Disclaimer on use of own equipment to make recordings during interviews:

Students participating in research projects in which interviews take place may record these interviews if participants have given their consent. This is on the condition that they take appropriate technical security measures to ensure the privacy and security of the recorded data. These measures include:

Strong Security of Devices: Students should use devices equipped with robust security mechanisms. This includes the use of PIN codes or biometric authentication as described in UU's Security Control Framework (IS.9.003. PIN and biometrics).

PIN codes: According to the guidelines, a PIN code should consist of at least 5 characters and should be numeric only. PIN codes are specific to the device and, where possible, also specific to the user.

Biometric Authentication: Biometrics can be used as an optional usability feature instead of a PIN, provided it is processed on the device itself. The use of biometric information is always optional, and there should be no central processing of biometric information. Biometric authentication is also subject to speed limitations.

Data encryption: Devices must encrypt the data collected. On iOS devices, for example, this is standard. Encryption ensures that data cannot be accessed without the correct encryption key, helping to secure sensitive information.

If students do not have access to devices that meet these security requirements, FSW Tech Support offers the possibility of borrowing iPod Touch devices. These devices are equipped with the necessary biometric security and encryption capabilities to meet the required security requirements.