from unknown or suspicious sources as they may contain a virus.
- LSCB members that do not have an LBR, NHS or Police email account should use Egress Switch (the secure email encryption service provided by the Council).
- Ensure that no one can view your computer screen/device when accessing LSCB reports at home or in an unsecure area.
- Ensure **ALL** (electronic and paper) LSCB confidential reports securely disposed (paper records should be shredded, electronic data must be permanently deleted).
- Ensure any LSCB or sensitive/confidential documents downloaded are securely deleted from your personal PC/device.
- Ensure you lock your PC/device when you are away from your desk
- Ensure you **promptly report** any loss, breach or unlawful disclosure of data to the LSCB Business Manager.

August 2017