**CODE OF CONDUCT**
**PUUMERKKI GROUP**
**Information and communication technology**

**ICT (Information and communication technology)**

**19th of May 2025**

# CODE OF CONDUCT

The ICT administration referred to in this code of conduct means the ICT Director and/or the ICT Manager.

## Information security instructions

At Puumerkki, each employee is responsible for ensuring information security. The overall safety of the company is based on the responsible actions of each member of its staff.

Follow the information security instructions and exercise due care in matters related to information security. Even though people tend to link information security strongly with ICT, it covers all areas of data processing: printouts, copies, archiving, pricelists, oral communication, etc. Information security is about maintaining the availability, confidentiality, and integrity of information. When you recognize risk situations, you will be able to act correctly. As the popularity of remote work increases, each member of staff should also take account of the special characteristics of remote and mobile work, in addition to general instructions.

### Workstation and mobile information security

- Do not allow outsiders to peek over your shoulder or see your screen when processing sensitive information or entering usernames and passwords.
- Always sign out of your workstation when you leave it unattended or when you stop working; also close all applications and switch the workstation off. This ensures the integrity of your workstation.
- Determine the origin of information and files before use. Do not connect storage devices (memory sticks, external hard discs, or other USB devices) to your computer if you are not certain of their content.
- Never open attachments whose source is unknown. Messages sent from an unknown source can contain viruses.
- Exercise due care when dealing with uploaded files. Do not install or try to install programmes on the computers. IT support is responsible for completing all installations.
- Only visit websites that you trust to be safe.
- Store all storage devices that you use in a safe place. Save your work during long work phases, either manually or by using the automatic saving option of the application. Do not leave incomplete work open on the screen unattended.
- If it is not necessary to share your files and/or folders, do not share them.

- Ensure the physical security of your computer – do not leave it visible on the back seat of your car, for example, and ensure that you are always aware of the location of your equipment!

- Do not panic or act hastily if you notice signs of an information security problem. You can always contact the IT support in matters/problems related to information security.

## Special characteristics of remote work and related information security instructions

If you are using an external network (e.g., in a hotel, at the airport, or on a train), always use a VPN connection or share the connection from your own mobile device.

In a public place, always use a privacy filter on your screen.

If you participate in a remote conference in a public place, take account of your surroundings and any persons who can see and hear you.

The workstation must also be locked at home and at a summer cabin when left unattended.

Personal usernames and passwords provided to you by the company must not be used on public workstations or equipment. For example, do not sign in on a public computer at a library by using your company credentials.

## Usernames and passwords

Usernames and passwords are always personal. Never allow another person, not even another member of the company's staff, use your credentials or a system activated by using them.

Choose a secure password (sufficiently long and containing letters, numbers, and special characters). The best type of password is a made-up string of characters (for example, an abbreviation of a sentence that you will remember, such as "4Le4i4ct4est" from "alea iacta est"). Do not use this example as a password!

Use a different password in each system.

Enter your password only on a computer that you trust or whose owner you trust. The applications that you use on the computer can save your password on the computer without your knowledge and someone else may be able to retrieve it later.

Additionally, it is possible to use Windows biometric authentication:

**Windows Hello login (PIN, fingerprint, facial recognition)**
Windows Hello login is allowed on supported devices to enhance security and user experience. The login is based on a biometric model stored in the device's TPM chip, which is not transmitted over the network.

**Terms of Use:**
• Windows Hello must be enabled together with a PIN code.
• Users are provided with the option to use a PIN code as an alternative to biometric authentication.
• The use of biometric login is voluntary.
**Administration and Monitoring:**
• Windows Hello settings are managed centrally (e.g., via Intune or GPO).
• Device compatibility and security requirements must be verified before deployment.

### The use of telecommunication networks

The company network can be used via a wireless local area network, VPN, or communications port. The personal credentials granted to the user that are used to sign in onto the computer are also used to establish a VPN and wireless LAN connection. When a communications port is used, the user is identified automatically.
Only devices conveyed to the user by the company must be connected to the company network. For example, you must not connect your personal mobile phone to the company's wireless network, but you must use the guest network.

A wireless local area network, which is not connected to the company's telecommunication systems, is available for guests at the office. There are separate credentials for the use of the guest network, which can be conveyed to visitors for the duration of their visit.

### Printing and the surrounding area

Printouts, copies, and scanned documents must be retrieved from the device immediately. Security bins, one of which is found in each office, are used for the secure destruction of documents.

Multifunction devices are intended for work-related printing. The use of the devices for personal matters is forbidden.

### Shared devices

The company has in use shared devices related to working, such as forklift terminals, mobile phones, radio phones, and workstations. Special care must be exercised by the ICT administration and the users when these are used. The said devices must only be used to perform work tasks. The ICT administration monitors these devices in order to ensure their appropriate use.

## Lifecycle management of the equipment and software

The ICT administration is responsible for the standard tools used by the staff and for their procurement, and selects the device models so that they are suited to normal work use. **All equipment is procured through IT support.**

The standard personal equipment of each member of the staff includes, based on their job description: a laptop, a mouse, and a headset. A docking station, keyboards, and monitors are

provided by the Employer at the Employee's primary designated workstation. The number of monitors is determined based on the job role, with a maximum of three monitors per user. One user cannot have more than one work computer.

Mobile phones and tablet computers: the supported operating systems are Android and iOS. Devices are equipped with a protective case and tempered glass screen protector. Additional accessories are provided based on the job role, such as a travel charger and a hands-free headset if needed. Phone models are standardized.

The minimum lifecycle of devices: laptops 48-60 months and mobile phones 24-36 months.
In telephone subscriptions, the blocking of foreign data traffic (non-EU) and a €50 balance limit are a default. Telephone bills that exceed €50 will be processed with the supervisor and telephone bills that exceed €150 will be reported to the ICT Director and the supervisor. Each user can only have one telephone subscription on behalf of the company. Outside the wireless network, the network should, principally, be shared from one's own mobile phone. If required by the job description, a separate data connection can be acquired subject to a supervisor's recommendation and approval of the ICT administration.

The more detailed instructions related to mobile phones and subscriptions are provided in a separate Annex and the valid instructions can be found at: Intranet: staff – instructions on mobile phones and subscriptions.

## Replacement and removal from use of devices

Work devices can be replaced when their expected lifecycle ends. If a work device is to be replaced before their expected lifecycle ends, this must be discussed with the ICT administration.

If the user breaks his or her work device, the user is responsible for compensating any remaining residual value. The supervisor can, however, make a decision to replace the device, taking account of the "negligence" aspect in his or her decision.

Used devices and devices that are to be removed from use must always be reported immediately to the ICT administration by email so that they can be removed from the company's systems in a controlled manner and destroyed physically in a secure manner.

Workers are responsible for returning their old devices to Kerava in connection to a replacement. This applies to mobile phones, workstations, and storage media (hard drives, memory sticks, and memory cards).

When the employment ends:

- The supervisor fills in an end of employment report on the HR page in the Intranet.
- The ICT administration closes any user accounts under its control, as well as telephone and data communication subscriptions in accordance with the valid contract model.
- The supervisor is responsible for returning the devices of his or her employees to Kerava when the employee's employment ends.

Workstations, telephones, storage media, and other similar devices are restored in a secure manner and redistributed or destroyed in an appropriate manner by the ICT administration.

### Software

The company offers its employees software required by their job description. The core of the standard software is formed by ERP systems, MS O365 software package (Outlook, Excel, PowerPoint, Word, Teams, Power BI apps, Forms, OneDrive, OneNote, Yammer, SharePoint). If the job description of the employee requires the use of some other applications than those listed in the above, his or her supervisor will submit a procurement request to the ICT administration for approval.

The ICT administration is responsible for ensuring that the applications are up-to-date and secure.

Services provided by partners and related applications (M2, Exflow, Sympa, Atlantis, Kuljetus Velho) will be installed on users' devices based on the need.

### General equipment procurements

General equipment procurements are temporary procurements that strengthen the structures and are needed quickly. These are always implemented based on the need and commissioned by the ICT administration.

### Other safety and security systems

The company has in use access, working time, and CCTV systems, fire and burglar alarm systems, and building automation systems. These systems can involve staff obligations.

Controls, usernames and passwords related to these systems and provided to the employees are always personal. Control panels, usernames and passwords must be stored so that they cannot be used by others.

## Operating environments

The ICT administration maintains up-to-date architectural descriptions of the environments.

### Online infrastructure

Consists of network assets, servers, data communication connections, and related auxiliary equipment. The ICT administration is responsible for maintaining, updating, and monitoring that these are kept up to date and for ensuring that the entity remains functional and is protected. Online infrastructure is updated based on the company's business goals.

### System infrastructure

The ICT administration is responsible for ensuring the integrity and reliability of the company's information as regards the existing systems and for supporting the staff in using them correctly. The structure of the company's system infrastructure will be implemented as cost-efficiently as possible, whilst observing synergy benefits, based on the business goals of the company.

### User right policies

The access and user right policies of different systems guide information security based on the job description, whilst also observing the needs of the employees.

## Consequences of the misuse of IT services

An IT breach means an activity that violates the instructions and regulations provided on the use of the company's IT systems or the use of the IT systems in a manner that is against the Finnish law.

This code of conduct describes the measures that can be imposed on a person who has or is suspected of having committed an IT breach. The measures have been divided into user rights restrictions, imposed for the duration of the investigation of the breach, and into the possible consequences of the breach.

The company can restrict the user's right to use IT services during the investigation. These restrictions are decided upon once the IT breach has been observed or is suspected. User rights are always restricted when there is a justified reason to suspect that the user has committed a misuse, and it is possible that maintaining the user rights can have a negative impact on the investigation of the breach or on the minimisation of the damage. An opportunity is reserved for the user to be heard, and, in more severe cases, the user will be summoned to be heard.

The ICT administration will make the decision on the restriction of user rights. The administrator of the service will implement the restrictions.

In urgent cases, the administrator can restrict user rights subject to his or her own decision for the maximum of three days; the ICT administration must be informed of such cases immediately.

Where required, the user's workstation can be disconnected from the network.

Restrictions will be removed once the investigation has been completed, unless the restoration of user rights would clearly be detrimental.

### Consequences

In minor cases, the inappropriate actions will be pointed out to the user.

If the user has committed an IT breach, the user might be liable to pay compensation for the resources (e.g., servers or data network) that he or she has misused, for any direct damage, and for the expenses related to the investigation of the misuse.

## Consequences to the employee

As regards the staff, the possible consequences include measures enabled by labour legislation (a written warning or termination of employment, either with or without notice) and reporting the offence to the police (actions specified in the law as being punishable).

User rights to individual systems can be denied for a fixed period or permanently due to a lack of trust caused by misuse. The ICT administration will make decisions on actions related to user rights.

## Consequences to other users

As regards external users of the company (interfaces with partners, clients, and suppliers), the possible consequences include, for example, the removal or restriction of user rights and reporting the offence to the police (actions specified in the law as being punishable).

User rights to individual systems can be denied for a fixed period of time or permanently due to a lack of trust caused by misuse. The ICT administration will make decisions on actions related to user rights.

## Examples of the misuse of IT services

- Unauthorised use of material that falls within the scope of the Criminal Code of Finland or the Copyright Act.
- Material that falls within the scope of the Criminal Code of Finland includes child porn, bestiality, brutal violence, racist material, and material that aims to incite the public; the use of the material includes, for example, its spreading and possession.
- Material that falls within the scope of the Copyright Act includes, for example, music, videos, cartoons, movies, games, and software.
- The conveyance of credentials means, for example, revealing your password to another user and leaving your computer turned on so that another person is able to use your credentials.
- Endangering the confidentiality of information includes, for example: conveying information that is confidential or otherwise protected by law to a third party that has no right to access the said information (e.g., conveyance of server user information), neglecting the information security of confidential information (passive lack of action), intentional confidentiality offences (active action), and breaching of the Personal Data Act.
- Neglecting personal information security includes, for example: leaving your password visible and neglecting the backup practices of the company.

**CODE OF CONDUCT**
**PUUMERKKI GROUP**
**Information and communication technology**

**ICT (Information and communication technology)**

**19th of May 2025**

The following will be reported to the administrative board of Puumerkki twice a year:

- Deviations from the scope of the procurement
- Procurements made before the end of the lifecycle
- Breakdowns of devices
- All misuse cases without exceptions