Guidelines for secure handling of confidential information from KLARA

(From Security and Safety Division)

When information is exported/retrieved from KLARA for purposes of handling it in paper form, on a USB stick or other external media, the following regulations, based on Uppsala University's procedures for secure information management (UFV 2018/668), must be followed:

- When storing information on a USB flash drive, the information should be stored in encrypted form.
- Non-digital information must also be provided protection that corresponds to the sensitivity of the information. Written material generated from KLARA and which contains confidential information must not be available so that unauthorized persons can access it. The material must be handled so that unauthorized persons cannot gain access to it. Apply the "Clear desk" principle - sensitive material should not be left accessible.
- It is essential to ensure that any sensitive documents taken outside the office environment are handled with adequate care.
- When sending/transmitting confidential Information retrieved from KLARA digitally (e.g. by email), the information must be encrypted before it is sent internally or externally.

Links to instructions for two methods for sending encrypted e-mails.:

Email encryption with S/MIME (nanolearning.com)

Sending sensitive information as an encrypted attachment (nanolearning.com)

Link to instructions for encryoting USB memory sticks:
https://www.groovypost.com/howto/encrypt-flash-drive-sd-card-windows-10-bitlocker/