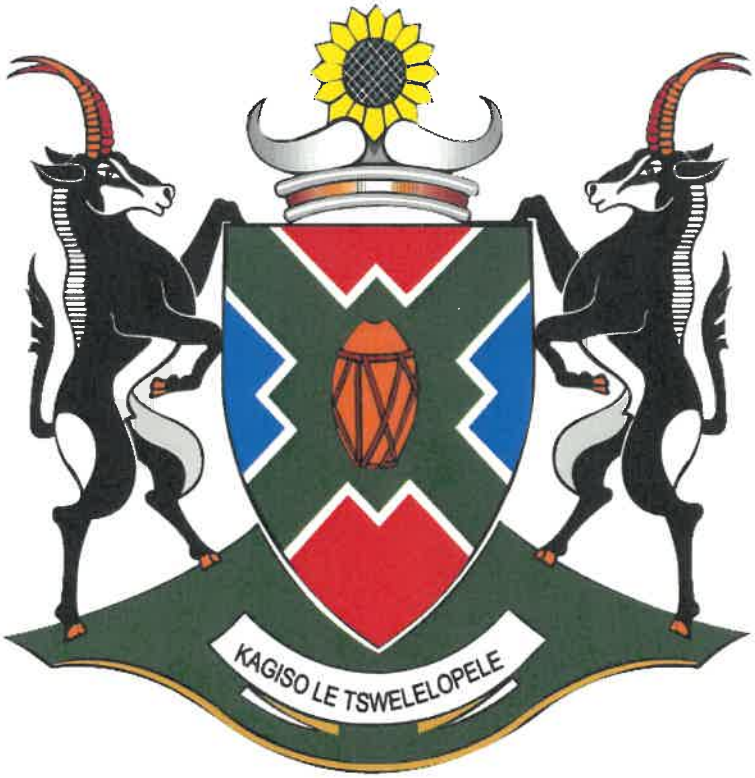
DEPARTMENT OF COMMUNITY SAFETY AND TRANSPORT MANAGEMENT



INFORMATION COMMUNICATION AND TECHNOLOGY SECURITY POLICY

(ICTSP-VERSION 1.4)

Document Details

Author	Directorate Strategic Support Services
Department	Community Safety and Transport Management
Division Name	ICT Management
Document Name	Information Communication Technology Security Policy
Sensitivity	Internal Use Only
Effective Date	<Date of Accounting Officer's signature>
Created Date	01-04-2013
Version Date	<Date of Accounting Officer's signature>
Version	ICTSP-VERSION 1.4

Change Record

Modified Date	Author	Version	Description of Changes
26-11-2012	Directorate Strategic Support Services	1	Original Security Document
01–04 -2013	Directorate Strategic Support Services	1	Compliance to DPSA requirements
26-09-2014	Directorate Strategic Support Services	1.1	Departmental Business Change
31-03-2016	Directorate Strategic Support Services	1.2	Annual Review
31-03-2018	Directorate Strategic Support Services	1.3	Annual Review
	Directorate Strategic Support Services	1.4	Review

Stakeholder Sign–Off

Name	Position	Signature	Date
Mr S. Matlhako	Departmental Information Technology Officer		03/06/2021
Ms K. Phatudi	Governance Champion		25/05/2021
Ms F. Nchoe	Chairperson: ICT Steering Committee		01/06/2021
Ms M. Dayel	Chairperson: ICT Strategic Committee		03/06/21
Ms M.G. Mothibedi	Departmental Chief Risk Officer		03/06/2021
Mr P. Namate	Director Legal Services		07/06/2021

Records Management Sign–Off

Name	Position	Signature	Date
Ms M. Malatji	Deputy Director Records		11/06/2021

TABLE OF CONTENTS

Glossary of Terms

CGICTPF	Corporate Governance of ICT Policy Framework
Contractors	A person or business which provides goods or services to the Department
Critical Information	Information is designated as critical information if its unavailability would have a catastrophic adverse impact on the following: • Client or employee life, safety, or health. • Payment to suppliers or Users. • Revenue collection. • Communications. • Legal or regulatory.
DCS&TM	Department of Community Safety and Transport Management
DITO	Department Information Technology Officer
Filr	Software by Novell used for backup and remote access of user information
HoD	Head of Department
ICT	Information Communication Technology
Information Systems	A combination of hardware, software, infrastructure and trained personnel organized to facilitate planning, control, coordination, and decision making in an organization.
Information	The study or use of systems (especially computers and

Technology(I.T.)	telecommunications) for storing, retrieving, and sending information.
ISO	International Organization for Standardization
Logical Access	user based authenticated access to application systems and the data that is processed
MISS	Minimum Information Security Standard
Mobile Devices	Mobile devices herein refer to official laptops tablets, mobile projector, mobile printers
MPSS	Minimum Physical Security Standard
NWPG	North West Provincial Government
Official devices	Items provided with permission to access the departmental resources. E.g. Desktop, Laptops etc
Remote Access	Distanced away from the NWPG server farm, Isolated network (3G e.t.c), network inaccessible areas
SACSA	Special Assistant for Counterinsurgency and Special Activities
SSA	State Security Agency
Sensitive Information	This includes any strategic information of the department, such
SLA	Service Level Agreements
Server	A software program, or the specialised computer on which that program runs, that provides a specific kind of service to client software running on the same computer or other computers on a network.
Third Parties *(Do not include AG, Internal Audit)*	Any and all stakeholders or service providers who are not employed by the department but are operating in the Departmental environment
User	Employee utilising ICT equipment

1. Preamble

Information Communication Technology (ICT) system is made up of people, hardware, software, telecommunications, facilities and data. All ICT systems entail the creation of a condition to protect computer hardware, software, and data against incidental and/or deliberate unauthorized changes, destruction, disposal, removal and disclosure. Securing the integrity, confidentiality and availability of the computers and technology systems of the department against threats such as sabotage, unauthorized intrusions, malicious misuse or inadvertent compromise is of paramount importance for the operational effectiveness of all activities of the department.

2. Purpose

The purpose of this policy is to ensure the effective protection and proper usage of the computer systems and its peripherals within the Department. Each employee of the department is responsible for the security and protection of electronic information resources over which he or she has control. Resources to be protected include but are not limited to networks, computers, software, removable media and data. The physical and logical integrity of these resources must be protected against threats such as sabotage, unauthorized intrusions, malicious misuse or inadvertent compromise.

3. Regulatory and Guidance Framework

i. Public Service Act (Proclamation No 103 of 1994)
ii. Protection of Information Act 84 of 1982
iii. Promotion of Access to Information Act 2 of 2000
iv. Protection of Personal Information Act of 2013
v. Electronic Communication and Transaction Act 25 of 2000
vi. Regulation of interception of communication and provision of communication-related information Act 70 of 2002
vii. Copyright Act 98 of 1978
viii. National Archives and Record Services of South Africa Act 43 of 1996
ix. Occupational Health and Safety Act 85 of 1993
x. Public Finance Management Act 1 of 1999 (as amended by Act 29 of 1999)

xi. State Information Technology Agency Act (No 88 of 1998 as amended by Act 38 of 2002)

xii. Minimum Information Security Standard (MISS) of 1996

xiii. Minimum Physical Security Standard

xiv. National Cyber Security Policy Framework 2012

xv. International Organisation for Standardization (ISO) 17799

xvi. International Organisation for Standardization (ISO) 27000 series

xvii. International Organisation for Standardization (ISO) 38500

xviii. Constitution of the Republic of South Africa, 1996 (Act no. 108 of 1996)

xix. Electronic Communications and Transactions A (no. 25 of 2002)

xx. Communication – related Information Act (no. 70 of 2002)

xxi. National Strategic Intelligence Act (no. 39 of 1994)

xxii. Provincial Asset Management Framework

xxiii. Corporate Governance of Information Communication Technology Policy Framework (CGICTPF)

4. Scope and Application

This ICT Security Policy is applicable to all Users in the department, third parties and contractors utilising the department's ICT resources and facilities in pursuit of the Department's Goals and Strategic Objectives.

5. Responsibilities

5.1 Head of Department

The HoD bears responsibility of overseeing the development, approval, accountability and implementation of the ICT Security Policy.

5.2 Departmental Information Technology Officer (DITO):

5.2.1 ensure the confidentiality, integrity and availability of ICT systems within the ICT environment;

5.2.2 oversee the development of the ICT policies and strategies, regulations, standards, norms, guidelines, best practices and procedures;

5.2.3 coordinate ICT Security management activities within ICT;

5.2.4 manage relationship with all stakeholders that supply Information Technology products and services, this is done by ensuring that all Business Agreements and SLAs are adhered to.

5.2.5 monitor and ensure compliance with relevant ICT regulatory framework and policies.

5.2.6 provide a holistic view of the department's current ICT security posture.

5.3 Provincial Internal Audit:

Provincial Internal Audit shall provide professional advisory services to the Departmental ICT.

5.4 ICT Security Risk Assessment

5.5 The Department shall conduct ICT Security Risk Assessment on annual basis in compliance with the *Departmental Enterprise Risk Management Policy.*Third Parties and Contractors

5.5.1 All ICT component third parties and contactors shall be screened /vetted by Security Services before provided with access to any ICT resources.

5.5.1.1 Shall sign a non-disclosure of classified information which will be provided and archived by the Security Services Component;

5.5.1.2 Shall not be provided with access to the sensitive information unless security clearance is provided to Security Services;

5.5.1.3 Service Level Agreements (SLA's) between the Department and Third parties and contractors shall be entered into in order to manage services prior to rendering services to the department.

5.5.1.4 Shall be accompanied at all times by ICT Component members when providing any services.

5.5.1.5 Shall not be provided with logical access to any critical information systems of the Department ; logical access shall be provided only with an approved authorization from HoD; *see annexure D: ICT Logical Access Authorization*

5.6 ICT Asset Management

5.6.1 All ICT equipments shall be recorded and /or tagged with an asset tag according to their classification

5.6.2 A register of all ICT Assets shall be kept containing a minimum of the following description:

(a) Value of the asset

(b) Asset owner

(c) Location of asset

(d) Date of acquisition

5.6.3 It is the responsibility of users provided with ICT equipment to ensure that such assets are protected from damage and theft;

5.6.4 It is the responsibility of users to ensure that the ICT resources allocated to them are in good working condition.

5.6.5 Users are not allowed to possess similar items performing the same function e.g. Laptop/Desktop except in circumstances that are unavoidable. In instances where the official is forced by circumstances to possess similar items performing the same function, authorization shall be granted by the Accounting Officer.

5.6.6 ICT asset(s) shall be managed in a manner which is compliant to the Departmental Asset Management Policy

5.6.7 Hard drive(s) shall be formatted prior to disposal.

5.6.8 Movement of ICT assets shall be controlled in conjunction with Asset Management and ICT, to ensure that the process is managed properly through the usage of the appropriate form i.e. *annexure B for movement of ICT asset and ICT Allocation form to declare that the computing resources received were in good working condition.*

5.6.9 In the event, the equipment is reallocated to a different user, *the ICT Reallocation Form (Annexure C)* shall be utilised to manage the process.

5.6.10 All losses to be reported to SAPS within 24 hours after acknowledgement. Subsequent to that, a report must be forwarded to Loss Control Committee through asset management office / Security Services Unit.

5.6.11 Departmental Human Resources management component shall notify the asset controller and ICT of any resignation/ /termination of employment to identify the computing resources in possession of the official and terminate or deactivate system access/ credentials.

5.6.12 Departmental Human Resources Management shall ensure that there is skills transfer plan/ succession plan for system users.

5.7 Desktop Security

5.7.1 Computing resources shall be allocated to Users based on their job requirements.

5.7.2 Users access to desktop operating systems functions shall be limited

5.7.3 Users shall ensure that they only utilise the computing resources for official work only.

5.7.4 Users shall only have logical access to their allocated desktop

5.7.5 Users are not allowed to physically open computing equipment

5.7.6 Only ICT personnel are allowed to open computing equipment. No computing equipment which is under warranty shall be opened.

5.7.7 No desktops shall be removed from Departmental premises without authorisation of Asset Management

5.8 Mobile Devices

5.8.1 Official mobile devices shall be issued to users in accordance with the SCM and ICT policies.

5.8.2 Securing of mobile devices is the sole responsibility of the employee issued with such a device.

5.9 Removable Devices

Removable devices herein refers to USB Flash Drives, Compact and DVD discs, external Hard-drive, HDMI and any other removable media storage devices.

5.9.1 Official removable devices are defined as documents as stipulated in the MISS and the Protection of Information Act 85 of 1985

5.9.2 Shall be issued to Users according to their job demand

5.9.3 All removable devices shall be requested from Supply Chain Management Directorate.

5.9.4 Official removable devices shall be locked away in accordance with the ICT Security Policy and MISS.

5.9.5 Any loss of Removable devices shall be reported to the Departmental Loss Control Committee and to the Asset Management / Security Services

5.10 Network Security

5.10.1 Only official desktop and mobile devices shall be connected to the NWPG network.

5.10.2 The Department shall not implement any wireless network without consulting the Provincial ICT; should IT manager fail to comply he/she will be held accountable on any security breach that may occur on such wireless network.

5.10.3 The Department shall be provided with network security procedures and guidelines by Provincial ICT.

5.11 Vulnerability Assessment

Vulnerability assessment is the responsibility Provincial ICT as the custodian of the network infrastructure.

5.12 Logical Access

The approved ICT user account management policy is in place to ensure protection of data in the departmental information systems and to regulate access to Departmental Systems. Access to Departmental virtual meeting shall be granted to officials who appear in the list of participants only.

5.12.1 Password Management

5.12.1.1 Password Construction

- Password should be seven (7) to twelve characters in length;
- Passwords must not consist of repeated character strings (eg. Odu1111);
- Passwords must not consist of sequential numbers or characters (e.g 123456);
- Passwords must be alphanumeric ;
- Users must be discouraged from using default passwords;
- Passwords must not mirror the corresponding user id;
- Password must be changed frequently, at least every ninety (90) days.

5.12.1.2 Password rules

- Passwords must be kept a secret;
- Do not write down your password, particularly anywhere near your computer or file it in a box file with the word "password" written on it;

- Do not tell or give out your passwords to other people, even for a very good reason.
- Do not display your password on the monitor.
- Do not send your password via email.
- Avoid using the "remember my password" feature associated with some websites, and disable this feature in your browser software. Always click on "Don't remember my password".
- Do not store your password on any media unless it is protected from unauthorised access (e.g. encrypted with an approved encryption method).When the user discover that his/her password has been used to access the system, the incident must be treated as a security violation and should be reported to Strategic Support Services immediately;Change your password immediately if you believe that it has been compromised. Once done, notify the system/security administrator for follow up.

5.12.1.3 Password Administration

- Old passwords must not be displayed at the time of typing the new password;
- System Administrator must be able to revoke passwords;
- Default passwords must have an enforced change on first use (temporary password has to be changed on the first log on);
- User account shall be locked-out after three (3) invalid access attempts;
- "Annexure D" shall be completed by the affected user and authorisation shall be granted by the Head of Department for the System Administrator to reset password or UserId;
- Re-use of previous passwords must not be allowed

5.12.2 Remote Access

5.12.2.1 Remote Access to Business Application systems is prohibited, unless authorised by the manager of the respective system;

5.12.2.2 The following are approved network resources that will be allowed to be accessed utilising the internet:

(a) Remedy Online

(b) GroupWise

(c) Business related research

5.12.3 Internet and Email

5.12.3.1 Email shall be accessed by utilising login credentials

5.12.3.2 Internet and Email access granted to Users shall not be abused and shall be utilised for work purposes only

5.12.3.3 Uploading government information in free cloud services is prohibited

5.12.3.4 Downloading of pirated and unlicensed software installation and files is prohibited and Users caught doing so shall be dealt with in accordance with disciplinary code of conduct

5.12.3.5 Users shall sign Acceptable Usage of Internet and Email form

5.12.3.6 The above shall be in accordance with the provincial Internet and Email policy

5.12.4 All Business Application Systems (Transversal and Non--Transversal)

5.12.4.1 Only approved Users shall be provided with logical access to these systems

5.12.4.2 Access to all Application Systems shall be monitored to ensure that passwords are changed regularly. **See 5.12.1.1**

5.12.4.3 Roles and responsibilities of system users shall be monitored by the System Administrator to ensure segregation of duties.

5.12.4.4 All systems breaches realised shall be reported to the Systems Administrator and Security Services for investigation.

5.12.4.5 All systems policies and procedures shall be reviewed regularly by System Administrators, Users and/or ICT management.

5.12.4.6 All ICT systems shall be reviewed by System Administrator(s) and /or ICT management

5.12.4.7 Request for access to any Departmental Application system within the control and accountability of Departmental ICT component shall be made through Annexure D: Logical Access Form.

5.12.5 Malicious Software

5.12.5.1 Malicious software, for the purpose of this document, refers to Virus, Trojans, Worms and Spyware.

5.12.5.2 It shall be ensured that Antivirus installed in systems is setup to scan desktops and mobile devices daily

5.12.5.3 Knowledge base system will be utilised in order to keep record of types of Malwares the department has faced

5.12.5.4 Users are prohibited from installing unauthorised software

5.12.6 Firewalls and Antivirus

- The Strategic Support Services shall ensure the activation of an effective desktop firewall and install anti-virus for the department
- It is the responsibility of Provincial IT to ensure the implementation of an effective network firewall and virus security strategy for the department.
- It is the responsibility of the Strategic Support Services to ensure that the latest version of antivirus software is installed on all computers.

- Remote users and users of portable computers should ensure that computers are plugged into Departments network at least twice a week for antivirus updates.
- Users should not disable or interfere with the firewall status and the virus scanning software
- Users are responsible for scanning all media (e.g. memory sticks, CDs, external hard drives) before use. Assistance can be requested from an IT technician(s) where necessary.
- Upon the detection of a virus, Users should notify the ICT section for assistance immediately.
- In cases of anti-virus license renewal delay by SITA and NWPG, the department shall install unlicensed / free software to ensure computers are protected from cyber attacks, viruses etc.

5.13 Incident Management

5.13.1 All the departmental ICT faults shall be reported to Provincial ICT Helpdesk.

5.13.2 Remedy System will be the tool used for logging ICT incidents

5.13.3 ICT incidents shall be prioritized according to the impact they have on the continuity of functions in the department and critical systems

5.13.4 ICT Services and Standard manual was developed and implemented.

5.14 Information System Acquisition, Development And Maintenance

5.14.1 All Information system acquisition shall be procured in line with the Suply Chain Management procurement prescripts and SITA contracts

5.14.2 Failure to procure information systems without following the Supply Chain Management procurement prescripts and SITA contracts shall constitute non-compliance.

5.14.3 The interest of the department in the ownership of the developed system and data should clearly be stated in the relevant contract.

5.14.4 Skills transfer of the development of the Information System shall also form part of the contract

5.14.5 All the developed applications should be audited to ensure that they fulfil the functions for which they were developed for.

6 ICT Disaster Recovery Plan

6.1 Information Backups

- To a certain limit, Departmental information/data shall be regularly backed up on the Server.
- Strategic Support Services shall facilitate the implementation of automated back up system with Provincial IT as back up mechanism for IT systems in the Department.
- Only work related information will be backed up on the server.
- It is the responsibility of Users of Laptops to ensure that Laptops are connected to the network on regular basis in order to backup information/data.
- Where need arises, the Supply Chain Management shall provide officials with removable devices for the storage of work related information.

6.2 Backup of DCSTM servers

- Backups of the systems database shall be done weekly on the Server via an automated process available in the operating system.
- Access to backups must be done in writing, signed and approved by the Head of Department.
- Log files to be maintained on server confirming backup.
- Bi-Monthly backups of the database and log files will be done
- Backups shall be done weekly and stored in a secure location by the System Administrator.
- A register for the maintenance and management of backups to be maintained. Register will include the following:
    - Identification of Backup (servername_YYYY/MM/DD).
    - Name of official who made the backup, Signature and Date,
    - verification of backup(Name of Official, Signature and Date),

- Random / Scheduled testing and restore of selected backup (Name of Official, Signature and Date, comment = successful or not),
- Provision for Monthly Sign off of Register By Programme Manager or delegated Official
- Testing of backups will be done monthly by departmental system administrators.
- Backup shall be stored in a secured offsite place by the System Administrator(s).

7 ICT Continuity Plan

7.1 ICT Continuity Plan shall be developed in line with the departmental Business Continuity Plan

7.2 Shall identify critical business information systems that should be prioritised

7.3 ICT Continuity plan shall be endorsed by the Departmental ICT committees.

7.4 Shall provide with details of alternative ICT Data centre to continue providing ICT services to the department

7.5 Shall provide estimated time to recover all systems to be back online

8 Security Awareness

8.1 Strategic Support Services directorate in conjunction with Security Services shall conduct Security awareness campaigns.

8.2 A security awareness plan shall be developed by both Strategic Support Services and Security Services

8.3 The awareness program shall make departmental users aware of internal security policies

8.4 Security awareness could either be presented in a form of face to face engagement, posters, newsletters or utilising the intranet and emails.

8.5 All directorates shall attend security awareness presentations when invited, failure to attend such awareness shall result in non-compliance to this policy.

9 Compliance

Any disciplinary action arising from non-compliance witth this policy, procedures and guidelines shall be dealt with in accordance with Public Service Disciplinary Procedure.

10 Review

This policy shall be reviewed after a period of three (3) years or as and when there is a major change.

11 Recommended/ ~~Not Recommended~~

Applicable protocols for policy compliance be complied with.

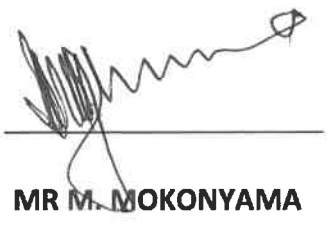
15/04/2021

MS B. MOFOKENG **DATE**

HEAD OF DEPARTMENT

12 Approval

This policy is agreed to by the Accounting Officer.



30/04/2021

MR M. MOKONYAMA **DATE**

ACCOUNTING OFFICER

Annexure A

ICT SECURITY POLICY DECLARATION FORM

I, (name and surname) _____ of (Persal no) _____ have read the Departmental ICT Security policy and I fully understand the terms and conditions and agree to abide by it.

The sharing, disclosure of passwords is an offence in terms of Section 3 and 4 of the Protection of Information Act. As the user / applicant, I understand and will refrain from engaging in any practices that could jeopardise the security of any Government system. I am accountable and fully responsible for ensuring that my user password is changed on a quarterly basis, this includes immediately on receipt of my NEW USER ID, to change my default password.

I understand that any violation of this policy may lead to me being liable for the cost of damage or theft of any ICT equipment in my possession. I therefore undertake to take proper care of any Departmental ICT equipment, software, data or peripheral(s) allocated to me.

_____ _____

Signature of User Date

_____

ICT Unit staff member (as Witness)

ICT ASSET MOVEMENT FORM

ANNEXURE B

Purpose of Movement:

Current Location / User information		New Location / User Information	
Office Number		Office Number	
Name of building		Name of building	
Head/Regional/District Office		Head/Regional/District Office	
Asset User		Asset User	
Asset Controller		Asset Controller	

No	Asset Bar Code #	Room Bar Code #	Asset serial Number	Asset Description	Condition of Asset
1.					
2.					
3.					
4.					
5.					
6.					
7.					
8.					
9.					
10.					

Movement of ICT Assets Sign Off			
Designation	Name	Signature	Date
Asset Holder			
Asset Receiver			

Department Stamp

ICT ASSET REALLOCATION FORM

ANNEXURE C

REASON FOR REALLOCATION:

Current user Information		New User Information	
Initials & Surname		**Initials & Surname**	
Office Number		**Office Number**	
Name of the building		**Name of the building**	
Head/Regional/ District Office		**Head/Regional/ District Office**	
ICT Technician		**ICT Technician**	
Contacts		**Contacts**	

No	Asset Bar Code #	Asset Serial #	Asset Description	Condition of Asset
1.				
2.				
3.				
4.				
5.				
6.				
7.				
8.				

Movement of ICT Assets Sign Off			
Designation	**Name**	**Signature**	**Date**
Asset Holder (Old)			
Asset Receiver (New)			
IT Technician			

dcstm
Department:
Community Safety and Transport Management
North West Provincial Government
REPUBLIC OF SOUTH AFRICA

ICT LOGICAL ACCESS AUTHORIZATION FORM

ANNEXURE D

Applicant's Personal Details	
First Name	
Surname	
ID No.	
Email	
Phone Number	
Fax Number	
Company / Department	
Section	
Location	
User ID/Persal No	

Please Tick where applicable:

New User ID		Reset User ID		Reset Password		Request for Reports		Remove System Access	
Specify Application:			Specify Application:			Specify reports:		Specify Location:	

If not listed above, kindly describe your request in detail, e.g. Access to specific server and folder:

Please sign below:

Applicant:

Signature: _____ Date: _____

Duly Authorised by Accounting Officer/delegated:

Initials: ____ Surname: _____

Tel: _____

Signature: _____ Date: _____

Department Stamp

"Together We Move North West Forward"