NWU Information Governance Framework

Reference number	1P_1.16_2020
Policy owner	Registrar
Policy administrator	Director: Corporate & Information Governance Services
Responsible division	Office of the Registrar
Status	Approved
Approved by	**NWU Council**
Date of approval	19 March 2020
Date of amendments	
Review date	March 2023

Registrar

INFORMATION GOVERNANCE FRAMEWORK

Approved by the University Management Committee on 11 March 2020
Approved by the NWU Council 19 March 2020

1 Preamble

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 this Information Governance framework on 19 March 2020.

2 Introduction

2.1 The NWU views Information Governance as an umbrella concept aiming at governing all information management activities that are performed to derive/ensure value from Information for the University while complying with all regulatory requirements and international best practices.

2.2 Information Governance:

- is a strategic, top-down approach to manage all aspects of information within the organisation in accordance with the strategic objectives of the University;
- provides the framework, systems and processes for ensuring the value of information is maximised, and risks are minimised;
- considers all information, regardless of its format and includes structured information[1] such as databases and unstructured information[2] such as documents[3] and e-mails.
- is a subset of Corporate Governance – it is a strategic rather than tactical discipline, which aligns information management with business strategy and processes and includes, but is not limited to, the following elements:

Cybersecurity[4] is about protecting the systems and information security used for business	*Information*[5] *Management*[6] focuses on the management of unstructured information.	*Records Management* is the activities required to provide evidence of business activities and processes.	*Data*[7] *Governance*[8] is the management of the integrity, security, availability, and usability of data used in the University.

[1] Information that is already structured in fields such as "date", "title", "subjected. and can be identified by metadata tags.

[2] Information that does not have a pre-defined information model or is organised in a pre-determined manner.

[3] A piece of written, printed or electronic matter that provides information or evidence or that serves as an official record.

[4] The technique of protecting computers, networks, programs, data and information from unauthorised access that are designed for theft or exploitation.

[5] Data applied to some purpose and adding value for the recipient.

[6] Information management plans, builds, runs and monitors the practices, projects and capabilities that acquire, control, deliver and enhance the value of data and information assets in alignment with the direction set by the governance structure.

[7] Information that has been translated into a form that is efficient for movement or processing / Facts and statistics collected together for reference or analysis purposes.

[8] Merging of data quality, data management and risk management surrounding the handling of data. Data Governance exercises positive control over the processes and methods used by data stewards and data custodians to handle and make best use of their data assets.

Privacy Is the legal obligation of the University to protect personally identifiable information.	*eDiscovery*[9] is the process of identifying data for evidence in litigation and enquiries.	*Data Analytics*[10] uses systems and software to examine data sets to provide insights from the information within.	*Risk & Compliance*[11] monitors and audits enterprise risk and compliance to meet regulatory requirements.

3 Definitions

All the definitions and concepts of relevant terms are indicated in the footnotes included in the text.

4 Purpose and scope

4.1 This framework guides the creation, use and management of the NWU's information assets. It concerns the management of all paper and electronic information and its associated systems within the organisation, as well as information held outside the University that affects its regulatory and legal obligations.

4.2 The NWU regards information generated by the University as a vital asset, and the framework is created to:

4.2.1 direct all staff and student leadership who generate information (i.e. either create or receive), use and distribute information, store and manage information, share information, as well as the disposal thereof;

4.2.2 determine the procedures for the management of information in the complete lifecycle as it is shared with all relevant stakeholders, partners and suppliers; and

4.2.3 distinguish between peculiarities in regard to the management of all paper as well as electronic information and their associated systems within as well as, where relevant, outside the institution.

4.3 This framework ensures that:

4.3.1 Stakeholder needs are evaluated to determine balanced, agree-on university objectives, which are to be achieved through the acquisition and management of information resources;

4.3.2 The direction is set for information management capabilities through prioritisation and decision-making;

4.3.3 Performance and compliance of the information resources are monitored against agreed-on direction and objectives;

4.3.4 Clear roles and responsibilities for information management and security are in place, supported by robust policies and procedures, including a framework to protect university information against unauthorised access/use, compromise of assets and interruption of University activities;

4.3.5 Information procedures comply with the relevant legislation.

4.3.6 The University complies with the principles of Good Corporate Governance as identified in the King IV Report on Corporate Governance;

4.3.7 Information risks are assessed appropriately;

4.3.8 Appropriate training is available to all staff members;

4.3.9 Robust arrangements for, and learning from, information related incidents such as data breaches or losses;

4.3.10 Adequate and appropriate records[12] are maintained, and the sharing of information is carried out in an appropriate manner; and

[9] The process of identifying, preserving, collecting, processing, searching, reviewing and producing data and information that my relevant to a litigation matter, regulatory notice or other formal inquiries. An effective Information Governance program helps to minimise the costs involved in litigation by reducing the costs of identifying, preserving, collecting, processing and searching of data and information.

[10] The application of E-Systems to the analysis of large data sets for decision making. Data Analytics is an interdisciplinary field such as statistics, patter recognition, system theory and artificial intelligence to name a few.

[11] A discipline to hold the institution to all related laws, rules, regulations and internal policies. A mature compliance function will perform an advisory, monitoring and educational role to support the institution in achieving compliance.

[12] At the NWU a record refers to anything that is produced due to the undertaking of a business activity or legislative requirement, and is evidence of the fact that a process of procedure took place in support of the activity or requirement.

4.3.11 University information is classified according to an approved classification system.

5 Principles[13] that guide information governance

5.1 The NWU is committed to the principles set out in this framework

5.2 The NWU recognises the need for an appropriate balance between transparency and confidentiality in the management and use of information and fully supports the practices in Principle 12 of King IV Report and other principles, rules, regulations, policies and procedures in accordance with international best practices[14]:

5.2.1 Accountability for as far as the University's information-management programme is guided by a set of policies and procedures, not only to guide the implementation thereof but to ensure auditability of the implementation thereof.

5.2.2 Transparency in respect to the fact that the processes and activities of the NWU information-management programme are properly documented to allow effective implementation of all relevant policies as well as the monitoring thereof.

5.2.3 The integrity of records and information generated at the NWU shall have a reasonable and suitable guarantee of authenticity and reliability.

5.2.4 The information-management programme is constructed to ensure a reasonable level of protection to records and information that are private, confidential, privileged or essential to business continuity.

5.2.5 The programme shall ensure compliance with applicable laws and all other binding directives, including relevant university policies.

5.2.6 In regard to availability, the University will maintain its records in a manner that ensures timely, efficient and accurate retrieval of information needed for business purposes.

5.2.7 The retention schedule of records is aimed at a maintenance programme that allows for the maintenance of information for an appropriate time taking into consideration relevant legal, regulatory, fiscal, operational and historical requirements

5.2.8 The University provides for secure and appropriate disposition of records no longer required to be maintained by applicable regulations.

5.3 In regard to the value proposition of information, the NWU believes that accurate, timeous and relevant information is essential to deliver the highest quality of service to all stakeholders. As such, it is the responsibility of all staff and student leadership to ensure and promote the quality of information and to use information in decision-making processes actively.

5.4 Any breaches of the stated principles in this framework should be reported in writing to the information officer or his deputy.

5.5 Failure to comply with the principles may result in disciplinary action for staff and students in accordance with relevant legislation and policies.

6 Roles and responsibilities

6.1 Information officer and deputy information officer

6.1.1 In accordance with the Promotion of Access to Information Act (2 of 2000) and the first draft regulations in terms of the Protection of Personal Information Act, 2013, the information officer of the University is the Vice-Chancellor, and the deputy information officer is the Registrar.

6.1.2 The information officer and his deputy have the overall responsibility for information governance within the NWU by ensuring that appropriate mechanisms are in place to support service delivery and continuity and that information is used appropriately and securely.

6.1.3 The information officer must be registered with the Information Regulator and this function may be delegated to other members of the University and deputy officers may be appointed to assist with duties.

[13] It is the vehicle to translate the desired behaviour into practical guidance for day-to-day management.

[14] 2009 GAR Principles developed by ARMA.(URL: https://www.arma.org/docs/bookstore/theprinciplesmaturitymodel.pdf?sfvrsn=2) [Accessed 29 March 2016

6.2 Governance

6.2.1 In accordance with the Higher Education Act (101/1997 as amended) and the NWU Statute, the Council, through the advice of the ***Technology and Information Governance Committee***[15] of Council fulfils a governance role in nurturing a culture at the NWU that values, protects and utilises information in an optimal way which will result in the following:

- The leveraging of information to sustain and enhance the University's intellectual capital.
- An information architecture that supports confidentiality, integrity and availability of information.
- The protection of privacy of personal information
- The protection of the University's reputation.
- The continual monitoring of information security.
- Consider risk factors in both the external and internal business environments and continually monitor significant risk.
- Ensuring the reporting to the DHET in the annual integrated report.

6.3 Management

6.3.1 The *University Management Committee (UMC)*, through advice from the Information Technology Committee and an Information Management Committee fulfils a management role in alignment with the direction set by the Council.

The UMC oversees the integration of the Technology and Information strategy into the University's strategic agenda and all relevant business processes to ensure and maintain overall compliance, cost-effectiveness, sustainability and proper role clarification in regard of the roles and responsibilities.

The UMC submits reports to the Council's Technology and Information Governance Committee in regard to ongoing assurance regarding the effective and efficient management of the University's information assets.

6.3.2 The *Information Management Committee* is involved in information management issues and comprises individuals who are suitably qualified. The Information Management Committee advises UMC on the implementation and monitoring of information management matters at the University.

6.3.3 NWU Employees

6.3.3.1 Day-to-day responsibility for administration and compliance with this framework is the responsibility of line managers, who need to ensure that:

- staff under their direction and control are aware of the policies and procedures in their respective departments and applying the policies and procedures in respect of IG in carrying out their day-to-day work.
- Mitigate information risks;
- Implement security authorisation of information;
- Ensure that all staff attend the relevant training sessions related to Information management.

6.3.3.2 All staff members have a responsibility to adhere to the relevant information governance and management standards, policies and procedures. This framework applies to all staff who create, store, share and dispose information.

[15] Terms of Reference of the TI Governance Committee

7 Informing policies and rules

Information Governance covers a wide range of policies. To assist the University in complying with its duties, the following university policies and rules, amongst others, will be developed that are relevant to information governance:

- Information Security policy
- Records Management policy
- Retention and disposal schedules i.e. NWU File Plan and Disposal Schedule
- Data Privacy policy
- ICT policy
- Information Sharing policy
- Remote Working policy
- Sharing of information with third parties
- Confidentiality Policy
- Data processing by third parties
- Digitisation policy
- Bring your own device policy
- E-mail management policy
- Data storage and storage devices policy
- Social media

8 Informing procedures

Procedures such as the following will be developed as needed:

- Legal and regulatory compliance procedures
- Creating and receiving information
- Storing and archiving information
- Disposing of information
- Acceptable content types
- Managing the volume of information
- Digitisation procedures
- Remote working procedure
- Bring your own device procedure
- Minimum metadata standards
- Reporting information losses
- Reporting information/security breaches
- Information backup and disaster recovery
- Managing personal information
- Collaboration and sharing of information

9 Informing procedures

Procedures such as the following will be developed as needed:

- Legal and regulatory compliance procedures
- Creating and receiving information
- Storing and archiving information
- Disposing of information
- Acceptable content types
- Managing the volume of information
- Digitisation procedures
- Remote working procedure
- Bring your own device procedure
- Minimum metadata standards
- Reporting information losses
- Reporting information/security breaches
- Information backup and disaster recovery
- Managing personal information
- Collaboration and sharing information

10 Legislation and external directives

Instances of statutory directives such as the following steer the process by means of which sound and effective information governance and management are to be established, maintained and monitored by the NWU:

- NWU Statute (24 March 2017)
- The Constitution of South Africa
- Higher Education Act (101/1997 as amended)
- King IV Report on Corporate Governance™
- Consumer Protection Act, No 68 of 2008
- Protection of Personal Information, No Act 4 of 2013
- Companies Act, No 71 of 2008 and Companies Regulations 2011
- National Credit Act, No 34 of 2005 and National Credit Regulations
- Electronic Communication and Transaction Act, No 25 of 2002
- Regulation of Interception of Communication Act, No 70 of 2002
- Financial Intelligence Centre Act, No 38 of 2001
- Banks Act, No 94 of 1990
- Compensation for Occupational Injuries and Diseases Act, No 130 of 1993
- Occupational Health and Safety Act, 85 of 1993
- Basic Conditions of Employment Act, No 75 of 1997
- \Employment Equity Act, No 55 of 1998
- Labour Relations Act, No 66 of 1995
- Unemployment Insurance Act, No 63 of 2002
- Income tax Act, No 58 of 1962
- Tax Administration Act, No 28 of 2011

- Value Added Tax Act, No 89 of 1991
- Public Finance Management Act, No 1 of 1999
- Health Act, No 63 of 1977
- Higher Education Act, No 101 of 1997
- National Archives and Records Services Act, No 43 of 1996
- National Payment Systems Act, No 78 of 1998
- Skills Development Act, No 97 of 1998
- Copyright Act of 1978
- Various ISO standards, ITIL, TOGAF, COBIT, Val IT, ISO/IEC 20000, ISO/IEC 27002 (formerly 17799), ISO/IEC 38500, ISO 9002, ISO/15489

11 Strategies and plans

Information is viewed as a strategic asset that needs to be governed and managed in careful and accountable ways.

This framework should be read in conjunction with, but not limited to:

- NWU Strategy 2015-2025
- Information Technology Strategy (2019-2023)
- Digital Business Strategy
- Teaching-Learning Strategy 2016-2020
- Annual Performance Plans of the NWU

12 Information management[16]

12.1 The NWU continuously oversees the information management practices that support good decision-making, integrity, accountability and transparency which are essential to delivering good business outcomes.

12.2 The NWU determines how all stakeholders work with the NWU's information, thus weighing up the practicalities of how to handle it, as well as taking into account the ethical considerations of managing what is at times sensitive and private information.

12.3 The NWU acknowledges that information management is the University's responsibility, and needs to be considered not only by the most senior levels of management but by all staff members.

12.4 Information management creates value and ensures that the statutory and regulatory requirements can be maintained at all times.

12.5 Information architecture

12.5.1 All NWU Information is classified in the NWU File Plan and Disposal Schedule into one of the 10 main business activities of the University, and after that into the related business process.

12.5.2 The NWU will ensure that the File Plan and Disposal Schedule:

- Define, classify and prioritise all information assets;
- Define the executive information asset manager;
- Define information asset owners;
- Define additional policies and procedures for handling information assets;
- Define a security strategy and related policies for information assets.

[16] Information management entails the activities and organisational function that are necessary in order to manage, control, and destroy data in any form – regardless their medium, origin and quality. Information is obtained from various sources.

12.5.3 The records retention schedule is included in the NWU File plan and disposal schedule and updated annually. This retention schedule applies to all information related to the business activity/business process.

12.5.4 This NWU File plan and Disposal Schedule applies to all paper documents, Electronically Stored Information (ESI) - along with the particular metadata, confidentiality, and other issues associated with ESI.

12.6 Records Management

12.6.1 All NWU business processes in support of the information lifecycle are managed within the records-management process. The records generated from the business processes are regarded to be evidence of the activities. Each business process has to develop its own business-process specific information policies/procedures and the combination of these policies/procedure would become the NWU Information Governance policies/procedures.

12.6.2 The procedures must fulfil the policies if followed. The guidelines must fill in any gaps that make the policies and procedures difficult to execute. All such rules must be easy for NWU to maintain and to modify when necessary.

12.6.3 The following are overall information and records management processes, but not limited to:

- Procedure for collecting, receiving and creating information
- Classification/indexing of information procedure
- Processing of information procedure
- Retention of information procedure
- Disposal of information procedure
- Procedure for managing personal information
- Procedure for physical storage of information
- Procedure for collaboration and sharing information with third parties
- Procedure for the management of NWU minutes and minute books
- E-discovery processes.

12.6.4 A *Records Management Policy* is in existence to direct the following:

- Define the extent of information for which records management is responsible;
- Define Records management's role in the classification, retention and disposal of information[17];
- Define Records management's role in legal and regulatory compliance.

13 Knowledge management[18]

13.1 Knowledge is information in action as it evolves from information management.

13.2 The NWU recognises that it is critical that the knowledge must be managed effectively.

13.3 The NWU will ensure that processes be defined to manage and measure knowledge flows.

[17] It is a requirement that records are destroyed according to the approved procedure. This entails that electronic records are made unreadable and irretrievable and by locating all files and backup copies, removing them or physical destruction of storage media. With paper records this is achieved by shredding.

[18] The discipline that promotes a unified approach to identifying, capturing, evaluating, retrieving and sharing and institution's information assets.

13.4 Information security[19] management

13.4.1 Physical security

The NWU's systems protect information on equipment and premises from unauthorised physical interaction through measures that can be seen or touched, such as:

Keeping filing cabinets locked	Shredding paper records	Locking office doors
Implementing access control using key cards or biometrics	Utilising reactive and live CCTV systems and video surveillance	Hiring security personnel
Fire alarms	Temperature monitoring alarm systems	Office alarm systems
Deployment of security staff		

13.4.2 Digital security

The NWU's system protects information on systems and networks from unauthorised electronic interaction through electronic and digital measures, such as:

Effective password management	Anti-virus software	Up-to-date Software
Ensuring firewalls	Encrypting hard drives, files, and e-mails	Managing mobile devices
Hiring cybersecurity experts to conduct penetration testing		

13.4.3 Operational security

The NWU's system protects information from operational risks inside the University through measures that relate to routine functions and operations, such as:

Fostering a culture of security	Adding communication messages when staff log in to the NWU network	IT providing in-house staff training and awareness regarding security
Providing external staff training	IT monitoring workstations of staff in the background to ensure the correct application of policies and procedures	Implementing employee on-boarding and exit procedures

13.4.4 Administrative security

The NWU's systems protect information from business risks outside of the University through measures that originate from key decision-makers or formal structures, such as:

Providing awareness training about business risks	Planning around security	Drafting privacy, incident response, and information security policies
Conducting due diligence of subcontractors	Implementing audit controls	Business continuity planning

- The NWU establishes and maintains policies for the effective and secure management of its information assets and resources;
- The NWU undertakes or commissions annual assessments and audits of its information and IT security arrangements;
- The NWU promotes effective confidentiality and security practice to its staff members through policies, procedures and training;
- The NWU establishes and maintains *incident reporting procedures* and will report, monitor and investigate all reported instances of actual or potential breaches of confidentiality and security by IT and Protection Services.

[19] Protects data and information from unauthorised access to avoid data breaches, identity theft and to protect privacy.

14 IT Architecture[20] and Technology

14.1 The NWU is concerned about the effective and efficient leveraging of IT technologies and resources to facilitate the achievement of strategic objectives.

14.2 The NWU is concerned with the content technologies, as these are the cause of and possible solution for most of the IG challenges.

14.3 The relevant technologies may include CS[21], Records Management (RM), e-discovery, and technologies involving mobile, social, cloud, and big data.

14.4 NWU develops a functional architecture for IG which create value through the realisation of benefits and optimisation of IT expenditure. Where relevant, it should align and integrate the different tools and capabilities required for Electronic Content Management (ECM), records management, e-mail management, e-discovery, social content, etc. This will help to ensure that IG becomes entrenched in NWU's IT strategy, enabling the IG program to leverage technical resources and technologies. Developing the architecture required to effectively fulfil the IG program requires not just technical expertise, but also ECM, records management, and related expertise to provide a more comprehensive strategy for controlling the risk of institutional information.

14.5 Based on new business processes and policies requirements, gaps in current architecture needs to be identified, and changes in architecture need to be planned/architected to support the additional needs, ensuring that stakeholder requirements are met.

14.6 Data storage and storage devices

The NWU develops and maintains policies and procedures to:

14.6.1 Identify approved and secure storage spaces for information/data/records (electronic) with specific reference to Cloud storage to limit the risks imposed on university data.

14.6.2 Manage physical storage areas.

14.7 Remote working

14.7.1 The NWU develops and maintains policies and procedures to manage the manner how staff should manage information when working remotely.

14.7.2 The University has a secure network, but when information is taken out of the office, security and confidentiality is at risk and policies and procedures should be developed to address this issue.

14.7.3 Employees need to be extremely careful when doing work in public places, working on public Wi-Fi.

14.8 Bring your own device (BYOD)[22]

Personal devices could include smartphones, personal computers, tablets, or USB drives. The NWU will develop and maintain policies and procedures which will:

14.8.1 Manage how information is going to be kept secure when staff members use a personal device for official university business.

14.8.2 Manage the higher risks for the University in terms of confidentiality and the potential loss of employee and university privacy.

14.8.3 Establish a register of users that use a personal device for official university business.

[20] Architecture can also be called a high-level map or plan of the information assets in an organization, including the physical design of the building that holds the hardware.

[21] Content Services

[22] Bring your own device - also called bring your own technology, bring your own phone, and bring your own personal computer —refers to being allowed to use one's personally owned device, rather than being required to use an officially provided device.

14.9 Metadata[23] Management

The NWU develops and maintains policies and procedures which:

14.9.1 Indicate how metadata should be applied and managed on all pieces of information;

14.9.2 Set minimum standards for metadata requirements.

14.10 E-mail management[24]

The NWU develops and maintains policies and procedures which:

14.10.1 Ensure data protection though the management of e-mail as information resources;

14.10.2 Provide standards to all staff on the management of e-mails.

15 Privacy[25]

15.1 Protection of personal information[26]

15.1.1 The NWU recognises the need for the ongoing management of information to ensure that it results in the protection of personal information;

15.1.2 The NWU will establish and maintain policies to ensure compliance with the Protection of Personal Information Act 4 of 2013 (POPIA);

15.1.3 The integrity of information will be developed, monitored and maintained to ensure that the information is processed only for the purpose for which it is intended.

15.1.4 All records of personal information will not be retained any longer than is necessary for achieving the purpose for which the information was collected and subsequently processed.

15.1.5 Students should have complete access to their personal information relating to their own studies.

15.1.6 The NWU will have clear procedures and arrangements[27] regarding the lawful processing of information in a reasonable manner that does not infringe the privacy of all stakeholders.

15.1.7 The NWU will have clear procedures and arrangements regarding the handling of evidence in litigation, administrative processes and disciplinary actions, labour matters, criminal matters and enquiries;

15.1.8 The NWU regards all personally identifiable information relating to students and staff as confidential except where legislation and/or policy requires otherwise;

15.1.9 In the event of the transfer of personal information to countries outside South African borders, this will be undertaken in accordance with the POPIA and relevant guidelines;

15.1.10 The Compliance Office will undertake or commission annual assessments and audits for its compliance with legal requirements;

15.1.11 Availability of information for operational purposes will be maintained within set parameters relating to its importance via appropriate procedures and computer system resilience.

15.2 Working with third parties

The NWU develops and maintains policies and procedures which:

15.2.1 Define practices and standard operating procedures for sharing information with third parties;

15.2.2 Define, through clear guideline and policies, how organisations/institutions can manage how third parties handle personal information and confidential information.

[23] Metadata describes described data. It summarises basic information about data, ensuring finding and working with data is easier.

[24] Email management involves the systematic control of the quality and quantity of electronic messages that are sent from within, and received by, an organization.

[25] Usually refers to data protection and specifically the compliance and reputational obligations on business to protect personal information.

[26] Also referred to as personally identifiable information. Information (including opinions) about identifiable persons. For example, name, contact details and email addresses of individuals are each likely to be personal information, as are fingerprints and photographs.

[27] The way that people and things are organised for a particular purpose, activity or function, including frameworks, structures, systems and methods.

16 Ethical and responsible use of technology and information

16.1 The NWU has clear standard operating procedures and arrangements for liaison with the press and broadcasting media;

16.2 The NWU has clear policies and standard operating procedures relating to social media;

16.3 The NWU has clear procedures and arrangements for handling enquiries from students and the public.

17 Digital transformation[28]

17.1 The NWU explores digital technologies to create new, or modify existing business processes, culture, and customer experiences to meet changing business and market requirements.

17.2 The NWU develops and maintains policies and standard operating procedures which:

- Emphasise the importance of digitisation;
- Set standards for digitising information;
- Manage digitisation at the NWU.

18 Monitoring risk, compliance and effectiveness

18.1 Disaster recovery, contingency and business continuity

18.1.1 The NWU implements adequate business continuity through clear policies and standard operating procedures in the event of a disaster.

18.1.2 The relevant contingency plans (preventative and proactive) and backup strategies are developed and implemented.

18.1.3 Business continuity is addressed in relevant NWU procedures in order to indicate per business activity/process what measures will be put in place to ensure business continuity.

18.2 Quality assurance

18.2.1 The NWU establishes and maintains policies and procedures to ensure and improve the quality of information and assessing and minimising risks to the University.

18.2.2 The NWU undertakes or commissions annual assessments and audits of its information quality and records management arrangements;

18.2.3 All managers are expected to take ownership of, and seek to improve, the quality of information within their respective services;

18.2.4 Wherever possible, information quality should be assured at the point of collection/generation;

18.2.5 Data standards will be set through the clear consistent definition of data items, in accordance with international/national standards.

19 Environment sustainability and performance

The NWU ensures that an appropriate environmental management system is implemented effectively to:

19.1 Identify the University's adverse and positive environmental impacts with particular emphasis on the University's direct and indirect impacts on waste and pollution, resource efficiency and climate change in accordance to relevant legislation.

19.2 Recognise the University's costs and opportunities of its identified environmental risks.

19.3 Develop an *Environmental Policy* that is relevant and achievable in both the short and long term and which inculcates its environmental values.

19.4 Consider the environmental aspects and significant impacts of IT and IT activities in terms of energy-saving, avoidance of wasteful expenditure and other green IT initiatives that should be aligned with the NWU strategy and its social responsibility programme.

[28] This reimagining of business in the digital age.

19.5 Develop initiatives and awareness programs to sensitise and educate the NWU community on environmental impact.

20 Training and support

20.1 The implementation of and continued adherence to the framework and associated policies are supported by an awareness and training programme.

20.2 IG training, including awareness and understanding of IG policies, principles, confidentiality, information security and data protection, will be mandatory for all staff members.

20.3 All newly appointed NWU staff members are expected to complete mandatory information governance and management training when commencing service at the NWU in order to acquaint new employees to relevant information governance matters.

21 Communication

21.1 This framework, upon approval by the NWU Council, will be available on the NWU website.

21.2 All related policies and procedures will be distributed to staff members via the NWU intranet.

21.3 Amendments and/or updates to the Information Governance framework, as well as any of the related policies or procedures will also be communicated to all staff members via e-mail communication and published on the NWU intranet.

21.4 IG newsletters will be produced regularly, including an annual update to all staff members. Newsletters will be distributed via e-mail communication and published on the NWU intranet.

22 Revision

This framework will be revised every three (3) years or as the need arises.

Original details: (11664754) P:\1. Governance\1.16 Information Governance\1.16.1_Framework\NWU Information Governance Framework.docm
3 October 2018

File reference: 1P_1.16.1