# Usage and Confidentiality Commitment for Data and Information Systems

Read the text thoroughly and completely before signing it.

Confidentiality and the usage of data and information systems are based on legislation and norm control. All data must always be processed carefully and in accordance with good governance.

Confidentiality means the confidentiality of information, irrespective of its means, and professional secrecy, i.e. the prohibition to disclose information to outsiders and the prohibition to use confidential information for one’s own or another’s benefit or to the detriment of another.

Seeking confidential information for non-work-related purposes or deliberate actions contrary to instructions are strictly forbidden and punishable as such. The unauthorised use of data may result in criminal, labour, and compensatory sanctions (e.g. a reprimand, warning, termination of employment/office, fine, imprisonment).

Confidentiality applies to me both during and after my employment or contractor relationship. The obligation of secrecy also applies to students and other staff who process the organisation’s confidential information.

## Commitment

* I shall only process information required for my work tasks. I shall not process information pertaining to me, my colleagues, my close relatives, or celebrities, unless my work tasks so require.
* In this context, information shall mean confidential information (e.g. customer and patient data or trade secrets) or other protected personal data.
* Processing shall mean e.g. the viewing, recording, usage, transfer, disclosure, retention, modification, merging, or removal of data.
* I shall not disclose confidential information to outsiders without proper authorisation or legal basis. Outsiders are used to mean persons whose tasks do not include the processing of the matter.
* I am aware that visits to information systems and actions carried out in them are recorded in logs, that usage is monitored, and that suspected misuses are reported to my supervisor.
* I shall adhere to binding provisions and instructions connected to the usage of data and information systems. These instructions and laws can be found in the Wellbeing Services County of Ostrobothnia’s intra in Services and Support >> Security >> Data Protection.
* I shall use the organisation’s information systems and devices only for work tasks, unless otherwise agreed upon with my employer.
* I shall answer for computers and other devices in my possession and ensure that the devices and information contained in them do not fall into the wrong hands. I shall remember to lock my office door or cabinet where I keep my laptop / confidential documents.
* I shall log out of information systems or lock my computer when it is not under my supervision (to easily lock the computer, press CTRL+ALT+DEL).
* I shall change my Windows or domain name as well as passwords and codes to information systems and device usernames in accordance with instructions. I shall store personal passwords and access codes carefully to protect them from outsiders.
* I shall answer for all actions (information systems, mobile devices, access control etc.) taken with my access codes, key cards, and codes.
* I shall adhere to binding instructions and regulations given for the use of electronic communication devices (e.g. email, calendars, instant messages, and smartphone). I shall not send e.g. confidential information via unprotected email.
* I shall not install, remove, or copy programs without permission.
* I shall dispose of unnecessary data and other protected materials appropriately / in accordance with instructions into e.g. confidential waste containers. If necessary, I shall ask for more information from my supervisor, an information service specialist, or a data protection officer.
* I shall not print out confidential information with an unmonitored printer. When using a network printer, I shall ensure its location and monitoring before printing out documents and use secure printing or a printing code, if one is available.
* I shall not store or transfer confidential information onto my home devices or unprotected on a memory stick or other unprotected devices.
* When working remotely, I shall ensure that outsiders, such as my family members, cannot see, hear, or use my remote devices or connections.
* I shall confirm with my supervisor that I receive sufficient training for the use of necessary information systems.
* I shall not request unnecessary access rights, and I shall notify of any remaining unnecessary or incorrect information system access rights so that they can be changed or removed. Unnecessary access rights may strain systems and increase costs and other risks, as well as weaken the user’s legal protection in the investigation of misuses.
* I shall notify appropriate persons in the organisation of any perceived misuses of data security, data protection, or information systems.
* If I function as a supervisor, I shall tackle the misuse of data, information systems, data security, and data protection.

I have read this Commitment. If I am unclear about the contents or meaning of the Commitment, I shall turn to my supervisor as soon as possible. Compliance with given instructions and regulations ensures the legal protection of all employees.

Signing this Usage and Confidentiality Commitment is a prerequisite for the use of data and information systems, and this version shall replace any possible previously signed versions.

I shall undertake to comply with the contents of this Commitment and to act accordingly.

\_\_\_\_/\_\_\_\_20\_\_\_

Signature, name in block letters, and personal identity code of the person accepting the Commitment

Supervisor’s signature and name in block letters