Niche Warning Marker Procedure

This procedure is part of North Yorkshire Police policy to which all Chief Constable personnel and the functions provided by the Police, Fire and Crime Commissioner are required to adhere.

Procedure Statement

Niche is an operational database of crime, intelligence and non-crime occurrences available to all police officers and staff within North Yorkshire Police (NYP) who have received the appropriate training. Niche includes functionality to record Warning Markers against those individuals considered vulnerable or who may pose a risk to others.

The Police National Computer (PNC) holds information relating to individuals sought by police and/or previously processed by police, courts and/or non-police prosecuting agencies. The PNC is an essential operational policing tool that provides police forces and other agencies with access to a range of information about a recorded individual including any Warning Signals. PNC Warning Signals identify where a subject may be vulnerable or pose a risk to others.

In order to maximise the benefits of both systems, NYP will fully utilise Niche and PNC to ensure warning information is recorded promptly and managed in compliance with information management rules applicable to each system.

The proper recording and management of warning information will assist in decision making and effective service provision by ensuring that police officers, staff and other agencies are aware of potential risks to the safety of themselves, the individual or others.

Overarching Policies:
Data Protection Policy
Information Security Policy

Procedures:
Police National Computer Procedure
Collection and Recording of Police Information Procedure
Data Procedure

Other Documents:
Niche Warning Markers: NYP Guidance Notes
PNC User Manual
PNC Code of Practice 2005

NPIA Warning Signal Review process
OEL and PNC Templates
Quick Reference Guide to Creating and Managing Niche Flags

Process

'Warning information' refers to any information identifying risk or vulnerability, that is relevant to the safe and effective management of a case or care of an individual.

'PNC Warning Signals' are applied to PNC where the PNC National criteria are met

'Niche Warning Markers' are applied to Niche where the PNC National criteria are met.

Niche Flags should be used to alert users to the existence of warning information that does not meet the PNC National criteria. If there is no flag specific to the situation the Info of note flag should be used. Niche Flag creation criteria.

Prior to attending, or whilst investigating or managing, a crime or occurrence NYP officers and staff will check both Niche and PNC to collate information that may be relevant to the enquiry, and to establish whether there is any warning information available.

Officers and staff will ensure Niche and PNC warning information is sufficient, accurate and that it remains relevant.

Where new warning information is identified by NYP, officers and staff must ensure that Niche is appropriately updated using Niche Warning Markers or Niche Flags to alert the user, and record supporting information within Niche (e.g. OEL and Custody record or Reports tab as appropriate). Niche Warning Markers should ***not*** be added if the only provenance for the information is an existing PNC Warning Signal owned by another force – the originating force hold provenance for and are responsible for managing this information.

A Niche Warning Marker should be added only where the warning information meets the criteria for a PNC Warning Signal *(criteria are detailed in the PNC User Manual, Chapter 11).* Niche Warning Markers should therefore mirror NYP-owned PNC Warning Signals for a person record with a PNC ID*. If there is no related PNC record, a Warning Marker should still be applied to Niche, providing the circumstances meet the PNC Warning Signal criteria, so that the information is available in Niche and PND should a PNC record be created in future or should that person otherwise come to notice (e.g. VA, victim).

** Please note that multiple Warning Markers in Niche may be represented by a single PNC Warning Signal, with review dates amended as appropriate.*

NYP officers and staff with permissions to create and update Niche Warning Markers should create these directly to Niche, ensuring that relevant supporting information is also recorded on the Niche record. New Niche Warning Markers will be identified by PNC Bureau during a daily search and reviewed to ensure that they meet the relevant criteria. If they do not, PNCB will send a task back to the creating officer.

Officers and staff who do not have permissions to create or update Niche Warning Markers must record the relevant supporting information on the Niche record, and task the PNC Bureau (via Niche Occurrence workflow) to update Niche Warning Markers and, where appropriate, PNC Warning

Signals.

PNC Bureau will assess available information on receipt of a Niche Warning Marker task. Niche and PNC will be updated in accordance with local and national guidance.

Reviewing Niche Warning Markers

Niche Warning Markers should be reviewed in line with the NPIA PNC Warning Signal Review guidance and end-dated (to appear greyed out) when no longer relevant.

When reviewing PNC Warning signals, PNCB will review/amend/end date corresponding Niche Warning Markers as appropriate.

Teams creating Niche Warning Markers are responsible for reviewing/amending/end dating those Niche Warning markers which do not have a corresponding PNC Warning Signal. Teams must have processes in place to ensure that:

- where a Niche Warning Marker is returned by PNCB because it does not meet the criteria, the Niche Warning Marker is promptly deleted (by request to Niche Systems Admin), and a relevant Niche Flag is applied to the record instead, with an appropriate review date
- where Niche Warning Markers are held on person records with no PNC ID, these are reviewed in line with NPIA PNC Warning Signal Review guidance, and retained/amended/end dated as appropriate

Governance

Niche and PNC are powerful investigative tools and all NYP officers and staff will safeguard information obtained from these systems.

The principles of PNC use are enshrined within the PNC User Manual.

Use of Niche and PNC is also governed by the Official Secrets Act, Data Protection Act 1998, and Computer Misuse Act 1990.

Access and Disclosure

Access to Niche and PNC data is only permitted for a legitimate policing purpose.

The handling and disclosure of personal information is subject to strict rules. Failure to adhere to those rules may result in disciplinary procedures or legal action which may attract a custodial sentence.

Only authorised trained users will have access to carry out Niche and PNC checks. PNC operators must adequately record the reason for each PNC check in accordance with the PNC Manual and published best practice. The reason entered for each PNC check is retained within the PNC Transaction Log for seven years and is subject to regular audit.

Niche and PNC Enquiry

Prior to carrying out a Niche and/or PNC check for another, the operator must satisfy themselves:

- Of the enquirer's identity and their entitlement to receive the information requested; and

- That the check is for a legitimate policing purpose; and
- That access complies with published guidance.

Niche and PNC Update/ Review

Information created on Niche and PNC will be accurate, relevant, and timely. PNC updates will only be performed by users who have completed the appropriate PNC update training and maintained proficiency in those skills.

Timeliness of PNC updates shall be compromised only where necessary to confirm accuracy of information provided and ensure compliance with legal and procedural requirements.

Disclosure

NYP will disclose Niche and/or PNC information, including warning information where necessary. Disclosure will only take place where required under a statutory obligation, permitted under a statutory power, or permitted under common law. This includes subject access requests received via ACRO, and Data Protection Act rights requests.

Hard copy disclosure of PNC information will only be completed using the appropriate PNC print format as defined within the PNC Manual. Hard copy PNC information will be stored, handled, and disposed of in accordance with its protective marking. Where hard copies are required by email these will only be sent to secure email addresses.

Auditing

Any user activity on Niche and PNC may become subject of audit.

For PNC auditing refer to NYP Police National Computer Procedure.

Security

All Niche and PNC data should be stored, handled, and disposed of according to its protective marking classification. The NYP Information Security Policy clearly defines the responsibility of all NYP officers and staff to ensure the safeguarding of information.

Should NYP officers or staff become aware that a request for information may not be legitimate they will not pass any information but will instead obtain as much information from the enquirer as possible including details of the information requested and a contact telephone number on which the enquirer may be contacted. Full details of the check will be passed to a line manager who will contact the Enquirer to confirm identity.

Where it is established the Enquirer is not authorised to receive PNC information (e.g. bogus caller purporting to be a police officer) the PNC Liaison Officer must be informed and will ensure other police forces and PNC Services are made aware of the bogus request.

RESPONSIBILITIES

NYP Officers and Staff

- Record sufficient, accurate and timely warning information within Niche

- When information meets the relevant criteria, create Warning Markers on Niche where Niche role allows (e.g. trained Custody staff), or request via Niche OEL workflow to PNCB for a Niche Warning Marker be created
- Ensure sufficient rationale is recorded within Niche to support PNC update requests
- Where Niche and/or PNC warning information requires update, task PNCB in a timely manner
- Respond promptly to PNCB requests for additional information to ensure PNC updates are not delayed
- Supervisors to ensure that their team's Niche Warning Markers with no corresponding PNC nominal record are reviewed in line with the NPIA Warning Signal Review criteria

Force Control Room

- Ensure incident logs are updated appropriately with warning signal information as it becomes available
- Ensure use of the correct tags, qualifiers and closing disposal codes

PNC Operators

- Ensure the purpose of each PNC check is sufficiently and accurately recorded in compliance with training, local guidance on the PNC Services subsite and the PNC Manual.
- Ensure PNC is accessed only for legitimate policing purposes and that PNC information is disclosed in the correct format and only to those persons authorised to receive it.
- Ensure Niche and PNC data is handled, stored and disposed of in accordance with the relevant protective marking.

PNC Bureau (additional to PNC Operators above)

- Create and update Niche Warning Markers in line with the above process and PNC criteria.
- Carry out a daily search of Niche to identify newly created Niche warning markers.
- Update PNC Warning Signal information, and corresponding Niche Warning Marker information accurately and in a timely manner, tasking back to teams where necessary.
- Review Niche Warning Markers with corresponding PNC records

- Adhere to Warning Signal guidance contained within the PNC Manual, NPIA Review guidance, and locally produced warning signal creation and review guidance.

PNC Liaison

- Deal with any challenges, disputes or deletion requests from the data subject in relation to PNC Warning Signal information, liaising with Niche RRD and Records Compliance as necessary.

Niche Systems Admin and DQ/RRD Teams

- Provide assistance, support and feedback as necessary to teams managing Warning Marker creation, content and reviews within Niche