

The employer should have guidelines regarding the use of the Internet and e-mail. How extensive and detailed these guidelines should be depends to a certain degree on the kind of work carried out at the specific workplace. An employer with thousands of employees may feel the need to have more detailed regulations than a small business, where everybody knows one another. A public authority must take into consideration that the personal data could be comprised by the principle of public access to official documents. Thus, an employer may consider himself to be in need of more regulations than those stated below as examples by the Data Inspection Board. In this check list the Data Inspection Board briefly highlights the regulations that are important enough that they must always be included in the employer's guidelines concerning the use of the Internet and e-mail. Each point is followed by an example and a comment where the Data Inspection Board clarifies what an employer should bear in mind when working out the guidelines.

## **Examples**

### **Use of the Internet and e-mail that is allowed**

It should be made clear by the employer's regulations to what extent the employee has the right to use the Internet and e-mail for private purposes.

**Example:** The Internet is a work tool and may only be used for private purposes in a way that it does not intrude on the work or lead to unnecessary costs for the employer.

**Comment:** Within the scope of this project it has become evident that most employers allow that the employees surf on inoffensive websites for private purposes, for example on their lunch or coffee breaks. Fundamentally the employees are always allowed to send short e-mail messages for private purposes as long as it does not intrude on their work. In this context, it should be pointed out that the guidelines of the employer must be of a serious kind. In the guidelines the employer ought not to prohibit all kinds of use of the Internet and e-mail for private purposes at the same time as the employer in practice is given that right.

### **Restrictions regarding the use of the Internet and e-mail**

If an employer wants to restrict the employees' use of the Internet and e-mail, this should be made clear by the guidelines and information provided.

**Example:** Surfing on websites with extreme political or pornographic content (for private purposes) is not allowed. Nor is it allowed to participate in chat rooms or download files from the Internet.

Sending chain letters is not allowed. It is only allowed to subscribe to mailing lists if the information of the lists is needed for the work.

**Comment:** The restrictions should as far as possible be expressed clearly and distinctly. It is not sufficient to refer to "implicit ethical regulations" or to prohibit access to "information that might be considered inappropriate from an ethical point of view" etc. The restrictions may specify which websites the employees are allowed to visit or what information the employees are allowed to spread on their own. Further, it is not unusual to impose restrictions in the interests of security, for example, in order to avoid virus infections or unnecessary straining of the net.

From the regulations that the Data Inspection Board has studied, it is evident that many employers want to prevent employees surfing on websites which express extreme political opinions, such as racism or terrorism, and on those containing pornographic material. The restrictions may also include downloading of music or films, purchasing/paying on the Internet, checking e-mails from a private e-mail box, participating in chat rooms etc. The extension of these restrictions is a question that should be dealt with at each specific workplace.

## **Monitoring the use of the Internet and e-mail**

If the employer carries out some kind of checks concerning the employees' use of the Internet and e-mail, this must be clearly evident from regulations and information provided. It should also be made clear how the check is carried out.

**Example:** All Internet use is registered in a log file. The log file includes information such as user names and the name of the website that has been visited.

A log file detailing all the e-mail messages, containing information such as the sender, receiver, subject, time and size of the message, as well as the name of the attached files is also being kept.

With the help of the log file, the IT-department presents a list each month that shows how many hours in total the employees have been surfing on the Internet. At this monthly control there is no check regarding the surfing of each individual. The accessible websites are divided into different categories such as sports, news, pornography etc.

If the control list shows that surfing on unauthorized websites has occurred, according to the guidelines, or if surfing on certain permitted websites occurs to an unusual large extent, the personnel manager can decide to initiate a check regarding the surfing of specific individuals.

The employer does not carry out any kind of check regarding the employees' e-mail messages. Nevertheless, in specific cases, the employer may control the e-mails if it is necessary for information security reasons, such as virus infections, or in order to investigate a suspected legal offence. The decision concerning the check is made by the IT-security manager.

**Comment:** Monitoring of the Internet could be carried out regularly (as in the example), by spot checks or for a specific reason. If a check is carried out for a specific reason or if a general check under certain circumstances leads to a check of an individual, it is important that the reason for which the employer has decided to check up on the employee is made absolutely clear. For example the check may be initiated if the log file indicates that an unusual high proportion of non-work related surfing or surfing on certain prohibited websites has occurred. It must also be made clear who decides that a check is to be carried out, for example, the personnel manager (as in the example) or the IT-manager or a specific group of officials.

## **Checking the contents of private e-mails**

If the employer might go through the contents of the employee's private e-mail messages, this must be made clear by regulations and information provided.

**Example:** The employer might study the contents of an e-mail message if it necessary in order to fulfil the duties of the public authority regarding public access to official documents.

The employer might also study the contents of an e-mail message if it is necessary for information security reasons, such as virus infections or hacker attacks, or in order to investigate or prevent a legal offence.

**Comment:** It is unusual that employers check the contents of the employees' e-mails. However, it does occur in connection with criminal investigations or for security reasons. This must be evident from the information. It may also be appropriate to mention what will happen with the employees' e-mail messages in the case of resignation or protracted illness.

## **Violation of the regulations**

It should be made clear in the guidelines what kind of measures that will be taken by the employer if the employee violates the Internet-policy.

**Example:** If the checks show that the guidelines have been broken, the case may be investigated by the personnel manager. In the first instance the employer will try to solve the problem by speaking with the employee. In the case of a more serious abuse, disciplinary measures may be taken.

**Comment:** It should be made clear by the guidelines who will be the person in charge of a possible investigation. It should also be stated what kind of measures the employer might take against the employee if he or she fails to comply with the guidelines.

## **Storing and deleting of data**

It should be made clear by the guidelines for how long the employer keeps the data that is the basis of the checks of the employee's use of the Internet and e-mail.

**Example:** The data that is the basis of the check of the employee's use of the Internet and e-mail is deleted after three months. If an investigation is initiated the data will be kept as long as the investigation is ongoing.

**Comment:** An employer is obliged to make sure that personal data is not kept longer than what is necessary, considering the purpose of the processing of the data. In the example in question, the employer presents a list with statistics of the employees' surfing on the Internet once a month. This list should then be gone over by the IT-department and in the case of suspected prohibited surfing, be handed over to the personnel manager for further measures to be taken. If the check is carried out in this way it should not be necessary to keep the data for longer than a maximum of three months. If an investigation concerning an individual's surfing is in fact initiated, it may be necessary to keep the data for as long as the investigation is ongoing, even if this means for a period longer than three months.

If the employer is monitoring the employees' use of e-mail, there should be a similar regulation regarding deleting the data that is the basis of the control of the use of e-mail.