

Privacy and Smart Technology

With the increasing number of smart devices being used in the homes of people we support, it is important to understand the potential implications for privacy.

Smart Technology includes smart speakers such as Amazon Echo and Google Home but also includes Smart TVs which are connected to the internet. These devices use advanced technology to help them work effectively but in order to do this they gather a lot of personal data about us.



****Smart Technology isn't always recording but it is always listening and inadvertent recordings can be made when the devices are accidentally activated****

The following precautions are advised:

Ensure any private and confidential discussions are held in rooms where there is no smart technology in use.

Mute the microphone of any smart speakers when there is potentially sensitive information being discussed.

Review the privacy settings of any devices regularly to ensure you are aware of what information is being collected, stored and shared. This can be done via the app or logging into the account via the amazon website.

Clear any data stored on a regular basis to reduce the amount of personal data being held about an individual by the device manufacturer.

Enable audible tones on smart speakers so you are alerted when they have been activated and can monitor whether this is being done accidentally.

Be aware of features such as 'drop in' on Echo devices which can allow devices to act as two way radios and be set to automatically answer. Either disable this feature or ensure it requires a voice command to answer the call.

Some devices also now have built in cameras. It is important you are aware that the camera is there and that appropriate settings are used to control access. On some devices the shutter can be manually closed and this is best practice to ensure privacy when not in use.



GDPR

Amazon collect the voice data from the recordings they store to improve the technology for future use, this data is anonymous and only a small fraction is accessed or used. Storing a person's voice data also helps the smart speaker learn the users speech patterns so that it can understand what they say more easily which can improve ease of use. Consideration needs to be given as to whether the storage of this data is an issue for the user and if so can be disabled in the account settings, however, this will affect future use and may not be in the persons best interests.

Access to the app or account should also be limited to key people as they can access the history of use for device, including what commands the device has heard.

Top Tips:

You can clear the recent search history of smart speakers either within the app or by giving a specific voice command once this feature is enabled within the device settings.

On Amazon Alexa devices, say:

"Alexa, delete what I just said" or "Alexa, delete everything I said today"

On Google Home devices, say:

"OK Google, delete my last conversation" or "Alexa, delete everything I said this week"

You can clear all of your recordings at any time within the app:

On the Amazon Alexa app go to the menu then **Alexa Privacy > Review Voice History**.

On the Amazon website go to **Your Account > Content and Devices > Privacy Settings**

In the Google App on an iPhone or iPad, click your image icon and follow this path: **Manage your Google Account > Personal info & privacy > My Activity**

You can also find this by going to Google.com and following the same process.

You can also set devices to automatically clear your search history at set intervals e.g. every 3 months. This can be done within the app or on the website.

Other useful documents:

H&S 080i Security Risk Assessment