IT GOVERNANCE

2024-06-05 Dnr C2022/916

Rules for employees' use of personal digital equipment

Purpose

The purpose of the rules is to determine how personal digital equipment may be used by employees at Karlstad University and what responsibility employees have for the personal digital equipment.

Document

- Rules for employees' use of personal digital devices at Karlstad University

Documentation

Date	Change
2023-05-10	First release. Produced by the IT governance and legal functions at the Department of Executive Support. The document replaces C2013/258 regarding the disposal of IT equipment.
2023-10-31	Adjustments following internal referral and responses from the faculties, the Office of Teacher Education, the IT Department, the Campus Department, the Department of Educational Administration, the Department of Communications and the Information Management Council.
2024-02-07	Adjustment in the chapter Controlls, after discussions with university management.
2024-06-05	Adjustment in the chapter Controlls. *Checks [...] may only take place in case of serious suspicion of criminal behavior ...*

Decision	RB 115/23	Dnr.	C2022/916	Replaces	C2013/258
Valid from	2024-12-26	until	until further notice	Administrator	Claes Asker

Rules for employees' use of personal digital equipment

Karlstad University provides its employees with digital equipment, such as computers, tablets and mobile phones, so that the employees can carry out their duties and so that they can access essential information relevant to their work.

The purpose of these rules is to describe the employee's responsibility for their digital equipment.

Personal Digital Equipment

For a couple of decades, computers have been the given digital tool for carrying out work tasks and for accessing essential information relevant to the work. Almost all personal computers today are portable, only a few exceptions exist. In other words, the computer is often not in the employee's office location, but is used elsewhere or is on the move.

For a few years now, mobile phones have also become a natural work tool for many employees. For some, the only digital equipment they have. In the autumn of 2022, desktop and cordless telephones were phased out and mobile phones were offered to all employees.

Personal digital equipment mainly refers to the computers, tablets and mobile phones provided to the employee, which the employee uses daily for his or her work activities and which are owned by Karlstad University.

Other digital equipment that the University provides the employee with, such as cameras, USB sticks and smart watches, are also covered by these rules as applicable.

Use

The employee has both rights and obligations regarding the personal digital equipment. A large responsibility rests on the employee to handle the personal digital equipment in a correct manner.

The personal digital device is to be used for the employee to perform his or her duties. It is permissible to use the digital equipment for private use as long it does not significantly deteriorate the equipment, do not result in increased costs for the employer or that it affects the performance of the work. The equipment may only be used by employees at Karlstad University. The use of personal digital equipment in side-line occupations is regulated in the *Policy for side-line occupations (C2022/897)*.

No private costs arising from the use of the personal digital equipment may be charged to Karlstad University. This includes, among other things, the purchase of software, subscriptions and communication costs (e.g. private international calls).

Information produced in the course of work with the help of the personal digital equipment (documents, images, sound recordings, etc.) must be saved or processed on the personal digital equipment or transferred to the other digital equipment or digital services provided by, or through, the university.

The employee has a responsibility to manage the personal digital equipment in a secure manner. This includes protecting the equipment to minimize the risk of physical damage and to prevent theft. The employee should also follow security advice to avoid cyber threats and digital intrusions into the equipment. Access to the

equipment must not be given to unauthorized persons. Information worthy of protection may not be found on digital equipment without adequate protection. In case of doubt, the employee must consult an information security officer when it comes to information worthy of protection and an IT security offices when it comes to adequate technical protection.

In the event of loss of digital equipment or suspicion of digital intrusion, the employee must immediately contact the university's IT support (e-mail to 2525@kau.se, telephone to +46 54 700 25 25 or visit to the reception for IT support).

Purchase and return

After approval from responsible manager, new personal digital equipment must be ordered by the employee through the university's IT support. When a new employee is hired, the responsible manager must ensure that the new employee receives personal digital equipment. It is the employee's needs linked to work activities that govern the choice of equipment and which subscriptions (e.g. data traffic) are relevant. It is the responsible manager who decides on the purchase. To support the employee and the manager, options to digital equipment is be published on the university's intranet.

In order to verify that the employee has received the personal digital device, and has been informed on his or her responsibilities under these rules, the employee must acknowledge this upon delivery. When returning personal digital equipment, the employee must acknowledge the return. A register for acknowledgement is handled by the university's IT support.

Upon termination of employment, the employee must return the personal digital equipment no later than one month after the last day of employment or earlier if the employer requires it. The same applies to leaves of absence of more than six months. It is possible to make exceptions for those who are on parental leave or on sick leave to have access to the personal digital equipment. It is also possible to make exceptions for associated researchers who participate in active research projects at the university. All exceptions must be decided by the responsible manager.

There are times when an employee may need to take over another employee's personal digital equipment. An example of this is when a substitute goes in for an employee who is on parental leave. In such cases, the transfer must be registered in the IT support's acknowledgement register.

Prior to the return of the personal digital equipment, the manager is responsible for ensuring that information on the equipment is preserved. After return, the IT support must ensure that information on the equipment is deleted before it is reused, scrapped or returned to the rental company. Subscriptions that the employee had are terminated by the IT support or reused in the organization.

Safety

As digital equipment is exposed to both physical threats (e.g. theft) and cyber threats (e.g. hacking or ransomware), security of the university's digital equipment is of essential importance. All established safety rules[1] must always be followed by the

[1] All policy documents regarding information security, IT security and physical security are published on the university's intranet.

employee as a lack of security can have serious consequences for the university's operations.

Software (apps) and services that the university deems unsafe may not be installed or used on the personal digital equipment.

When the employee processes sensitive personal data or stores confidential information on the personal digital equipment, guidance is provided in *Rules of procedure for the processing of information in systems and services (C2019/1022),* which is published on the university's intranet. If the supervision does not provide guidance, the processing must be preceded by a risk analysis in accordance with the applicable policies for information security.

Security updates of the operating system and software on the personal digital device shall be made by the employee as soon as possible. If an update is urgent and necessary for security, the university can carry out such an update without the employee's involvement.

The employee is responsible for ensuring that the personal digital device is protected by a password, passcode or biometric protection method (fingerprints, facial recognition, etc.) in accordance with the policy documents for *Digital Identity (C2014/59).*

All personal digital equipment assigned to the employee must be centrally managed. This means that the personal digital equipment is registered in and connected to a university-wide management server. One purpose of this is to be able to trace and delete equipment that for some reason has gone astray and thus prevent the university's information from falling into the wrong hands. Another purpose is to be able to keep track of which licensed software is on each employee's equipment and to be able to follow up if unsafe software and services are used.

For backup and recovery of the personal digital equipment, the employee must use services or products provided or approved by the university. As a rule, this is already installed and configured at the time of handing over the personal digital equipment. Current services or products are published on the university's intranet by the system group owner[2].

Controls

In some cases, the university may need to carry out controls on the content of the employee's personal digital equipment. Controls involving access to an employee's private information contained in the personal digital device may only take place in case of serious suspicion of criminal behavior or that the personal digital device has been used in violation of these rules. Moreover, such a review must be both necessary and proportionate to the objective pursued. A careful assessment is always made in each individual case. The HR Director decides whether such a check should take place, after consultation with the Legal Support.

[2] The system group owner refers to the role in the system management model that is responsible for the group “IT workplace”.