Computer and Network User Regulations

Firstly you have to keep to the rules and regulations of the organisation you are working at. If information is not available understated will apply.

These regulations apply to all the facilities and amenities provided.
They apply to all persons working at the workstation or making use of the facilities and amenities, irrespective of whether they are at the workstation.

Care
Use the computer responsibly, it is on loan.
Do not install any software yourself without first consulting the ICT Manager.
Do not store large quantities of private material (photographs, films, music) on the work computer.
Do not use illegal software.
Log off or lock your screen when you leave the workstation.
Store documents in logical locations so that the names are recognisable to other users and the location is obvious (e.g. to your replacement if you are off sick).
Change your password regularly (at least twice a year) and use different passwords for private and work access.

Use of data
Handle the data you are working with carefully.
When sending an email check that the correct addressee is shown in the To: field.
Be aware of sensitive personal data and how to handle it.
Do not send confidential (sensitive personal) data to other people unencrypted.
Do not pass on confidential data or information to third parties without permission.
In order to use email on a phone or tablet, set up a PIN code or password so that the device locks automatically after a few minutes and requests the code when it is used again.

Do's and don'ts
Use the teleworking environment when you are off the premises (so that data never needs to 'leave the premises' in principle).
Never take sensitive data with you on an unencrypted memory stick or other storage medium.
Ask the ICT Manager for advice on secure ways of transporting data if necessary.
Do not upload sensitive personal information to cloud boxes such as Dropbox and OneDrive if it is unclear who has access.
Do not access/open any emails or links from people/companies that you do not know personally.
Check that emails from suppliers (e.g. KPN) really are from KPN (check links, do not open attachments and check whether the email is personalised and that everything is correct). If in doubt ask the ICT Manager to assist.
Use teleworking facilities with care. Follow the ICT Manager's teleworking instructions.

When sending confidential data to third parties you must protect it with a password or pack it in an encrypted zip file. Send the password separately, preferably using a different route than the one used for the data (e.g. SMS/WhatsApp/phone).

Personal responsibility and liability

You are personally responsible for your data usage.

Your user name, password and email address are strictly personal. You are responsible for any use made of your user name, password and email address.

You are liable for any harm resulting from misuse of the facilities and amenities: this applies to harm resulting from the incorrect, careless or improper use of your user name, password or email address.

Management may impose sanctions for the misuse of computer facilities or the deliberate disclosure of confidential information. The deliberate leaking of confidential information may also lead to criminal prosecution in certain circumstances.

Reporting

If you discover or suspect that there has been a data leak – including unauthorised access to and/or unauthorised use of confidential information – you must inform your supervisor immediately.

In the event of theft or loss of a storage medium (phone, laptop, etc.) inform your supervisor and consult the ICT Manager on any follow-up action required. Always change your password(s) afterwards.

UvA Ventures Holding
1 March 2017.