Hints and tips for using a shared device safely

Do

- Ensure all the operating systems, anti-virus operating systems, software, and apps up-to-date.
- Ensure that all users agree to the Acceptable Use Policy for your project.
- Place the device in an area that allows for privacy.
- Ensure that when the device camera is in use, no other venue users are visible.
- Remind users not to save personal files to the device: use a memory stick or cloud account instead.
- Set all internet browsers to the most private and secure modes by default. Detailed information for most major web browsers can be found by clicking on this link.
- Educate users about staying safe online and remind them to log out of online accounts before ending their session.
- Remind users not to save personal information, such as website favourites or bookmarks, usernames and passwords, credit card information, or other personal information on the shared device.
- Ensure that pantry staff clear the browsing history, cookies and cache from the device in the presence of the user, at the end of each user session.
- Report any concerns you have regarding cybercrime.

Don't

- Allow unacceptable use to go unchallenged. Refer to your venue's acceptable use policy.
- Allow users to store any personal files on the hard drive or desktop of a shared device. Check that they have alternative means of saving their documents before they start their session.
- Help users to set up passwords, record passwords, enter payments or other sensitive information into online forms without considering and planning how you can do this to maintain confidentiality and privacy.
- Allow another user to help someone set up a password, record a password, enter payments or other sensitive information into online forms.
- Allow another user to log onto the device until the browsing history, cookies and cache have been cleared from the previous session.