**Security measures when processing personal data in student projects**

* The most fundamental security measure is never to collect more data than necessary.
* The project/essay should preferably be completed using entirely anonymous data.
* Ensure that any survey tools fulfil requirements. Sunet Survey or Microsoft Forms (via Microsoft 365) are recommended.
* You must use the computers in the university’s ICT suites (in the library) or borrow a laptop from the Infocenter.
* Cloud services that are not provided by Södertörn University may not be used when processing personal data. This includes storage services such as Dropbox, Google docs, iCloud, etc.
* Sensitive personal data must never be stored on your personal computer, unencrypted USB stick telephone or tablet.
* You must keep an eye on any printouts or similar material, and lock or log out of the computer when taking a break.
* You may be able to process pseudonymised data on private equipment. Pseudonymised data is when an identity marker, such as a name or personal ID number, is replaced with a pseudonym that cannot easily be linked to that person. The pseudonym can be linked to the person via extra information, such as a list of names and pseudonyms that is stored separately. A precondition for processing pseudonymised data is that the data cannot be directly or indirectly traced to individuals without using this key and that the key is stored separately and securely with your supervisor.
* Pseudonymised personal data is not the same as anonymised data. It is still legally the same as personal data, but the security is considerably better because only the person who needs to make the connection has access to the key.
* Authorisation – the supervisor must ensure that there is documentation showing who is authorised to access the data that has been collected.