maastricht university
employment agency

User regulations regarding computer and network usage.

The user regulations mentioned apply to all facilities made available. They apply to every person employed at the workplace, or using the facilities, regardless of whether or not they are present at the workplace.

Careful use

Please use the computer with care, this is not your property. Do not install any software without discussing this with the ICT-administrator. Do not save large amounts of personal data on the company computer (photo's, movies, music). Do not use illegal software. Log off, or lock your screen when leaving your workplace by using WIN+L. Save documents in a logical fashion: name and location has to make sense to others (for instance in case of substitution during illness). Change your password regularly (at least twice every year) and use different passwords privately and at work.

Means of use

Be careful when handling data. Make sure you have the correct address of the correct person in the "to" field when sending an e-mail. Be aware when using privacy sensitive data and be aware of the proper handling of such data. Do not simply provide third parties with sensitive information. When using e-mail on your phone or tablet, use a password or pin code and make sure the device will be put in stand-by mode when the device is not used for a couple of minutes, meaning that a password/pin code has to be entered when continuing the use.

Do's and don'ts

When working somewhere else, log on to the electronic work environment. This way, data never 'leaves the workplace'. Never take (sensitive) data with you on an unsecure USB stick or other (portable) data device. Consult with your ICT-administrator about safe ways to transport data. Do not transfer privacy sensitive information on Cloud services like Dropbox or OneDrive when it is not clear who has access to these services. Do not open or respond to e-mails/links from people or companies you do not know personally. When receiving e-mails from providers (e.g. KPN), check if the e-mails are from the actual provider (check if the e-mail is genuine: check links, do not simply open attachments, check if the e-mail is personalised and if the information provided is correct). When in doubt, contact the ICT-administrator. Send the password separately from the concerning data, preferably through a different medium than the concerning data (e.g. through sms/Whatsapp/phone).

Personal responsibility and accountability

You are personally responsible for your data usage, your username, password and e-mail address are strictly personal. You are responsible for all usage of your username, password and e-mail address. You are held responsible for any damage done by misuse of the facilities: this includes damage done by incorrect, careless or unjustified usage of your username, password and e-mail address. Improper use of the computer facilities as well as (purposely) publishing sensitive information will be sanctioned by the management. Purposely leaking out data will, in certain cases, be criminally prosecuted.

Reporting

When discovering or suspecting a data breach – including unauthorised access and/or unauthorised usage of personal data – you have to contact your supervisor immediately.

In case of theft or misplacement of a data carrier (laptop, phone etc.), inform your supervisor and discuss with your ICT-administrator on how to proceed. Please change your password(s) in all cases.

May 2018