INFORMATION AND COMMUNICATION TECHNOLOGY FAIR USE RULES

Against the background of the dream to be an internationally recognised university in Africa, distinguished for engaged scholarship, social responsiveness and an ethic of care, the council of the North-West University (NWU) has adopted these rules to provide the framework for responsible management of Information and Communication Technology (ICT).

1 Interpretation and application

1.1 These rules must be interpreted and applied in a manner consistent with the –

1.1.1 Constitution of the Republic of South Africa, 1996

1.1.2 Higher Education Act, No 101 of 1997

1.1.3 The Promotion of Access to Information Act, 2 of 2000 (PAIA) and

1.1.4 The Electronic Communications and Transactions Act No. 25 of 2002 (ECTA)

1.1.5 The Regulation of Interception of Communications and Provision of Communication-related Information Act No. 70 of 2002 (RICA)

1.1.6 The Protection of Personal Information Bill, No. 9 of 2009 (Data Privacy Bill)

1.1.7 International Code of Practice for Information Security Management (ISO 27002)

1.1.8 European Union Directive on Privacy and Electronic Communications (EU Directive)

1.1.9 All other legislation and international instruments applicable to ICT

1.1.10 The Regulations for Reporting by Public Higher Education Institutions issued in terms of the Higher Education Act, 1997

1.1.11 The Statute of the North-West University (2017)

1.2 These rules must be read in conjunction with the Communication Policy and other policies of the NWU that may be relevant to the use of ICT.

1.3 Addenda must be read as an integral part of this document.

2 Definitions

In these rules and for the purposes of the governance, management, operation and use of ICT at the NWU –

"enterprise application" means both purchased and internally developed ICT systems and services used by the NWU as a whole in support of mission critical university activities and processes;

"ICT" means information and communication technology, and where it is indicated by the context, it refers to the NWU's information and communication technology department;

"ICT architecture" means an integrated set of technical ICT choices made to guide the university in satisfying core needs and requirements;

"ICT facilities" include –

- ICT hardware provided by the University, such as PCs, laptops, tablets, smart phones and printers; all electronic, audiovisual, fire detection and other security or facilities control infrastructure and related technologies, software, data and authorized access to these systems;
- software provided by the University, including operating systems, office application software, web browsers and special deals for employees and students on commercial application packages;
- data provided by the University, or that the University arranges access to, including online journals, data sets and citation databases;

- access to the network provided or arranged by the NWU, including network connections in halls of residence, on campus Wi-Fi and connectivity to the internet from computers of the University;
- online services arranged by the NWU, including Office 365 and Google Apps;
- ICT credentials, including users' NWU logins and any other token such as an email address, smartcard, Eduroam access and dongles issued by the University to identify users when using ICT facilities.

"ICT infrastructure" means all the underlying technology that makes ICT function, including servers, the network, personal computers, printers, operating systems, databases and all other hardware and software required to ensure the reliable, efficient and secure delivery of ICT services;

"UMC" means the University Management Committee, and

"user" means anyone using the ICT facilities of the NWU, including students, employees, visitors to NWU's website, anyone accessing the NWU's online services from off-campus, external partners, contractors and agents based onsite while using the NWU's network, or offsite when accessing the NWU's systems, tenants of the NWU using computers, servers or the network of the NWU, visitors using the NWU's Wi-Fi and anyone associated with another institution while logging on via Eduroam.

3 Statement

It is the ICT rules of the NWU that –

3.1 ICT decisions made by any component of the University may be made only within the established set of standards, architectures and infrastructure, while keeping in mind the interconnected nature of ICT and that most ICT decisions have university-wide implications, the need to enable cost effective operations and manage risk and that local decisions must in principle be funded from the resources of the component concerned;

3.2 the University's ICT facilities are used safely, lawfully and equitably;

3.3 the University's ICT facilities are made available to users for the purposes of promoting the achievement of the NWU's mission.

4 Monitoring

4.1 The IT Department may monitor and record the use of the University's ICT facilities for the purposes of

- detecting, investigating or preventing misuse of the facilities or breaches of rules and or policies of the University;
- ensuring the effective functioning of the facilities, and
- the effective and efficient planning and operation of the facilities.

4.2 The IT Department may, in consultation with the registrar, provide information regarding the infringement of rules or the law to appropriate law enforcement agencies or any other organisation whose regulations have been breached by a user.

5 Fair use guidelines

5.1 In order to ensure that the University's ICT facilities are used safely, lawfully and equitably, the fair use guidelines contained in Addendum A applies to anyone using the those facilities, including hardware, software, data, network access, third party services, online services and ICT credentials.

5.2 When an employer or student who produced information in the course of employment or enrolment becomes unavailable, the Registrar may in consultation with the Chief Director IT grant permission for such information to be retrieved if required for official university purposes.

5.3 The demand for IT goods is managed on a centralised basis by the Chief Director: Information Technology, with due regard to general and technical standards and guidelines set by the IT Division and budgetary constraints. The final decision in respect of IT goods requirements is made within each

Division with regard to their specific area of responsibility, subject to institutional standards and guidelines set by the IT Division.

5.4 The fair use guidelines may, subject to the approval of the Deputy Vice Chancellor: Campus Operations and Information Technology, be amended from time to time by the Chief Director Information Technology.

5.5 IT must make the latest version of the fair use guidelines accessible online to all users.

Addendum A

Fair Use Guidelines

1 General guidelines

1.1 Use of the NWU's ICT facilities is subject to the authority to do so by obtaining a username and password, or explicit receipt of access rights to a specific system or resource.

1.2 Every user, including a user using the University's open access facilities, is required to use the University's ICT facilities safely, lawfully and equitably.

1.3 No user may put the NWU's IT facilities at risk by introducing malware, interfering with hardware or loading unauthorised software.

1.4 The NWU's ICT facilities may not be wastefully or abusively used by infringing copyright or privacy.

1.5 The use of the NWU's ICT facilities for personal, non-profitable purposes is permitted, subject to cancellation on reasonable grounds by the Chief Director IT.

1.6 Use of IT facilities for non-NWU commercial purposes or for personal gain requires the explicit approval of the Chief Director IT.

1.7 Software licensed in the name of the NWU may be used only for academic and official purposes.

1.8 When using services via Eduroam, the user is subject to both the regulations and policies of the NWU and of the institution from whose facilities the services are accessed.

1.9 Breach of any applicable law or third party regulation is regarded as a breach of the policies of the NWU.

2 Responsibilities of users

2.1 Users must safeguard personal data by preventing anyone else from using their ICT credentials and by not disguising their online identities and must take all reasonable precautions to safeguard all the ICT credentials issued to them.

2.2 A user must respect other users' information and not attempt to obtain or use anyone else's credentials.

2.3 Users must abide by the regulations applicable to any other organisation, including Tenet, Telkom and Vodacom, whose services they access.

2.4 Where software licenses procured by the NWU impose obligations on users, or the related agreements contain requirements for lawful use of the software, those obligations must be complied with.

2.5 All users must administer their passwords and other personal information responsibly and securely.

2.6 A user may not leave a logged in computer unattended and must log out properly at the end of a session.

2.7 When dealing with personal, confidential or sensitive information, a user must take all reasonable steps to safeguard such information and must observe the NWU's Information Policy.

2.8 When users use the ICT facilities for communication purposes, the NWU's Communication Policy must be complied with, with specific reference to the Social Media Framework and the Online Publications Framework (Addenda 3 and 4 of the Policy).

2.9 When dealing with protected information as contemplated by the NWU Information Policy, users must –

2.9.1 use a method with appropriate security for sending it;

2.9.2 if the information is sent using removable media, use a secure, tracked service;

2.9.3 if the information is accessed from off-campus, avoid working in public locations where the screen can be seen, and use an approved connection method that ensures that the information cannot be intercepted;

2.9.4 not store protected information in personal cloud services, such as Dropbox, unless the information is first securely encrypted.

2.10 When using shared facilities for personal or social purposes, users must vacate the facilities if they are needed by other users for university related work.

2.11 When using shared spaces, users are required to be sensitive to what may disturb other users in that space and to what they may find offensive.

2.12 Users may not consume bandwidth excessively, waste paper when printing and waste electricity by leaving equipment switched on needlessly.

2.13 When a user becomes aware of an infringement of this policy, the user is obliged to report the infringement to the registrar.

3 Transgressions by users

3.1 Users may not attempt to obtain or use, usurp, borrow, corrupt or destroy another user's credentials, may not impersonate another person or otherwise disguise their identity when using the facilities.

3.2 Users may not create or transmit or cause the transmission of –

3.2.1 any offensive, obscene or indecent images, data or other material, or any data capable of being resolved into obscene or indecent images or material;

3.2.2 material with the intent to cause annoyance, inconvenience or needless anxiety;

3.2.3 material with the intent to defraud;

3.2.4 defamatory material;

3.2.4 material that infringes copyright, or

3.2.5 unsolicited bulk or marketing material to users of networked facilities or services, save where that material is embedded within, or is otherwise part of, a service to which the user or their user organisation has chosen to subscribe;

3.3 No user may ddeliberately access networked facilities or services without authorisation.

3.4 Users may not do anything to jeopardize the integrity of the infrastructure, including –

3.4.1 damaging, reconfiguring or moving equipment;

3.4.2 loading software on the NWU's equipment other than in approved circumstances;

3.4.3 reconfiguring or connecting equipment to the network other than by approved methods;

3.4.4 changing the setup of the infrastructure without authorisation, and

3.4.5 add or remove software without authorisation.

3.5 Users may not without authorisation set up any hardware or software that would provide a service to others over the network such as games servers, file sharing services, data sharing servers, IRC servers or websites.

3.6 The running or usage of any radio network is prohibited - even within the unlicensed radio spectra - on the property of the University without the consent of the Chief IT Director - irrespective if such networks may have a link with the University network or not.

3.7 Users must take all reasonable steps to avoid introducing malware to the infrastructure.

3.8 No user may disrupt or circumvent any ICT security measures or attempt to do so.

3.9 No user may attempt to access, delete, modify or disclose information belonging to anyone else without their permission, or explicit approval granted by the registrar to do so.

3.10 Users may not publish information on behalf of third parties without the approval of the registrar after consulting the Chief Director ICT.

3.11 Users may not send unsolicited bulk emails or chain emails other than in specifically authorised circumstances.

3.12 No user may monitor or attempt to monitor the use of the facilities, including monitoring of network traffic, network or device discovery, Wi-Fi traffic capture, installation of key logging or screen grabbing software that may affect another user and attempting to access system logs or servers or network equipment without explicit permission granted by the Registrar after consulting the Chief Director ICT.

3.13 No user may attempt to access, delete, modify or disclose restricted information as contemplated by the NWU Information Policy belonging to anyone else without their permission, unless it is clear that they intend others to do so.

3.14 Where a user's transgression causes damage to the University, the cost of such damages may be recovered from the user.