NWU INFORMATION STRATEGY AND FRAMEWORK FOR INFORMATION GOVERNANCE

Reference number	1P_1.16.1
Accountable executive manager	Registrar
Policy Administrator	Director: Corporate and Information Governance Services
Responsible division	Office of the Registrar
Status	Approved
Approved by	Council
Date of approval	19 March 2020
Date of amendments	17 June 2021
Review date	June 2024

Office of the Registrar

NWU INFORMATION STRATEGY AND FRAMEWORK FOR INFORMATION GOVERNANCE

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.

1 The information strategy of the NWU

The university views the information that is generated through its knowledge-creation and business operations as an indispensable strategic asset and enabler to improve operational effectiveness and efficiency, and to ensure a competitive advantage.

Therefore

1. the information provided by the NWU is of high quality, accurate and relevant, accessible and supported by appropriate technical and administrative systems;
2. information sharing and reuse of information from a single and authoritative data source contributes to data integrity;
3. the ownership of and responsibility for types of NWU information is clearly defined in order to ensure optimal security, protection as well as compliance to the relevant legal frameworks; and
4. an information-management framework is implemented that is undergirded by optimal support so as to ensure positive user experience

2 Framework for information governance

2.1 NWU statement on information governance

1. Against the background of the Gartner[1] definition of information governance being "the specification of decision rights and an accountability framework to ensure appropriate behaviour in the valuation, creation, storage, use, archiving and deletion of information", the NWU views information governance as an overarching framework for oversight of information and the processes by which it is generated, processed, and curated at the university.
2. Information governance at the NWU: -
   - is implemented as a strategic, top-down approach to oversee 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;
   - encompasses all information, regardless of its format and includes structured information such as databases and unstructured information such as documents and e-mails.
   - is a subset of corporate governance, viewed as a strategic rather than tactical area, which aligns information management with business strategy and processes.

[1] URL: https://www.gartner.com/en/information-technology/glossary/information-governance [Accessed 2020.10.30]

2.2 Definitions relevant to the implementation of the information governance framework

In this framework and in policies and related documents emanating from this framework–

"**Architecture**" means the arranging of information in a way that is easy to understand in order for stakeholders to share and access information.

"**Bring your own device (BYOD)**" 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.

"Cybersecurity" refers to the body of technologies, processes, and practices designed to protect networks, devices, programmes, and data from attack, damage, or unauthorized access.

"Data Governance" is the process of managing the availability, integrity and security of the data in enterprise systems, based on internal data standards and policies that also control data usage.

Data Science is an inter-disciplinary field that uses scientific methods, processes, algorithms and systems to extract knowledge and insights from many structural and unstructured data. **"**

"**Data**" means a set of facts, descriptors and values that relates to people, objects, systems, processes, etc. 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.

"**Digital transformation**" is the reimaging of business in the digital age.

"**Discovery**" is the process of identifying data for evidence that maybe relevant to a litigation matter, regulatory notice or other formal inquiries.

"**Disposal of information**" means 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.

"**Documents**" means pieces of written, printed or electronic matter that provides information or evidence or that serves as an official record.

"E-mail management" involves the systematic control of the quality and quantity of electronic messages that are sent from within and received by an organisation.

"Information governance" is policy-based control of information to meet all legal, regulatory, risk and business demands.

"**Information management**" means 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.

"**Information security**" means the protection of data and information from unauthorised access to avoid data breaches, identity theft and to protect privacy.

"Knowledge Management" is the process of creating, sharing, utilising and managing the knowledge and information of an organization with a view to maximise its value.

"Metadata: describes described data, i.e. it summarises basic information about data, ensuring that finding and working with data is easier.

"**Personal information**" also referred to as personally identifiable information, including opinions about identifiable persons. For example, name, contact details and e-mail addresses of individuals are each likely to be personal information.

"**Principles**" means the vehicle to translate the desired behaviour into practical guidance for day-to-day management.

"Privacy management" refers to the legal obligation of the university to protect personally identifiable information.

"Records management" refers to the activities required to provide evidence of business activities and processes.

"**Records**" refers to anything that are produced due to the undertaking of a business activity or legislative requirement and is evidence of the fact that a process took place in support of the activity or requirement.

"**Risk and Compliance**" monitors and audits enterprise risks and compliance to in order to account for the uncertainties and consequences of possible events; also the process of measuring adherence to laws, regulations, policies, standards and procedures.

"**Structured information**" means information that is already structured in fields such as "date", "title", subjected", and can be identified by metadata tags.

"**Unstructured information**" means information that does not have a pre-defined information model or is organised in a pre-determined manner.

2.3 Purpose and scope of the information governance framework

1. The purpose of the framework is to indicate the conditions under which the value of information for the NWU would be maximised, while (i) complying with relevant regulatory requirements, (ii) aiming to meet the University's business demands, and (iii) striving to adhere to and implement international best practice.
2. The framework establishes oversight of and guidance in the creation, use and management of the NWU's information assets. It provides oversight of 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
3. In pursuit of the NWU's information strategy, information generated by the University is regarded as a vital asset, and the framework is created to:

3.1. Implement information management in a fully integrated way, with the understanding that business value in regard to information assets is created in the relevant business-process or line-management environment; also indicating that the relevant line manager takes responsibility for the management of risks and related matters within the relevant line function.

3.2. Ensure accountability of all staff and students 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;

3.3. State principles to guide the establishment of procedures for the management of information in the complete information lifecycle, as it is shared with all relevant stakeholders, partners and suppliers; and

3.4. Provide the framework for the integration and alignment of procedures in regard to the management of all paper, as well as electronic information and their associated systems within and outside the institution.

4. This framework determines the following:

4.1. Stakeholder needs are considered to determine balanced, agreed-upon university objectives, which are to be achieved through the acquisition and management of information resources;

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

4.3. Performance and compliance of information resources are monitored against agreed-on direction and objectives;

4.4. Clear roles and responsibilities for information management and security are in place, supported by robust policies and procedures, including a framework aimed at protecting university information against (i) unauthorised access/use, (ii) compromise of assets and (iii) interruption of university activities;

4.5. Information procedures comply with the relevant legislation;

4.6. The university complies with the principles of good corporate governance as identified in the King IV Report on Corporate Governance;

4.7. Information risks are assessed appropriately;

4.8. Appropriate training is available to all staff members;

4.9. Arrangements are in place for, and learning from information-related incidents such as data breaches or losses;

4.10. Adequate and appropriate records are maintained and the sharing of information is carried out in an appropriate manner and

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

2.4 Principles that guide information governance

The NWU is committed to the principles set out in this framework and recognises the need for an appropriate balance between transparency and confidentiality in the management and use of its information assets.

Therefore, the University subscribes to the following principles to guide the University's information governance project:

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.
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.
3. The *integrity* of records and information generated and held at the NWU shall have a reasonable and suitable guarantee of authenticity and reliability.
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. The programme shall ensure *compliance* with applicable laws and all other binding directives, including relevant university policies.
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.
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
8. The university provides for secure and appropriate *destruction and archiving* of records.
9. Regarding 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.
10. It is the *responsibility of all staff and students* to ensure and promote the quality of information and to use information in decision-making processes actively.
11. Any *breaches* of the stated principles in this framework should be reported in writing to the information officer or his deputy.
12. *Failure to adhere* to the principles may result in disciplinary action for staff and students in accordance with relevant legislation and policies.

2.5 Roles and responsibilities

2.5.1 Information officer

1. In accordance with Section 55 of the Promotion of Access to Information Act (2 of 2000) and Section 4 of the Protection of Personal Information Regulations (2017), the information officer of the university is the Vice-Chancellor.
2. In terms of Section 17 of the Protection of Personal Information Act (4 of 2013), stating that the information officer must designate a deputy information officer to ensure that all the necessary duties are fulfilled, a delegation was made to the Registrar.
3. The information officer and his/her deputy/deputies have the overall responsibility for information governance within the NWU by ensuring that appropriate mechanisms are in place to support service delivery and that information is used appropriately and securely.

2.5.2 Governance

In accordance with the Higher Education Act (101/1997) and the NWU Statute, the Council, through the advice of the ***Technology and Information Governance Committee*** 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:

1. The leveraging of information to sustain and enhance the university's intellectual capital.
2. An information architecture that supports confidentiality, integrity and availability of information.

3. The protection of privacy of personal information
4. The protection of the university's reputation.
5. The continual monitoring of information security.
6. Consider risk factors in both the external and internal business environments and continually monitor significant risk.
7. Ensuring the reporting to the DHET in the annual integrated report.

2.5.3 Management

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.
2. The UMC oversees the integration of the 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.
3. 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.

2.5.4 The Information Management Committee

The mandate of the Information Management Committee as a sub-committee of the UMC is to advise the UMC on the implementation of policies relevant to information management and the monitoring of information management matters at the university.

2.5.5 Employees

1. In accordance with the integrated information-management approach referred to above, the 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 are applying the policies and procedures in respect of information governance in carrying out their day-to-day work.
   - Information risks are mitigated;
   - Security authorisation of information is implemented; and
   - All staff attend the relevant training sessions related to Information management.
2. Any employee who creates, stores, shares and disposes of information has a responsibility to adhere to the relevant information governance and management standards, policies and procedures as implemented by the University.

2.5.6 NWU students

Any student who creates, stores, shares and disposes of information the responsibility to adhere to the relevant information governance and management standards, policies and procedures implemented by the University.

2.6 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, that are relevant to information governance to be in force:

- Information Security policy
- Records Management policy, incl. retention and disposal schedules i.e. NWU File Plan and Disposal Schedule
- Information and Data Privacy policy (incl. data security and confidentiality)
- ICT policy
- Information Sharing policy (incl. processing by and sharing with third parties)
- Digitisation policy

- Bring your own device policy (incl. information and data needs in remote-working environments)
- E-mail management policy
- Data storage and storage devices policy
- Social media policy

2.7 Implementation procedures

Procedures such as the following should 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 back-up and disaster recovery
- Managing personal information
- Collaboration and sharing information

2.8 Steering

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

- NWU Statute (8 May 2020)
- The Constitution of the Republic of South Africa, 1996
- Higher Education Act, 101, 1997
- King IV Report on Corporate Governance™, 2016
- Consumer Protection Act, Act, 68 of 2008
- Protection of Personal Information, 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, 25 of 2002
- Regulation of Interception of Communication Act, 70 of 2002
- Financial Intelligence Centre Act 38 of 2001
- Banks Act, 94 of 1990
- Compensation for Occupational Injuries and Diseases Act, 130 of 1993
- Occupational Health and Safety Act, 85 of 1993
- Basic Conditions of Employment Act, 75 of 1997
- Employment Equity Act, 55 of 1998

- Labour Relations Act, 66 of 1995
- Unemployment Insurance Act, 63 of 2002
- Income tax Act, 58 of 1962
- Tax Administration Act, 28 of 2011
- Value Added Tax Act, 89 of 1991
- Public Finance Management Act, 1 of 1999
- Health Act, 63 of 1977
- National Archives and Records Services Act, 43 of 1996
- National Payment Systems Act, 78 of 1998
- Skills Development Act, 97 of 1998
- Copyright Act of 1978
- Relevant ISO standards, amongst others, ITIL, TOGAF, COBIT, Val IT, ISO/IEC 20000, ISO/IEC 27002 (formerly 17799), ISO/IEC 38500, ISO 9002, ISO/15489

2.9 Strategies and plans

1. In accordance with the NWU's information strategy, all data, information and knowledge created by members of the University, are viewed as a strategic asset that needs to be governed and managed in careful and accountable ways.
2. This framework should be read in conjunction with, but not limited to strategic documents such as the following:
    - NWU Strategy 2015-2025
    - Information Technology Strategy
    - Digital Business Strategy
    - Teaching-Learning Strategy
    - Five-year strategy and annual performance plans

3 Information management

3.1 Point of departure

1. The NWU ensures the implementation of information management practices that support good decision-making, integrity, accountability and transparency which are essential to delivering good business outcomes.
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.
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 and students
4. Information management creates value and ensures that the statutory and regulatory requirements can be maintained at all times.

3.2 Information architecture

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.
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.

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.
4. This NWU File plan and Disposal Schedule apply to all documents and records as well as Electronically Stored Information (ESI) - along with the relevant metadata, confidentiality, and other issues associated with ESI.

3.3 Records Management

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.
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.
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
- Discovery processes.

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;
- Define Records management's role in legal and regulatory compliance.

3.4 Information security management

3.4.1 Physical security

The NWU has measures and procedures in place to protect information on equipment and premises from unauthorised physical interaction through measures that can be seen or touched, such as:

1. Keeping filing cabinets locked	2. Shredding paper records	3. Locking office doors
4. Implementing access control using key cards or biometrics	5. Utilising reactive and live CCTV systems and video surveillance	6. Hiring security personnel
7. Fire alarms	8. Temperature monitoring alarm systems	9. Office alarm systems
10. Deployment of security staff		

3.4.2 Digital security

The NWU has measures and procedures in place to ensure diligence in the protection of information on systems and networks from unauthorised electronic interaction through electronic and digital measures, such as:

1. Effective password management	2. Anti-virus software	3. Up-to-date Software
4. Ensuring firewalls	5. Encrypting hard drives, files, and e-mails	6. Managing mobile devices
7. Hiring cybersecurity experts to conduct penetration testing		

3.4.3 Operational security

The NWU has measures and procedures in place to protect information from operational risks from within the university by means of programmes, actions and routine functions and operations, such as:

1. Fostering a culture of security	2. Adding communication messages when staff login to the NWU network	3. IT providing in-house staff training and awareness regarding security
4. Providing external staff training	5. IT monitoring workstations of staff in the background to ensure correct application of policies and procedures	6. Implementing employee on-boarding and exit procedures

3.4.4 Administrative security

1. The NWU has measures and procedures in place to protect information from business risks external to the university by means of programmes, actions and routine functions and operations, such as:

1. Providing awareness training about business risks	2. Planning around security	3. Drafting privacy, incident response, and information security policies
4. Conducting due diligence of subcontractors	5. Implementing audit controls	6. Business continuity planning

2. The NWU establishes and maintains policies for the effective and secure management of its information assets and resources;
3. The NWU undertakes or commissions annual assessments and audits of its information and IT security arrangements;
4. The NWU promotes effective confidentiality and security practice to its staff members through policies, procedures and training;
5. 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.

3.5 Architecture

3.5.1 Information architecture

1. The NWU implements a structural design of information environments to ensure that in NWU information being organised and classified in such a way that it is easily retrievable in accordance with the university's main business activities and related business processes.
2. This classification will apply to all paper and electronic records in any format or medium, along with the relevant metadata and confidentiality.

3.5.2 Information technology architecture

The NWU:

1. Designs, develops, implements and evaluates the IT-technologies and resources that provide points of access to university information, sharing, collecting and the retention thereof.

2. Ensures that the information technology architecture must fit and support internal technologies and processes to be an effective part of the university

3.6 Data storage and storage devices

The NWU develops and maintains policies and procedures to:

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.
2. Manage physical storage areas.

3.7 Information management in remote-working environments

1. The NWU develops and maintains policies and procedures to manage the manner how staff should manage information when working remotely.
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.
3. Employees need to be extremely careful when doing work in public places, working on public Wi-Fi.

3.8 Bring your own device (BYOD)

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

1. manage how information is going to be kept secure when staff members use a personal device for official university business.
2. manage the higher risks for the university in terms of confidentiality and the potential loss of employee and university privacy.
3. establish a register of users that use a personal device for official university business.

3.9 Metadata Management

The NWU develops and maintains policies and procedures which:

1. Indicate how metadata should be applied and managed on all pieces of information;
2. Set minimum standards for metadata requirements.

3.10 E-mail management

The NWU develops and maintains policies and procedures which:

1. Ensure data protection though the management of e-mail as information resources;
2. Provide standards to all staff on the management of e-mails.

3.11 Privacy management

3.11.1 Protection of personal information

1. The NWU recognises the need for the ongoing management of information to ensure that it results in the protection of personal information;
2. The NWU will establish and maintain policies to ensure compliance with the *Protection of Personal Information Act 4 of 2013* (POPIA);
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.
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.
5. Students should have complete access to their personal information relating to their own studies.
6. The NWU will have clear procedures and arrangements regarding the lawful processing of information in a reasonable manner that does not infringe the privacy of all stakeholders.
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;

8. The NWU regards all personally identifiable information relating to students and staff as confidential except where legislation and/or policy requires otherwise;
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;
10. The Compliance Office will undertake or commission annual assessments and audits for its compliance with legal requirements;
11. Availability of information for operational purposes will be maintained within set parameters relating to its importance via appropriate procedures and computer system resilience.

3.12 Ethical and responsible use of technology and information

1. The NWU will ensure that all staff and students take responsibility for the ethical use of technology and information.

2. The ethical use of information will be guided by clear policies and standard operating procedures.

4 Digital transformation

1. In pursuit of its digital business strategy, the NWU explores digital technologies to create new, or modify existing business processes, culture, and customer experiences to meet changing business and market requirements.
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.

5 Monitoring risk, compliance and effectiveness

5.1 Disaster recovery, contingency and business continuity

1. The NWU implements adequate business continuity through clear policies and standard operating procedures in the event of a disaster.
2. The relevant contingency plans (preventative and proactive) and backup strategies are developed and implemented.
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.

5.2 Quality assurance

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.
2. The NWU undertakes or commissions annual assessments and audits of its information quality and records management arrangements;
3. All managers are expected to take ownership of, and seek to improve, the quality of information within their respective services;
4. Wherever possible, information quality should be assured at the point of collection/generation; and
5. Data standards are set through clear consistent definition of data items, in accordance with international/national standards.

6 Environmental sustainability

1. The NWU subscribes to the principles and practices of environmental sustainability and puts in place the relevant measures to ensure that its information governance and -management practices are aligned to best-practice principles.

7 Training and support

1. The implementation of and continued adherence to the framework and associated policies are supported by an awareness and training programme.
2. IG training, including awareness and understanding of IG policies, principles, confidentiality, information security and data protection will be mandatory for all staff members.
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.

8 Communication

1. This Information Governance Framework, as approved by the NWU Council, is published on the NWU website.
2. All related policies and procedures are published on the NWU intranet.
3. Newsletters relevant to information governance and management will be produced regularly, including an annual update to all staff members. Newsletters will be published on the NWU intranet.

9 Revision

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

Original details: (11664754) P:\Policies\2021\1P_1.16.1\NWU Information Governance Framework.docm
6 July 2021

File reference: 1P_1.16.1_2021