Reference: SB/UIM/12/1018/khv
Date: 9 December 2013

Use of “own” devices and applications
Consequences for the UT workstation

Contents

Summary

The University of Twente (UT) workstation is based on a bring/choose-your-own-device (BYOD/CYOD) system, which allows for flexible working, both in and outside of the campus.

The i-Strategy UT 2014-2017 describes this system in the following outlines, which may easily serve as a summary of this policy document.

Rationale

The use of a wide variety of mobile devices is expanding rapidly: smartphones, tablets, ultrabooks, notebooks, etc. All kinds and types of devices are replaced by new ones at an increasingly fast pace. These devices have been purchased by students and staff members themselves (BYOD), or have been paid for by the UT (CYOD). Both options are referred to as "BYOD". Due to these fast developments, prescribing a certain set of devices is undesirable in a community of professionals, as such would unnecessarily limit creativity and state-of-the-art IT use.

Mobile access to information and IT services is highly desirable. Students and staff members are increasingly mobile and expect to have proper access to information and IT services when they are on the way. Conversely, the UT organization and third parties also expect staff members to be easily contactable at all times, irrespective of their whereabouts. As the New Way of Working is coming into fashion ever more, this will strongly contribute to the wish for mobile access to information and IT services with personal devices.

Implications

The UT facilitates the use of devices chosen by students and staff members themselves. The UT determines policy, agreeing upon the frameworks for use, support and funding of BYOD.

The UT keeps a list of preferred devices, for which more extensive support options are available. For other devices, users will have to depend on manuals, published on-line for each type of device and/or operating system.

To the extent possible, UT information and IT services are accessible through open standards, causing the least possible dependence on certain types of devices.

The UT informs staff members and students about the privacy and security risks of using mobile devices. Not all risks can be covered by taking technical measures. A lot also depends on the awareness and behaviour of staff members and students, who have to take their own responsibility.

This policy document among other things provides frameworks for a BYOD project to be started by the ICT Service Centre (ICTS) in 2014. Technical and practical feasibility will impact all project decisions on the structure of the BYOD services yet to be made. Part of the ICTS services as described in the memorandum can only be provided after the project has produced its results. ICTS will publish further information on this aspect over the course of 2014.

Introduction

The past few years have seen a trend at the University of Twente (UT), which has staff members and students increasingly make their own choices as regards their use of devices, applications and cloud services. This raises questions regarding the desired level of support and the necessary security.

This trend is often described as Bring/Choose Your Own Device (BYOD/CYOD), as Consumerization of IT (CoIT), Bring Your Own Computer (BYOC) or as Use your own. The New Way of Working is also about working independently of location and time, for instance by using private computers. This policy describes the consequences of this development for the UT. There are areas of overlap with the Software Licence Policy, the Information Security Policy, the sourcing strategy and the working conditions policy.

The University of Twente (UT) workstation *is based on a bring/choose-your-own-device (BYOD/CYOD) system, which allows for flexible work, both in and outside of the campus.*

General

1. A standard workstation (laptop, desktop) administered by the ICT Service Centre (ICTS) is available, which is a perfectly suitable normal workstation for most staff members. Making equal choices in equal cases (standardization) is more efficient and cheaper for the UT as a whole.
2. Considerations for using other devices include working elsewhere, at home or on the road. As well, depending on use and personal preference, certain devices, applications or cloud services are more suitable or productive than others.
3. The UT places the responsibility on individual staff members when it comes to choosing the device and applications to be used. In order to have a grasp of the consequences, they can make use of the expertise of ICTS, Procurement and HR. This policy describes the preconditions with respect to these choices.
4. The freedom of choice to deviate from the standard and use more or other devices and applications - and associated individual responsibility - are facilitated as described in this policy. Preconditions are set from different points of view.
5. Obligations arising under European tenders apply to the purchase of devices. These may be deviated from only with good reasons.
6. The UT accepts the fact that, due to the use of mobile and/or private devices, a staff member's work and private life become more intertwined. If staff members do not want this, they may choose to switch off UT devices outside working hours (if their position allows this).
7. Working with other devices or at other hours and locations may involve risks as regards working conditions. Managers and staff members may discuss this during the annual performance appraisals and are supported by HR through information on the HR website and the efforts of the occupational health and safety officers.

Costs and reimbursements

8. The UT does not reimburse the costs of devices, applications and cloud services purchased for private purposes or compensate any damage caused to private devices by work-related use.
9. Units may opt to reimburse all or part of the costs of work-related apps, even if the relevant staff member uses a private device.

10. The Tax and Customs Administration considers the provision of devices (such as an iPad and laptop) as wage, unless it is demonstrated that the business use is more than 90%.[1] The rule of at least 10% business use applies to smartphones and mobile telephones.
11. The relevant unit will consider whether mobile devices are provided to the relevant staff member. In that case, a standard UT loan for use agreement must be concluded. This agreement also sets out any preconditions, financial or otherwise.

Support

12. Support is available to users for the selection, configuration, malfunctions, etc., of devices, applications and cloud services. It is, however, not possible to facilitate all user wishes and device options. The below text details per subject how and to what extent support is offered.
13. Insofar as the device enables this, support is at least available for:
    a. Being able to use the fixed and wireless network (UT-Net) and VPN.
    b. The possibility to read and send e-mails and synchronize their agenda (via a secure connection) on (mobile) devices.
    c. The possibility to read and process documents (via a secure connection) on (mobile) devices. Explanations are available on how to access user data (on network drives, for example), what software is the most suitable for various purposes and what technical limitations apply.
    d. The possibility to print documents from (mobile) devices. Explanations are available on which devices support printing.
    e. Being able to use Unified Communications (telephony, messaging, data, etc.) on (mobile) devices. Explanations are available on which devices supports Unified Communications, and to what extent.
    f. Configuring and restoring a back-up.
14. Support is available on the ICTS website in the form of manuals. For all devices for which active support is offered (refer to item 22), staff members can contact the service desk for support.

Procurement

15. Users are supported in the selection of devices (tablets, smartphones, laptops, USB sticks, external hard drives, etc.), applications (software) and cloud services (data storage, data transfer, collaboration, storage and playing videos and presentations, etc.). This support is offered through manuals on the ICTS website, describing the advantages and disadvantages of the most important alternatives. One goal of providing this advice is stimulating equal choices in equal cases. Staff members can also contact the service desk for support.
16. Moreover, Educational Services provides information through its website on what devices, applications and cloud services can be used in education.
17. Devices, applications and cloud services are purchased through the UT and provided to the relevant staff members and continue to be the property of the UT. A (small) stock is kept of the most common devices and parts. Stock management will be further coordinated during the quarterly consultations on IT & Research & Operational Management. Reference is made to the Software License Policy for the purchase of software.[2]
18. Staff members will ensure that they only install software with a valid license.

[1] So far, the Tax and Customs Administration has adopted the position that an iPad is suitable for private purposes and that it is difficult to demonstrate a 90% business use. It is expected that the Tax and Customs Administration will revise its position when detailing the work-related expenses scheme (starting date 1 January 2015 at the UT).
[2] Software Licenses and the UT [Softwarelicenties en de UT], reference SB/UIM/12/0601/khv, was approved by the University Operations Committee (UCB) on 12 March 2013, http://www.utwente.nl/sb/uim/vooreindgebruikers/softwarelicenties_en_de_UT.pdf

19. Staff members may opt to use privately bought devices and applications for UT purposes; this will not give rise to any obligation on the part of the UT.
20. Many app stores for tablets, smartphones and other devices, do not allow the purchase of applications taking place via the Procurement department of the UT, so staff members will have to purchase these applications themselves. Units are advised to establish standard amounts for a set of recommended apps to ease reimbursement for the costs of these applications.

Devices

21. Users can receive support for the installation, and for any malfunctions, of devices. For the most common devices, this support is offered by way of manuals available on the ICTS website, explaining the most important aspects of the device.
22. For a limited set of devices and operating systems, active expert support is available via the service desk. The ICTS website lists the devices for which this active support is offered.
23. The support does not make a distinction on whether the device is the property of the UT or of the user.
24. If a private device or parts thereof become defective, the user will be referred to his supplier for repairs and warranty.

UT applications

25. For the use of web applications that are used in the back office of various administrative processes, it is assumed that the staff member has a standard workstation administered by ICTS. An example is the use of Oracle Applications by Directorate for Financial and Economic Affairs (FEZ) and HR staff members and the use of Osiris by Educational Affairs Office (BOZ) staff members. The use of a certain web browser and specific plug-ins may be necessary. If another device is incompatible, it cannot be used for this purpose.
26. By default, web applications that are part of the front office of various administrative processes use open standards. This means that users may assume that the web applications are compatible with their device and browser.[3] Examples of front office applications are the use of Osiris self-service by students and teachers and the use of the student and staff portal. Users may determine for themselves which device and browser they will use to work with the web application, without any plug-ins being required. ICTS will draw up a plan on how to implement this.
27. The UT will not develop any apps for brand-specific devices. In order to facilitate students and others to develop such apps, a standard programming interface (REST API – which is preferably also used by the UT web applications) will be made available. ICTS will draw up a plan on how to implement this.

Education

28. If a degree programme sets any requirements on the hardware or software that students should have at their disposal, the students will be informed of this well in advance in a manner similar to the one used to communicate on the purchase of textbooks.
29. The UT, like a kind of virtual computer room, can make applications available irrespective of the operating system and capacity of a student's device. ICTS provides this service to degree programmes as a customized service.
30. Teachers want to be supported in the selection and application of modern educational tools and techniques. Educational Services cater to this wish.

[3] There are still differences in the implementation of html5 by web browsers, so problems may occur incidentally.

31. It will be clear to the teacher which connections are available in any given lecture room for using the equipment present, such as a beamer, smartboard, etc.

Research

32. Each research project will make its own choices as regards the devices to be used; no additional general guidelines can be given for this matter. ICTS can offer advice on the issue.

Information Security

33. As described in the Information Security Policy[4], information security is the responsibility of both the organization and of every individual user.
34. Depending on the classification of information[5], it needs to be assessed whether it is safe for this information to leave the UT and what security measures - such as encryption, screen locks and the possibility of remote deletion - are required. The UT will not implement these security measures for all devices as a standard. Instead, ICTS is developing services which are, whenever possible, provided through a self-service web application.
35. Users are responsible for preventing malware (viruses, etc.) from becoming active on the device. If an infection of the network is discovered, the device will be isolated until the problem has been solved. Information is provided on how to prevent and remedy an infection on the ICTS website. Active support is also offered through the service desk.
36. Mobile devices are more sensitive to damage, theft and failure than desktop devices are. A point of attention is the accessibility of data, which can be ensured by backing data up in time. Another point of attention is the integrity and confidentiality of data, especially if family, friends or children also have access to the device. Users are personally responsible and these risks are pointed out to them by ICTS and immediate superiors. Reference is also made to the general integrity code yet to be developed for the entire UT. This code describes the ethical values which we support and for which one can hold us accountable.
37. On its website, ICTS will place guidelines which deal with these risks, outline what prevention options are available (such as using encryption and passwords) and describe what to do if a device is stolen or lost. These guidelines cover matters including changing passwords as soon as possible in order to prevent any more information from being compromised.
38. It is not safe for all types of data to leave the UT. This may relate to data stored on devices as well as to cloud services. Users require a risk assessment checklist. University Information Management is set to develop this checklist in consultation with ICTS and will make it available via the ICTS website.
39. When securing the UT network, ICTS will take into account the fact that there are no guarantees that the device used is free from malware.
40. When securing applications, ICTS takes into account the fact that the network between the device and the web server is not safe. Confidential information is sent through an encrypted connection.

[4] Information Security Policy of the University of Twente [Informatiebeveiligingsbeleid Universiteit Twente], SECR/UIM/11/0405/khv
http://www.utwente.nl/sb/uim/informatiebeveiliging/informatiebeveilingsbeleid_ut.pdf
[5] Classification Guidelines on Information and Information Systems of the University of Twente [Cassificatierichtlijn Informatie en Informatiesystemen Universiteit Twente], SECR/IM/11/0412/khv
http://www.utwente.nl/sb/uim/informatiebeveiliging/classificatierichtlijn_ut.pdf