HEDDLU
GOGLEDD CYMRU
NORTH WALES
POLICE

Response Date:27/06/2025

2025/658 - Security procedures

In response to your recent request for information regarding;

Please could I request the "security procedures" or "SyOps" as it may be termed for users using these systems.

Email/Internet

North Wales Police does not have any SyOPs for email/internet however we have the email and network drive policy and internet policy which details the use of either email and internet.

Records Management System RMS

Please see the attached draft RMS (WCC) SyOPS.

This document has been redacted to remove any personal data under Section 40 (2).

Therefore, in accordance with the Freedom of Information Act 2000, this letter acts as a Refusal Notice under section 17 (1) of the legislation.

Single User Log On (SULO)

North Wales Police does not have SyOPs for SULO.

THIS INFORMATION HAS BEEN PROVIDED IN RESPONSE TO A REQUEST
UNDER THE FREEDOM OF INFORMATION ACT 2000, AND IS CORRECT AS AT 25/06/2025

West Coast Collaboration
Working together and sharing information to keep our communities safe

West Coast Collaboration
Niche RMS

Generic SyOPs for Users and Administrators

Version: Version 2.0
Date: 28/02/2021

Amendment History

Issue	Date	Description of Change	Issued by
1.0, draft 4	25/5/2017	Based on the Niche RMS SyOps produced by Dave Binns, Merseyside Police.	…
1.0, version	21/6/2017	Addresses feedback from Security and Data Protection Group	…
1.1 Version	20/10/17	Review by TFN InfoSec Working Group	…
2.0	28/01/2021	Re-write of document for West Cost Collaboration	…

The purpose of this SyOps is to set out the procedures that will be followed by all staff when dealing when accessing the West Coast Collaboration Niche RMS System.

All employees will be asked to read and confirm acceptance of this document at the start of their employment, and annually thereafter.

This guide ensures that common practices are followed by all staff to ensure the security of information. This guidance only covers access to the West Coast Collaboration Niche RMS.

Failure to follow the procedures and guidance defined in this document may lead to disciplinary action being taken.

Contents

1 Personnel security

1.1 Authorisation

1.1.1 Police officers and staff

Access to the Niche RMS application will only be authorised for individuals who have:

- A legitimate business requirement for access as endorsed by their line manager
- Successfully completed a Niche RMS training course
- Received Data Protection/Information Security awareness training
- Had their identity established
- Been security vetted in accordance with their level of access to Niche RMS

1.1.2 Third-Party Users

Access to the Niche RMS application will only be authorised for individuals from third party organisations who have:

- A legitimate business requirement for access, in-line with the particular contract between the Force and third-party organisation, and endorsed by the point of contact for the individual from within the Force
- Successfully completed a Niche RMS training course
- Been security vetted in accordance with their level of access to Niche RMS
- Signed a copy of the Official Secrets Act
- Agreed to comply with partner force information security policies

1.2 Vetting

Before being provided with access to the Niche RMS application, individuals must have been security vetted to a level that is commensurate with the sensitivity of the information with which they will be dealing. The following security clearance levels are required:

Role	Minimum Vetting Requirement
Niche RMS Users (up to RESTRICTED)	NPPV2 / Recruitment Vetting
Niche RMS Users (up to CONFIDENTIAL)	NPPV3 or Management Vetting (MV)
Niche RMS System Administrator / IT Administrator	Management Vetting (MV) / NPPV3

1.3 Training and Awareness

All Niche RMS users must, before they are granted access to the Niche RMS application, have received training appropriate to their use of the system.

2 Acceptable usage

2.1 Policy and Legislation

- Users shall adhere to any legislation, national guidance for the Police Service, policy, procedures and Information Sharing Agreements (ISA) that relate to the information and services provided from the Niche RMS, e.g. Data Protection Act 1998 and the Code of Practice on the Management of Police Information (MOPI).

2.2 Access rights

- Users must not seek to obtain account privileges beyond those for which they have been authorised.
- Users must not access, or attempt to access, resources on the Niche RMS for which authorisation has not been provided.

2.3 Professionalism

- Information that is received and requires action on the part of the recipient should be dealt with professionally and in a timely manner.
- Users should not intentionally process or transmit the following content types, unless it is a function of their role, and as such is formally documented:
  - Material that is threatening, obscene, indecent, defamatory, or blasphemous
  - Malicious code including viruses
  - Spam or other junk mail, including unsolicited commercial or advertising material
  - Material that is designed or likely to cause annoyance, inconvenience or needless anxiety
  - Material that infringes copyright law
  - Material that commits the Force to an undertaking not subject to the official authorisation process
  - Material that does not represent the Force in a good light, or is a breach of any legal requirement
- The Niche RMS must only be used for purposes that have been approved (formally) by the Force. Furthermore personal use of the Niche RMS is not permitted.

3 Access to the Niche RMS

3.1.1 Access up to Standard Users

Access to the West Coast Collaboration Niche RMS requires users to enter a unique ID ‘and ‘strong’ password. Note it is acceptable to rely on the corporate ‘Single Sign-on’ solution (to ‘remember’ the password).

The password shall adhere to the following requirements:

- Have at least eight characters
- Must contain lower and capital case letters
- Must include special characters (!"$%^&*@~? >)

In addition, the password must:

- Not be word based. i.e. based on the months of the year, days of the week, people's names, the names of police forces or divisions, anything that someone else might associate with you or any dictionary based word;
- Not be the same as a password used for any other purpose;

3.1.2 Access to the Niche RMS by Administrators

Access to Tri-Force Niche RMS for administrative purposes shall be subject to a 'very strong' form of authentication based on the use of a unique ID and eleven (11) character password.

NOTE: Password strength compliance will be scrutinised in all partner forces.

3.2 Management of credentials

When a user account is first created, the Niche RMS Administrator shall set a password that is securely disseminated to the account user.

On receipt the User is required to change the password (when logging on for the first time).

Passwords must:

- Not be divulged to anyone else;
- Not be used to access Niche RMS when someone else is watching;
- Not be written down or recorded in any way.

NOTE: in order to help prevent password compromise, passwords are not displayed on screens when being entered.

3.3 Management of User Accounts

Access to Niche RMS by users shall be controlled by an administrator for the Niche RMS.

The Administrator shall grant access to the Niche RMS on receipt of:

- A request from a manager (which will normally be submitted by email), or
- A list of starting police officers

As part of the creation process for the account, the administrator for the Niche RMS shall assign a specific 'Level' of access to the user reflecting their role(s) / training, and as described in the request. Note this provides the user with one of a number of permissions.

Administrators for the Niche RMS shall be notified by Personnel of all staff leaving the Force, and as a result shall suspend the associated accounts.

Niche RMS Administrators shall review user access records to ensure that access to the system remains appropriate.

4 Home Working

- All Agile Working policies and procedures will be followed.
- Non-employees, including family members, will not be given access to any Force equipment or information.
- Consideration should be given to any smart devices i.e. Alexa/Google and cameras that may be near by – the microphones should be disabled when discussing anything sensitive and cameras should not overlook your work area.
- Personal printers will not be connected to Force equipment.
- Force information will not be copied to any personal device in order to work on it.

5 Monitoring & Auditing

Staff should be aware that all actions within Niche RMS are monitored and regular audit dip samples are carried out to ensure that Force policy and procedures are being followed.

HEDDLU GOGLEDD CYMRU
NORTH WALES POLICE

POLICY

EMAIL AND NETWORK DRIVE POLICY

Governance:	**Senior Leadership Team**		
Document Type:	**Policy**		
Policy Owner:	**Chief Information Officer**		
Department:	**Finance and Resources**		
Policy Writer:	**Chief Information Officer**		
Policy Number:	**019**	**Version:**	**2.1**
Effective Date:	**03/08/22**		
Recommended Review Date:	**03/08/26**		

CHANGE HISTORY				
Version No	**Author**	**Changes**	**Ratification**	**Date**
1.0	Data Protection & Information Assistant	New document structure & review	Change Committee	16/12/09
1.1	Data Protection & Information Assistant	Minor change made 17/03/10. Contact IS&C		
1.2	Head of IS&C	Amendments to take account of Force structure changes	Change Committee	21/4/11
1.3	Head of IS&C	Amendment to 1.6 – authorisation level	CIO after consultation with stakeholders	3/4/12
1.4	Head of IS&C	Cosmetic changes PA to PCC transition		
1.5	Head of IS&C	Amendments to provide further detail in various sections	CIO	28/08/2014
1.6	Continuous Improvement Officer	Email & Internet Procedure separated into 2 standalone Procedures		
1.7	Electronic Communications Manager	Amendments to implement Business Rules following Efficiency Review Recommendations		
1.8	Electronic Communications Manager	Amendments following consultation		
1.9	IS&C	Changed to reflect changed to Data Protection legislation	CIO	
2.0	FG&P Officer / IS&C	Brought in line with current policy principles and transferred to the new corporate template. Additions to reflect introduction of NEP and O365.	CIO	
2.1	Information Assurance	Minor amendments made and deletion of MSG groups due to the decommission of the telephone directory.	Head of Information Assurance	**0/08/2024**

CONTENTS

1. WHY IS THIS POLICY REQUIRED?

This policy will

1.1 Provide information on the correct use of email and network drives for a policing purpose.

1.2 Support the Force Information Security Policy (FISP)

2. WHO SHOULD USE THIS POLICY?

This policy should be used by all NWP personnel, i.e. Police Officers, Police Staff, Police Community Support Officers, Special Constables, Agency Staff, Volunteers, Partners, Office of the Police & Crime Commissioner, Victim Help Centre, Work Experience and anyone who has an active SULO account and are authorised to use a police computer

Throughout this document the term 'employee' is used to refer to the above personnel.

This policy includes:

- Guidance on the use of email
- Guidance on the use of network drives

3. WHAT SHOULD I CONSIDER WHEN USING THIS POLICY?

NWP email facilities are provided for **WORK-RELATED PURPOSES ONLY** and there should be no expectation of privacy. Transaction and business monitoring is undertaken in Force. Any misuse of the email system may amount to gross misconduct and could lead to loss of employment and/or criminal proceedings.

4. ROLES AND RESPONSIBILITIES

4.1 Individuals	When using emails, it is your responsibility to operate your email account in accordance with this policy, including appropriate retention and storage to ensure the confidentiality, integrity and availability of the information that is held. It is your responsibility to maintain your OneDrive / H drive and any group network drives to which you have access, in accordance with this policy and departmental instructions, including appropriate retention and storage to ensure the confidentiality, integrity and availability of the information that is held. At all times, work related information should be retained on Department/Team network drives or the appropriate force system (e.g. RMS, Fotoweb). Evidential data must not be stored on the Fileserver, H drive or OneDrive.
4.2 Departmental Managers	Responsible for ensuring group drives are operated and maintained in accordance with local instructions to ensure the confidentiality, integrity and availability of the information that is held

4.3 Force Wide Group Drive Owners / Teams Sites	Responsible for ensuring the confidentiality, integrity and availability of the information that is held

5. THE PROCESS

5.1 Email

The email system is a necessary tool to facilitate the business need; however, its use introduces risks to the Force. These risks need to be balanced with the needs of the Business to ensure that information systems are maintained at a level which is appropriate to the needs of the Force. Appropriate controls must be in place to reduce the security risks created by email usage.

The email system should be used for work related purposes only, which is defined as follows.

Correspondence in which you would reasonably expect to engage in during the course of your employment with NWP. It includes any correspondence related to your employment such as emails to HR, Occupational Health or staff associations.

The sending of chain/round robin emails and non-work-related pictures is unacceptable.

Work-related social events such as retirement 'do's' or athletic events are also acceptable subjects, providing of course there are no innuendos or comments which would breach the Code of Ethics. Also remember some staff members will not wish for their personal details in relation to retirement or births etc. to be publicised, so appropriate consent should always be sought.

Sending information to and from home computers/devices, is only acceptable in limited circumstances with the base point being that any personal information or information classified as OFFICIAL or above **must be removed** prior to sending**.** The following are examples of the restrictions:

- It **is** acceptable to send generic training materials and practice guides subject to permission being granted by the trainer/information owner
- It **is** acceptable to send your own duty roster (but not those of others) and payslips
- It **is** acceptable to send details of Federation and Unison information
- It **is** acceptable to send details for use in Classified Ads which should be referenced in the subject line of the email
- It is **not** under any circumstances acceptable to send official agenda papers, minutes of meetings, force policies, power point presentations and other performance data to assist with private or work-related study or tasks
- It is **not** acceptable to send operational information to home computers/devices
- It is **not** acceptable to send personal documents, e.g. tickets, insurance policies, labels etc., into Force for printing unless agreed with the Force Printing Department for the relevant fee
- It is **no**t acceptable to send in family or other private photographs to be used as screen savers, to be printed or to be forwarded on

- It is **not** acceptable for you to retain any personal information on your OneDrive / H: drive

REMEMBER - NWP email facilities are provided for **WORK-RELATED PURPOSES ONLY** and there should be no expectation of privacy. Transaction and business monitoring is undertaken in Force. Any misuse of the email system may amount to gross misconduct and could lead to loss of employment and/or criminal proceedings.

You must only access the email system with your single user logon (SULO). This will ensure that you only have access to the email account(s) that have been allocated to you. This also ensures that when you email external recipients your correct email address is used, and the automatic bilingual North Wales Police disclaimer is displayed.

When using Email consider if it is the most appropriate means of communication when other methods could be used. Urgent requests should be made via direct conversation not e-mail.

Out of Office replies must be set and must be very clear in providing instructions to where emails should be re-directed during any planned absences. Out of Office messages are a useful tool if used properly. They must only be set for the periods set out within the Business rules at Appendix B.

The 'Out of Office' message should clearly state who to direct urgent enquiries to and that individual shall be made aware that they are the nominated point of contact. Overuse of the 'Out of Office' message generates unnecessary e-mail traffic.

If there is an unexpected staff absence steps should be followed as per Business rules at Appendix B.

The auto forwarding of emails **out of Force** is not permitted without authorisation. Please refer to Information Assurance (IA)for advice. Please be aware that when changing access privileges to your outlook account and/or setting up rules, that there will be privacy and confidentiality implications for both the potential recipient and sender, particularly if it is an email of a sensitive nature/HR issue. Please consider carefully before changing your account and consider what you are emailing, to whom, and who may have access to it.

A message to 'All Mailboxes' should only be sent in exceptional circumstances and with the agreement of your Departmental Head*. Inappropriate use of 'All Mailboxes' leads to increased traffic on the network, is a waste of time for those people who have no interest in the mail, and could lead to an inappropriate disclosure to people who do not need to know the content of the mail. All Mailboxes emails must **only be sent by an Inspector rank or above, or Police Staff POA grade and above**. Authority may not be passed on to a rank or grade below this

**A Head of Department may delegate the authorisation to another member(s) of their team providing that:*

- *The delegation of authority is **not below Inspector or Police Staff equivalent (POA)***

- *The delegation includes the caveat that the new authorising person(s) must fully acquaint themselves with the requirements of the Email procedure.*

- *The Head of Department understands that whilst the authority can be delegated the responsibility remains with them to ensure the Email authorisation procedure within their department is adequate.*

Prior to sending an e-mail to a distribution group consider whether everyone within that group needs to be aware of the information. Wherever possible direct it to individual e-mail accounts.

Use the self-service MSG groups where appropriate. The principle behind these groups is that if a user wishes to distribute a non-business-related message across the Force then the appropriate self-service group can be selected. Examples of appropriate messages include leaving messages and facility updates. Details on how to subscribe/unsubscribe are found in Appendix A.

All users (employees) must adhere to the Email Business Rules (Appendix C) to ensure effective use of the email system.

SSF are responsible for the overall management of email distribution groups, however new group accounts and Departmental Mailboxes will need to be authorised by an Inspector or Police Staff Equivalent, and should be allocated an owner, generally in the department to which they relate. SSF will advise a new owner of their responsibilities and will also prompt the owner to periodically review membership of the group, and to verify it is still required. Appendix A holds further details.

5.2 Network Drives

Network drives are storage devices and are essential in the retention of business-related information.

Information retained on network drives should be for work related purposes only as defined above. Again, there should be no expectation of privacy.

All media files, which include CCTV, video, audio and image files such as .mov / .mp4 / .vob / .avi / .jpg / .mpg-4 audio / .jpeg / .png should be retained on the appropriate storage system, not on OneDrive/H: drive or Teams Group/G: drive unless authorised by the Chief Information Officer. This list is not exhaustive.

All users should familiarise themselves with the guidance on effective use of network drives listed in Appendix C.

You must only access network drives with your single user logon (SULO). This will ensure that you only access the network drive(s) you have been authorised to access which may be in addition to your personal OneDrive/H: drive.

Users should store files within the H and G drives in accordance with the below guidance.

One Drive/H Drive – Personal	
Suggested Uses ✔	**Not Intended for** X
✔ Active file storage for individuals	X Active file storage for departments
✔ Course work	X Administrative information storage
✔ Critical individual document backup	X Critical dept document backup
✔ Short term data transport	X Department wide software
	X Departmental file sharing
	X Multi-departmental file sharing
	X Movies
	X Music

	✗ Pictures
	✗ Evidential Data
	✗ System Backups
Teams Group/G Drive – Group	
Suggested Uses ✓	**Not Intended for** ✗
✓ Active file storage for depts.	✗ Active file storage for individuals
✓ Administrative information storage	✗ Critical individual document backup
✓ Departmental file sharing	✗ Document archiving
✓ Critical document backup for dept.	✗ Multi-dept. file sharing
	✗ Movies
	✗ Music
	✗ Pictures
	✗ Evidential Data
	✗ System Backups

5.3 Data Retention and Access

For "**Exceptional Need**" reasons only access to an email account or a OneDrive/H: drive (\\fhqfile001)(H:) is permitted for a line manager, but for a **maximum** period of time of 24 hours (Monday to Friday) and if further access is required it will be treated as a separate request and the appropriate level of authorisation required. Permission will only be granted under sudden unforeseen circumstances needing immediate action. Examples of such occurrences include, but not limited to; public safety, employee welfare risk, risk to life or a valid policing purpose. There is NO expectation of privacy.

If this is required, you will need the written approval from the Department Head of your Business Area. In every case, it must be made clear why access to the information is vital and, in all instances, a clear audit trail must be maintained. This explanation must demonstrate the necessity for such access, in the event of a challenge from the user or the Information Commissioner. The Business Systems Unit, when it is deemed appropriate, will validate requests of this nature.

This written authority should be forwarded to the relevant SSF Purchasing Team who will submit the service request.

Access to specific network drives and mailboxes across the Force must be **role specific** and authorised by the owner of the network drive or mailbox and the appropriate level of access determined:

- **Read Only** - displays the files data, attributes, owner and permissions
- **Read/Write** – write to file, append to the file and change its attributes in addition to displaying the files data, attributes, owner and permissions
- **Full Permissions** – no restrictions

Written authority should be forwarded to the relevant SSF Purchasing Team who will submit the SRM request.

When employees move Departments/Roles, to maintain confidentiality and to avoid any breach of the Data Protection Act, it is the responsibility of the releasing Head of Department/Line Manager to ensure that access rights and mailbox membership are reviewed and removed when necessary.

As part of the recruitment/appointment procedure, the SSF will ensure that the following documents are forwarded to the releasing Line Manager and the new Line Manager so that access rights are duly removed or added:

- NWP System Access Rights – New or Change Requests (SSF Ref. 0001)

- NWP System Access Rights – Removal (SSF Ref. 0591)

Data associated with email accounts and OneDrive/H: drives will normally be retained for 60 days from the official date of leaving the force, unless under exceptional circumstances SSF Business Systems Unit are advised otherwise that the data is required to be retained longer. The retention period of data for Superintendents/Police Staff equivalent and above will be retained for 1 year.

Line Managers should ensure that any essential work-related information that is held in the leavers email account or OneDrive/H: drive is moved/transferred accordingly, to ensure it remains accessible to the organisation.

If a leaver from NWP is re-employed there is **no automatic right** to have access to any previous data retained on the email account or OneDrive/H: drive. Access to retain information will only be granted when it is deemed truly appropriate. This includes those who have been seconded.

If access is required, you will need the written approval from the Departmental Head of your Business Area. In every case, it must be made clear why access to the information is vital and, in all instances, a clear audit trail must be maintained. The SSF Business Systems Unit, when it is deemed appropriate, will validate requests of this nature.

This written authority should be forwarded to the relevant SSF Purchasing Team who will submit the SRM request.

If the retention period has lapsed and no exceptions were noted, no data can ever be recovered.

5.4 General Use

You should take care when addressing emails. Using an incorrect address could lead to you making an unauthorised disclosure, which could be a risk to the force, to Officers and to members of the public. If you are sending an email to a distribution list, you should review the list before sending to ensure that only relevant people are receiving your mail.

Email is not intended for trivial or inconsequential messages which increase the traffic on the email system and can be a waste of time to the recipient. When sending emails, you should consider whether your email is necessary before you send it and, for example you should use a suitable group account facility if one is available, for example TEAMS. Further details about group accounts and all mailboxes can be found in Appendix B.

If you have any security concerns about the North Wales Police email system (to include unauthorised/unrecognised attachments or receipt of inappropriate emails and vulnerabilities),

you should contact Information Assurance by or emailing the Information Security Incidents mailbox. If you are in any doubt concerning the authenticity of any email do not open it.

You must not use any third-party email or personal services such as Hotmail.com, via the force computer except where it is required for the policing purpose. You must obtain written approval from Information Assurance before you use any such service providers.

The email system is not intended to be a filing or storage system. You should retain emails only for as long as they are required, and documents should be stored on the relevant drive on the network. Emails should be archived according to the business need and legislative requirements. There must be no global automatic deletion of emails without adequate notice and agreement by the Force owners of the information. Please see the Records Management procedure for further information.

5.5 Government Security Classification

You must value and protectively mark all internal email and, where appropriate, external email. For example, you should include a Government Security Classification, when sending an email to other forces, but not when sending an email to a member of the public. Full details can be found in the Government Security Classification Policy.

- Emails to all police.uk, gov.uk, .csjm are considered secure. A full list of other secure email addresses can be found on Forcebook by searching email security.

- Our email servers now attempt to send all external emails using TLS encryption and in the vast majority of cases this method ensures secure delivery. Although limited in number, there will always be some email addresses which do not support TLS encryption and as a result email will be sent insecurely. That does not mean that the email will not arrive at its intended destination or that it will be intercepted en route. If you are sending any emails of a sensitive nature to an email address not on the TLS list on Forcebook then Information Assurance would recommend additional security measures, for example password protecting any documents.

- If the business need to send information by email outweighs this guidance, you need to be confident that you are the correct person to make that decision before any decision is made. You may wish to seek advice from Technology and Information Assurance before you transmit anything. Please refer to the Government Security Classification Policy for further details

5.6 Use of Language, Libel and Inadvertent Contracts

Take care with the language that you use in your emails. NWP is opposed to any form of discrimination on the grounds of race, gender, age, nationality, disability or sexual orientation. The language that you use should give colleagues and the community we serve a clear message that we value diversity and respect individual differences. The storage and/or transmission of any inappropriate or discriminatory language are prohibited (except where it forms part of an investigation).

You must be mindful about libel. Email is increasingly replacing more traditional methods of communication, and is viewed by many to be less formal than a letter. However, emails can be stored indefinitely, and the content can subsequently be disclosed, for example under the Data Protection or Freedom of Information Acts. You must therefore ensure accuracy, integrity and professionalism in the emails you send.

You must take care to avoid inadvertent contracts and negligent mis-statement. Provided that an outside party reasonably believes that an employee has authority to negotiate, or enter into, an agreement, then the employer will be bound by what the employee says. You must remember

that the law imposes a duty of care on a person or company providing advice, where the recipient relies on the advice.

5.7 Data Protection Action 2018

Remember that all the work you undertake on the email system must be compliant with the Data Protection Act 2018.

Failure to protect personal information can lead to significant harm and sanctions from the ICO, which may include monetary penalties imposed on the force.

You should exercise care if you are sending an email outside the European Economic Area (EEA) (roughly the area of the European Community) as many countries do not have the same protections as we do in the EEA. You should contact Information Assurance and Technology for advice prior to sending any information.

5.8 Security

Technical security of the Force network is the responsibility of the Technology Department, who will provide adequate technical controls and monitoring to ensure that Force information is not put at risk through the email facilities. Further details are in the Information Security Policy. Risks include:

- Vulnerability of messages to unauthorised disclosure, access or modification
- Denial of Service attacks
- Malicious software in emails and/or attachments
- Vulnerability to error
- Interception and eavesdropping
- Compromise of the organisation to include integrity issues

Whist standalone workstations do not use the NWP email system the principles within this policy must be observed, and full permission for any email to be available via a standalone workstation must be obtained from the relevant departmental Heads, Technology and the Head of Information Assurance prior to use.

5.9 Bulk Data Transfers

The movement of bulk data from one system to another, or to another device, or to another agency via email (perhaps as an attachment) must be authorised by the Chief Information Officer. Contact Information Assurance for advice.

5.10 Audit and Monitoring

Email monitoring (transaction and business) is undertaken by Information Assurance the Anti-Corruption Unit to protect the confidentiality, integrity and availability of North Wales Police information and its reputation.

Automatically quarantined emails (both incoming and outgoing) which contain offensive, derogatory or operationally sensitive material and incoming emails containing spam or specific attachments which have the potential to affect the availability of data through, for example, size or virus, will be reviewed by Information Assurance.

Covert monitoring will be used by the Force where it supports the evaluation of compliance with force standards, or it is considered proportionate and necessary in the circumstances.

Remote access (e.g. mobile phones, tablets, and laptops) email use is subject to the same audit and monitoring as networked workstations.

5.11 Accounting

Suitable accounting facilities and measures should be in place. All log on attempts, successful or not, must be recorded and unsuccessful attempts interrogated on a regular basis. This is the responsibility of Technology.

5.12 Third Party Use of North Wales Police Email System

If it is necessary for non North Wales Police personnel to have access to the NWP email system, a risk assessment must be undertaken to identify any risks. Suitable countermeasures must be put in place to protect the NWP email system, the NWP network and the information held thereon. Contact should be made with Information Assurance for further assistance.

5.13 Cyber Harassment and Bullying

Cyber harassment and/or bullying are unacceptable. If you experience any form of email contact which you consider to be harassment or bullying, please contact your line manager or someone else that you trust, or Police Integrity Line (0800 111 4444).

6. DECLARATION & LEGALITIES

6.1 In line with all Force policies, the overarching purpose of this document is to directly support the PCC police and crime plan objectives. Overall the intention of this policy is to make North Wales the safest place to live, work and visit in the UK

6.2 In the writing of this policy cognisance has been taken of the college of policing code of ethics (2014).

6.3 North Wales Police policies will be written in accordance with the approved corporate format and published on Forcebook, allowing access to staff and public, where appropriate, on the pages of the public facing Internet site under the Force publication scheme and Freedom of Information Act 2000.

6.4 The following main legal requirements have been identified within this policy:

- Equality Act 2010
- Human Rights Act 1998
- The Welsh Language (Wales) Measure 2011 and the Welsh Language Standards for the Chief Constable
- Data Protection Act 2018
- Freedom of Information Act 2000
- Health and Safety Act 1974

6.5 This policy has been written giving due regard to the above legislation and has considered the risk of unfair and/or disproportionate impacts on individuals or groups (actual or perceived) and has done so via an equality impact assessment (EIA).

6.6 New legislative requirements or changes in Force structure may necessitate a review of this policy document.

7. APPENDICIES

7.1 Appendix A - Group Account facilities and the use of All Mailboxes

A Group account is an email account to which more than one person has access to. Special interest group accounts are available for employees to join, for example Sports and Social, Federation/Unison, charity events.

Make use of the Group Account facilities to ensure you direct items of special interest to the right people. This will reduce the number of emails being sent. If you are raising money for a particular individual, make sure you have their consent before you use their personal details in an email – you still need to comply with the Data Protection Act. Further information can be obtained from the SSF Business Systems Unit and Information Assurance.

An email group is a distribution list to a specific group of individuals. Email groups are useful tools, however they need to be appropriately named and managed to ensure that they are easily recognisable and that the correct people have access to them.

If you identify a need for a new group account, contact the relevant SSF Purchasing Team for further details. SSF are responsible for the overall management of email distribution groups, however new group accounts will need to be authorised by an Inspector or Police Staff Equivalent, and should be allocated an owner, generally in the department to which they relate. SSF will advise a new owner of their responsibilities, and will also prompt the owner to periodically review membership of the group, and to verify it is still required.

It is recommended that email group names include the Business Area as the prefix to the name of the group, e.g. LPS, CS, to assist in locating the correct group.

If you find that you no longer need access to a particular email group, you must advise the SSF. Similarly, if you become aware that other people no longer need access to an email group, you should advise the SSF via email.

7.2 Appendix B - Business Rules – Use of North Wales Police E-mail System

1. Introduction

These rules underpin the Force Information Security Policy (FISP). They provide guidance for all users of the North Wales Police e-mail facility.

All Force personnel, i.e. Police Officers, Police Staff, Police Community Support Officers, Special Constables, Agency Staff, Volunteers, Partners, Office of the Police & Crime Commissioner, Victim Help Centre, Work Experience and anyone who has an active SULO account and are authorised to use a police computer are required to respect and follow these rules.

2. Why Are Business Rules Needed?

E-mail is an important business tool but its use introduces risks to the Force. Clear business rules are required to ensure that the use of e-mail is maintained at a level which is appropriate to the needs of the Force.

Business rules will assist in reducing the amount of unnecessary e-mails being circulated internally and externally.

3. When Should The E-mail System Be Used?

The e-mail system is provided for work purposes only. A definition of work related purposes is in the main policy.

Prior to sending an e-mail consider whether it is the most appropriate form of communication. If not consider a face to face conversation, telephone conference or the use of Lync instant messaging or teams.

Urgent requests should be made via direct conversation not e-mail.

4. Managing Recipients Effectively

The use of 'All Mailboxes' e-mails is strictly limited to the circulation of critical information in exceptional circumstances and requires the agreement of your Department Head. All Mailboxes emails must only be sent by an Inspector rank or above, or Police Staff POA grade and above. Authority may not be passed on to a rank or grade below this. Abuse of this facility leads to waste demand and the potential for inappropriate disclosure of information.

Prior to sending an e-mail to a distribution group e.g LPS Patrol Sergeants Anglesey, consider whether everyone within that group needs to be aware of the information you are passing. Wherever possible direct it to individual e-mail accounts. By directing your message more carefully it is more likely to be actioned.

Avoid the CC'ing culture. If Copy (CC:) someone into your e-mail you **must** clearly state why you have done so and what action is required of them.

Don't automatically use 'Reply all'. Think about who needs to see your reply. In doing so, this could potentially result in a personal data breach.

Use the self-service MSG dispatch groups where appropriate. The principle behind these groups is that if a user wishes to distribute a **Non Business** related message across the Force then the

appropriate self-service group can be selected. Examples of appropriate messages include leaving messages and facility updates.

5. Compiling E-mails

5.1. Subject Lines

Provide clear, specific subject lines that help the recipient identify what they must do or understand what the message relates to.

Modify the subject line when appropriate; do not continue using the original subject in your reply if the topic has changed.

Use **NRN / DAA** in the subject line; saying No Reply Necessary / Dim Angen Ateb saves you both and your correspondent unnecessary e-mail.

1.2 Body of E-mail

Ensure that your e-mails are –

A – Accurate
B – Brief
C – Clear

Format the layout so that the reader quickly, clearly and directly gets the message you intended. This helps avoid the unnecessary and annoying back and forth of e-mails.

Limit the message to one subject. If you need to raise multiple issues, clearly state this in the first line.

Avoid sending attachments where possible. If appropriate send links to documents which can be stored securely on Sharepoint. If attachments do need to be sent let the recipient know which one is relevant to them and if possible highlight relevant sections.

5.3 Corporate E-mail Signature

The corporate e-mail signature should be used and all contact details kept up to date.

6. Automatic Replies (Out Of Office Messages)

'Out of Office' messages are a useful tool if used properly.

- They should be activated by – Shift workers – Rest days and periods of annual leave.
- Non-shift workers – Periods of annual leave.

The 'Out of Office' message should clearly state who to direct urgent enquiries to and that individual shall be made aware that they are the nominated point of contact.

Over use of the 'Out of Office' message generates unnecessary e-mail traffic.

If there is an unexpected long term staff absence it is the responsibility of the line manager to determine when an 'Out of Office' message is to be initiated. Appropriate wording of the message should be sent to the SSF Purchasing Team.

7. Supervisory Responsibility

Local supervisors will be supported in challenging minor breaches of the E-mail procedure and associated business rules. It will be at the discretion of the supervisor as to whether any identified breaches are reported to Information Assurance (IA)

Supervisors are a key driver in changing poor working practises and should ensure that they comply with the e-mail business rules and promote alternative forms of communication with their staff members.

8. Active Monitoring of E-mail Communications

There should be no expectation of privacy when using North Wales Police Force systems. Information Assurance IA) monitor and audit e-mail use in the form of dip-sampling.

7.3 Appendix C - Guidance on Effective Use of OneDrive & Teams Groups

Always maintain your OneDrive/H: Drive and Teams Group/G: drive. Ensure that the data you store is work related. Keep folder structures and filenames simple and precise. This way we can

guarantee that all relevant work-related data is backed up and secure. Do not keep information for longer than necessary; if information is being temporarily stored on your OneDrive/G: Drive or Teams Group/G: drive ensure its deleted when no longer required, or once the information has been uploaded to another force system or central repository.

1. make sure that all files saved on personal and group drives are **work related**.

2. be selective of what you save. Consider whether it is the appropriate place to save the document.

3. make sure that any image files and media are stored on the image server. (Fotoweb)

4. make sure that the information stored is relevant and up to date, and not kept for longer than necessary

5. make sure that the data on you OneDrive/H: Drive is relevant to your post.

6. make sure that the appropriate version controls are in place.

7. be aware of duplication of data. Delete if the same information is recorded on another force system or central repository.

8. be selective. Who needs to see the document? This will determine where it should then be saved.

9. be selective of e-mailing the document. Is it better to save to a Teams group /G: drive or make available on SharePoint?

10. make sure that the file is named correctly and that a minimum amount of characters are used for your reference i.e. change Terms of Reference.doc to TOR.doc

11. ensure that the folder structures are simple and precise.