



Police National Database (PND) Access Control

This document is part of North Yorkshire Police policy to which all Chief Constable personnel and the functions provided by the Deputy Mayor for Policing as part of the York & North Yorkshire Combined Authority are required to adhere.

Procedure Statement

The Police National Database (PND) is a national data store of operational policing information provided by individual forces. It holds copies of records relating to intelligence, crime, custody, child protection and domestic abuse investigations.

Effective access control is an important part of safeguarding operational police information and intelligence to fulfil a legal duty. North Yorkshire Police (NYP) restrict direct PND use access to key operational teams with a specific policing purpose.

This procedure is designed to be compliant with standards required as part of the overall security approach for PND.

Overarching Policies:

Information Security Policy

Procedures:

Police National Database Procedure
Security Incident Reporting Procedure
Protective Marking

Other Documents:

United Kingdom Security Vetting
APP Vetting
APP Information Management
Code of practice on the operation and use of the Police National Database - GOV.UK
PND Manual of Guidance
Restricted PND Password Reset Instructions
PND new user process maps
Secure Communications Guidance

Police National Database Access Control Procedure

PROCESS

A key part of the PND security approach is to prevent unauthorised system access. The Identity Management System (IMS) holds and manages identity data within Identity and Access Management Central Services (IAMCS). IAM is a national system that provides police forces with access to national applications such as the PND.

This technical approach has enhanced security by confirming a user's identity and ensuring access to the different PND environments (restricted PND and confidential PND) is complemented by different security access controls. CONFIDENTIAL PND requires two factor authentication (2FA) that being a smartcard and PIN. RESTRICTED access is achieved through user credentials and password. It ensures confidence in system security and a consistent approach across the police community, particularly common business processes such as sponsoring, identity proofing and authorising users.

1 Access control

PND Users will be briefed, during training, on their responsibilities in relation to PND access control. Confidential PND users are also required to sign an End-Entity Agreement that defines additional security responsibilities. Operational PND users must conform to business processes outlined in the NYP Police National Database (PND) procedure including the safeguarding of passwords and smartcards (if issued) to prevent unauthorised access.

PNC Liaison will monitor the movement of users (changing roles or leaving NYP) through the normal People Services e-forms enabling a review of access where appropriate.

Business Insight will carry out monthly PND transaction audits to ensure all accounts remain active. This audit will also involve the validation of PND transactions ensuring they have been carried out for a legitimate purpose. Where a user is found to have not used the system in six months, the Business Insight team will notify PNDSPOC requesting a review of that user's access.

The following PND gatekeepers are together responsible for granting and removing PND access:

- Business Sponsor (applicant/user line manager)
- Business Approver (Head of Professional Standards)
- Identity Registrar (ICT/PNC Department)
- Identity Approver/Card Approver (PNC Department)
- Card Issuer (Atos/ICT/PNC Liaison)
- PND Registrar (PNC Liaison)

2 Initial request

The user authorisation process will be subject to periodic external audit.

Direct user access is limited to key operational units for specific policing purposes and authority will only be given where the individual performs an appropriate role.

Initial PND access requests will be emailed by line managers to PNDSP0C@northyorkshire.police.uk. The PND Registrar will review each application and check the applicant's vetting status before informing the line manager of the outcome.

The PND Registrar will arrange for the names of those approved for training to be added to the appropriate PND training nominations list.

3 Vetting

The PND Manual of Guidance and Business Rules sets out minimum vetting levels for police and police staff carrying out PND roles.

- Restricted user: Recruitment Vetting (RV)
- Confidential user: Management Vetting (MV) and Security Check (SC)
- Administrator: Management Vetting (MV)
- Auditor: Management Vetting (MV) and Security Check (SC)

Should an uplift in vetting clearance be required, the applicant/user will liaise with Vetting to arrange. The applicant will notify the PND Registrar once the required clearance has been confirmed. The PND Registrar will confirm vetting status using the force vetting database CoreVet.

4 Training

PND training is assigned according to the PND procedure and organisational need. PND users must successfully complete training delivered by an accredited PND trainer before accessing to the system is provided. Details of all PND training is maintained within the Training Administration System.

The PND Registrar will liaise with users to confirm availability for training before providing a list of confirmed attendees to RMU Training at least two weeks in advance.

At the conclusion of each PND training event, the PND trainer will notify PNDSP0C of the outcome for each attendee. Applicants who successfully complete the training assessments, and for whom IAM registration is complete, will be notified by the PNDSP0C once their account is ready for use.

Applicants who do not successfully complete the assessment/s will be invited to attend the next available event.

Confidential access only: users must complete the smartcard process prior to accessing the confidential platform.

5 IAM registration – new users

The PND Registrar will contact users at least one month in advance of allotted training to initiate IAM registration.

The IAM Registration e-form will document the process of authorising an operational PND User. A submitted form can be accessed at any time by the applicant, the line manager or a PND administrator. An application must at least be authorised by the Business Approver prior to PND training.

The Applicant will:

- Complete section 1 (User Application) indicating whether Restricted or Confidential access required
- Ensure their warrant / identity card photograph is a true likeness. Should the image need to be updated the applicant will contact Front Counter, HQ to arrange this prior to attending PND training
- Confidential access only: when notified, complete section 11 (User Acceptance) confirming receipt of their smartcard and attaching a scanned copy of the End Entity Agreement, with wet signature

The Business Sponsor may reject or support an application.

To reject the application the Business Sponsor will:

- Complete the 'Application rejection' field on the IAM Registration e-form

To support the application the Business Sponsor will:

- Complete section 2 (User Identity Verification Record) of the IAM Registration e-form to confirm the photograph on the Applicant's warrant or staff identity card is a true likeness
- Complete section 3 (Identity Proofing and Vetting Status) of the e-form
 - Applicant police vetted: referring to CoreVet (general access), confirm vetting level(s) and vetting expiry date(s)
 - Applicant not police vetted: carry out Identity Proofing and record details of identification. Proof of identity may be an original valid 10 year British or European Union Passport or valid UK photocard driving licence. Proof of address may be an original bank statement or utility bill dated within the previous three months and clearly showing the applicant's name and address. Email scanned copies of the original documents under separate cover to the Business Approver (Head of Professional Standards) explaining purpose.
- Complete section 4 (Business Sponsor Authorisation) of the e-form confirming the Applicant has a legitimate business requirement for the type of PND access requested
- Ensure the Applicant will work or operate in an environment that meets the requirements of Official (for PND Restricted) or Official Sensitive (for PND Confidential) Government Security Classification (GSC)
- Ensure the Applicant is afforded time to respond to carry out and respond to requests for PND searches received from non-PND users

The Business Approver may reject or support an application.

To reject the application the Business Approver will:

- Complete the 'Application rejection' field on the IAM Registration e-form

To support the application the Business Approver will:

- Review the provided information (and identity documentation if appropriate) to verify and validate the Applicant's identity
- Confirm the Vetting information against CoreVet
- Complete section 5 (Business Approver Authorisation) of the e-form

The Identity Registrar will:

- Validate the Applicant's identity from the IAM Registration e-form
- Create a user identity in IAM Central Services (IAMCS)
- Confidential access only: create an IL4 (Impact Level 4) Active Directory account and complete associated system processes, including smartcard request
- Liaise with the Identity Approver for approval at each stage
- Complete section 6 (Identity Creation) of the e-form once all processes complete
- Confidential access only: liaise with the Applicant to arrange collection of their smartcard following successful training. Ensure End Entity Agreement (with wet signature and smartcard collection date) produced and remind Applicant to scan and upload to e-form

The Identity and Card Approver will:

- Check identity details entered in IAMCS are correct and approve identity creation
- Confidential access only: authorise the smartcard request and complete approval
- Raise any discrepancy with identity or smartcard request with the Identity Registrar
- Request the Identity Registrar disable the identity where necessary
- Complete section 7 (Identity Approval) of the e-form
- Confidential access only: complete section 8 (Card Approval) of the e-form

Upon receiving confirmation of successful training from the PND trainer, PND Registrar will:

- Complete section 9 (Privilege Assignment & PND Register) of the IAM Registration e-form
- Confidential access only: Liaise with the Identity Registrar to ensure smartcard collection arranged. Ensure the Applicant completes section 11 (User Acceptance) and attaches a signed copy of the End Entity Agreement.
- Update the PND Register and PND licence register
- Add PND user to the PND User Outlook distribution list

People Services will:

- Complete section 12 (Staff Record) of the e-form and update any relevant staff system to signify the user is IAM authorised

6 Issuance of smartcard and confidential credentials (confidential PND)

Upon successful completion of IAM registration and PND training, a confidential PND user must collect their smartcard and confidential credentials. The Identity Registrar or Card Issuer will contact the user to agree a suitable time for collection from Police Headquarters.

The user must produce their warrant/identity card when collecting the smartcard. If the user is unable to attend and collect the card, they may nominate another to collect the card on their behalf. Any nomination of another must be agreed in writing to the Identity Registrar or Card Issuer in advance.

The Identity Registrar or Card Issuer will:

- Email instructions for smartcard setup (PIN and security answers) to the PND user
- Examine the warrant / identity card of any person collecting a smartcard to confirm they are authorised to collect
- Ensure an End Entity Agreement has been signed and dated with the day of collection
- Complete section 10 (Card Issue) of the IAM Registration e-form to verify identity and confirm smartcard handed to user
- Remind the user to complete section 11 (User Acceptance) of the e-form
- Forward the completed form to the PND Registrar

The PND user will:

- Complete section 11 (User Acceptance) of the e-form
- Change the smartcard PIN and security answers as directed

PND users should not keep a written record of their smartcard PIN and under no circumstances should a smartcard and associated PIN be stored together.

7 Identity modification

All PND users must notify of a change in identity.

The PND user will:

- Ensure all systems are updated to reflect new identity
- Obtain a warrant/identity card reflecting new identity
- Request an IAM Registration Form (Word version) from PNDSPPOC
- Provide original evidence of identity modification (e.g. marriage certificate, deed poll) to their line manager
- Complete the Application Type (Identity Modification) and section 1 (Applicant Identity Details) of the IAM Registration Form and forward the form to their line manager and cc to PNDSPPOC
- Confidential access only: forward a new signed End Entity Agreement to PNDSPPOC

The line manager (Business Sponsor) will:

- Carry out the necessary identity checks and scan the identity modification evidence
- Complete section 2 (User Identification Verification Record) of the IAM Registration Form confirming new warrant/identity card produced
- Complete section 3 (Identity Proofing and Vetting Status) to record method by which identity modification evidenced
- Complete section 4 (Business Sponsor Authorisation)
- Forward the form and scanned identity modification document to the Business Approver (Head of Professional Standards)

The IAM Registration form will follow the IAM Registration – new user process detailed in section 6 above.

8 Withdrawal of PND access

PND access, together with any related smartcard access, may be suspended where the user is absent from their role for greater than one month. Circumstances may include secondment, role change, maternity leave, sickness or career break.

It is the line manager's (Business Sponsor) responsibility to notify PNDSPOC when a PND user no longer has a legitimate need for access. PNDSPOC will forward a PND Access/Smartcard Suspension/Termination form to the PND user for completion.

The PND user (Business Sponsor if the user has already left the organisation) will:

- Complete the Application Type section recording the reason why suspension is required
- Complete section 1 (Applicant Identity Details)
- Forward the form to their line manager (Business Sponsor) and cc to PNDSPOC
- Confidential access only: contact the Identity Registrar to arrange return of their smartcard

The Business Sponsor will:

- Complete section 2 (Business Sponsor Authorisation) of the form before forwarding to the Business Approver (Head of Professional Standards) and cc to PNDSPOC
- Confidential access only: store the smartcard securely (short term suspension) or arrange to return the smartcard to the Identity Registrar (long term suspension)

The Business Approver will:

- Complete section 3 (Business Approver Authorisation) of the form before forwarding to the Identity Registrar and cc to PNDSPOC

The Identity Registrar will:

- Liaise with the Identity Approver to effect suspension of the IAM identity
- Complete section 4 (Identity Deactivation) of the form
- Confidential access only: disable smartcard access and, if long term suspension, arrange for smartcard return with the Business Sponsor
- Confidential access only: Complete section 6a (Smartcard Suspension/Termination)
- Confidential access only – long term suspension: Complete 6b (Smartcard receipt) and arrange destruction of the smartcard. If the smartcard has not been retrieved update section 6b to indicate that it is missing
- Upon receipt from the Identity Approver, forward the completed form to the PND Registrar

The Identity Approver will:

- Complete section 5 (Identity Approval) of the form and return to the Identity Registrar

The PND Registrar will:

- Disable or terminate the PND user account as indicated in Application Type on the form.
- Update the PND Register and licence register
- Update the PND User Outlook distribution group
- Forward the form to People Services Helpdesk

People Services Helpdesk will:

- Make the necessary changes to relevant staff systems

Smartcards may be returned via internal mail by agreement with the Identity Registrar. Smartcards returned in this way must comply with the Secure Communications guidance for official sensitive content.

Where a confidential PND user leaves the force without surrendering their smartcard, the Business Sponsor must make every effort to retrieve it from the user. If they are unable to take possession of the smartcard the Business Sponsor must complete a Report an Information Security Incident in addition to notifying the Identity Registrar and PND Registrar.

Where suspension of user access cannot be anticipated and is required immediately:

- The Business Sponsor will contact the ICT Service Desk to request immediate suspension
- The ICT Service Desk will notify the Identity Registrar who will immediately de-activate the user in IAMCS and, for confidential users, disable the Active Directory Account
- The Business Sponsor will then email PNDSPOC and retrospectively complete the Suspension of PND Access process described above

IAM identities can be transferred between forces and agencies. For this reason, IAM identities will not normally be terminated unless there is clear indication the user will never again require access via any force or agency.

9 Theft, damage, loss or unauthorised use of a smartcard/PIN

PND users will treat their smartcard and PIN as extremely valuable items. Any theft, damage, loss or unauthorised access must be reported immediately to the ICT Service Desk during office hours or the Force Control Room (FCR) outside office hours.

Users must also Report an Information Security Incident within 24 hours where their smartcard or PIN has been stolen, lost or resulted in unauthorised access.

If a smartcard requires suspension/termination within office hours, the ICT Service Desk will notify the Identity Registrar or Card Issuer. Where the User still has possession of their smartcard, they may be asked to return it for suspension/termination.

The Identity Registrar will:

- Disable the user's Active Directory Account
- De-activate the user's credentials / identity within IAMCS
- Terminate and destroy the smartcard (if returned)
- Notify the PND Registrar confirming whether smartcard lost, stolen or returnable so the PND Register can be updated where appropriate
- Order a replacement smartcard

If a smartcard requires suspension/termination outside office hours, the FCR will take the report and contact ICT Service Desk as soon as possible to initiate the office hours process outlined above.

On all occasions where the theft, permanent loss or unauthorised access to a smartcard or PIN has occurred, the smartcard will be terminated. Authorisation for termination is automatic in these circumstances.

10 Account reactivation / smartcard replacement

When a suspended PND user returns to their role and has a legitimate need for PND access then their PND user account will require reactivation. If the user requires confidential access, a new smartcard will also be required.

The PND user will:

- Contact PNDSPOC to request an IAM Registration Form (Word version)
- Complete the Application Type and section 1 (Applicant Identity Details)
- Forward the form to the line manager
- Confidential access only: read and print a fresh End Entity Agreement ready to sign and date on the day of card collection

The line manager (Business Sponsor) will:

- Complete only section 4 (Business Sponsor Authorisation) of the form then email to the Head of Professional Standards (Business Approver)

The IAM Registration form will follow the IAM Registration – new user process detailed in section 6 above.

Confidential access only: when a replacement smartcard is required.

The Identity Registrar or Card Issuer will:

- Email instructions for smartcard setup (PIN and security answers) to the PND user
- Examine the warrant / identity card of any person collecting a smartcard to confirm they are authorised to collect
- Ensure an End Entity Agreement has been signed and dated with the day of collection
- Complete section 10 (Card Issue) of the IAM Registration e-form to verify identity and confirm smartcard handed to user
- Require the user to complete section 11 (User Acceptance) of the form
- Forward the completed form to the PND Registrar requesting update of the PND Register

The PND user will:

- Complete section 11 (User Acceptance) of the form
- Complete the End Entity Agreement (wet signature and dated with day of collection)
- Scan the End Entity Agreement and email to PNDSPOC

The IAM Registration form will follow the IAM Registration – new user process detailed in section 6 above.

11 Password management – restricted environment

Confidential and restricted PND users will be instructed how to log into the restricted platform during their training.

Restricted passwords expire after 90 days, and users are expected to change their password before it expires. A user may change the password at any time within the 90 days by selecting 'Change Password' on the PND home page.

If a user has forgotten their restricted password, they should follow the 'Forgotten Password' link at the bottom of the login screen.

Full instructions detailing PND restricted password set/reset can be found below the PND login link on the PND bulletin board and login.

12 Password and smartcard management – confidential environment

To access the confidential PND platform, users will require a Cisco IL4 password in addition to their smartcard and PIN. ICT Service Desk can set and reset Cisco IL4 passwords. When requesting a new password, users should ask that the ICT Service Desk do not tick the password prompt box.

Once the user has successfully logged into Cisco with a new or reset password, they must remember to change that password immediately to something memorable.

A confidential user may change their smartcard PIN at any time using My Digital ID which can be found on the confidential platform along with confidential PND and other IL4 applications. A smartcard PIN should not reflect the user's employee number, collar number or date of birth. It is good practice to change the smartcard PIN at regular intervals.

A smartcard will become locked if an incorrect PIN is entered on more than three consecutive attempts. The PND user may unlock their card in one of two ways.

- Self-service using My Digital ID (accessed within the IL4 environment).
- Assisted smartcard unlock. If the user is unable to answer the security questions in My Digital ID correctly, they will need to contact the Card Issuer to assist.

13 Smartcard certificate renewal

A smartcard certificate will be valid for a period of three years. The smartcard certificate expiry is displayed within the 'Confirm Certificate' window that pops up each time the smartcard is used. One month before expiry, the user must contact the Identity Registrar (ICT) to request a replacement smartcard.

RESPONSIBILITIES

Officers and staff

- Discuss the reason for PND training requirement with first line supervision
- Complete IAM Registration when prompted following allocation of training
- Carry out checks in response to requests from non-PND users

- Notify PNDSPoC to notify when access no longer required
- Confidential access:
 - Complete End Entity Agreement
 - Surrender smartcard to line manager when no longer required
 - Properly report any theft, loss, damage or inappropriate use of smartcard/PIN
 - Order new smartcard prior to certificate expiry

Line manager (Business Sponsor)

- Email PNDSPoC nominating team member for PND training, Specify training type (basic, advanced or basic & advanced) and access type (restricted or confidential). If confidential access required specify location of IL4 terminal to be used.
- Complete required identity checks and IAM documentation
- Afford PND user the time to carry out checks in response to requests from non-PND user
- Notify PNDSPoC when no longer requires access
- Recover and securely store or return smartcard when no longer required

Head of Professional Standards (Business Approver)

- Authorise PND access/suspension
- Complete vetting/identity checks and forward required IAM documentation
- Complete and forward required IAM documentation

Identity/Card Approver (PNC Liaison)

- Review IAM changes made by Identity Registrar and approve as necessary
- Submit requests to the Identity Registrar or Card Issuer when confidential access required
- Complete and forward required IAM documentation

Identity Registrar (ICT / PNC Department)

- Initiate activation and deactivation of user identity in IAMCS and Active Directory
- Notify the Identity/Card Approver where authorisation required
- Complete and forward required IAM documentation
- Arrange confidential smartcard allocation and smartcard renewals for confidential users
- Assist users with IAM and smartcard issues

Card Issuer (PNC Liaison)

- Complete smartcard issuance, suspension/termination and replacement/reactivation
- Assist users with smartcard PIN unlock
- Complete and forward required IAM documentation

PND Registrar

- Liaise with Training to schedule PND training
- Assess and respond to all nominations for PND training
- Liaise with Training Support and RMU to align users with training events
- Complete and forward required IAM documentation
- Maintain the PND Register, licence register and PND user Outlook distribution list
- Create and manage PND user accounts and user groups
- Maintain PND Source site, including PND login and password reset links

People Services Helpdesk

- Complete and forward required IAM documentation
- Update relevant staff records

Training Department

- Agree scheduled PND training with the PND Registrar
- Email the outcome of every PND training event to PNDSPOC

ICT Service Desk

Notify the Identity Registrar (ICT) of any reported issue with confidential PND access or reports of compromised smartcard/PIN

Force Control Room

Outside office hours, receive reports of smartcard loss, theft, damage or unauthorised use and notify the Identity Registrar and PND Registrar (PNDSPOC) at the earliest opportunity to enable smartcard termination.

ICT out of hours support

- Deactivate user identity within IAMCS and Active Directory
- Notify Identity Registrar and PND Registrar (PNDSPOC) of action taken