



**Public
Prosecution
Service**

Independent
Fair
Effective

PPS Privacy Notice – Staff Management

Status

The current status of this document is: Final

Version History

Number of this Version: 5.0

Date of this Version: 21/05/2026

1. Data Controller

1.1. The Data Controller is:

Public Prosecution Service, 93 Chichester Street, Belfast BT1 3JR

The Data Protection Officer for PPS can also be contacted by email (dpo@ppsni.gov.uk) or telephone (028 9089 7100).

2. Why are you processing my personal information?

2.1. We are processing your data for the purpose of managing staff.

2.2. The PPS also processes your data in the public interest to protect PPS Staff and information from possible threat and to ensure that the PPS meets its obligations under the GDPR and Data Protection Act 2018 to provide “appropriate technical or organisational measures”.

2.3. PPS also processes your data for the purpose of National Security Vetting (NSV). See the separate Privacy Notice on NSV.

3. What categories of personal data are you processing?

3.1. PPS Resource Management Unit processes your data to carry out aspects of staff management. This includes:

- a) identifying data such as name, address, date of birth, National Insurance Number, Telephone Number, email address
- b) your level of National Security Vetting (if any)
- c) qualifications and skills
- d) current posting
- e) payroll (including bank account details)
- f) pensions

3.2. PPS Line managers may also process your data to carry out staff management such as:

- a) informal discussions with members of staff
- b) flexi sheets
- c) job descriptions
- d) evidence to assist with completing annual performance appraisal etc
- e) information relating to sickness absence, medical certificates, performance reports, conduct and employee relations, OHS and Welfare Reports. However, note that this information is processed for the purpose of long term storage on HR Connect.

3.3. The PPS Communications Team processes your email address to provide you with information about the PPS and its activities such as the Core Brief.

3.4. PPS Property Management processes your personal data to manage its access control systems. This data is stored on standalone computers in each building. The data processed includes:

- Name
- Photograph
- Times and dates when you use your proximity card to access doors with proximity card access controls

3.5. PPS Property Management processes your personal data from the operation of its CCTV systems. This data is stored on standalone computers in each building. The data processed includes:

- Images of you when you are in areas covered by CCTV
- Dates and times of those recorded images

3.6. PPS ICT processes your personal data to carry out monitoring of IT and line of business systems. Further details of this can be found in the PPS Monitoring at Work Policy, but the personal data processed may include:

- Examining email and attachments for evidence of malpractice or breaches of security;
- Examining logs of browser usage to ensure users are complying with PPS policy;
- Receiving and examining reports of attempted or actual use of telephone premium-rate lines;
- Checking mobile telephone bills for use of premium phone lines or excessive personal use;
- Examining PPS Network access and usage to ensure it complies with PPS Policy
- Checking access to invoices and payments processed by Account NI to ensure it complies with PPS Policy and to prevent fraud
- Checking CMS access and usage to ensure it complies with PPS Policy
- Checking CRV access and usage to ensure it complies with PPS Policy
- Checking access to the NICS Links portal to determine who has completed training

3.7. PPS ICT also processes personal data if you use the PPS BOX application. The use of PPS Box requires you to register an account. To do this you provide a name, email address and mobile phone number (to allow for two factor authentication). When you log in to PPS Box, PPS Box will also record:

- Your IP Address
- Login and logout times
- Files that you view
- Files that you upload
- Files that you download

Data not processed by PPS

3.8. With the development of shared services within the NICS, there are a number of areas where PPS formerly processed your data but this has now been transferred. These are:

- Data in relation to your employment other than that mentioned in paragraphs 3.1 and 3.2 is now processed by NICS HR and HR Connect on behalf of PPS and the NICS. As noted above, the data mentioned in 3.2 e) is initially processed by PPS but then transferred to Departmental HR and HR Connect.

- HR Connect passes on some of your data to Links and to Meta Compliance for the purpose of providing e-learning.
- Data in relation to the provision of IT Services to you is now processed by ITAssist.
- If you have a civil service pension then your data is also processed by Civil Service Pensions NI. Their Privacy Notice is [here](#).
- Travel and subsistence payments are also processed by Account NI on behalf of PPS and the NICS.

4. Where do you get my personal data from?

- 4.1. Data used for staff management comes from you and your line manager, either as data that you provided to PPS or previously provided to DHR or HR Connect.
- 4.2. Detail on email addresses and other IT services are managed and provided by IT Assist.
- 4.3. Data collected to manage access control systems comes from the following sources:
 - Name and Photograph from you
 - Data on when and where you use your proximity card is collected automatically by the relevant system.
- 4.4. Your image is recorded whenever you pass a CCTV camera.
- 4.5. Monitoring at work data is collected whenever you use PPS IT and Line of Business Systems. Data on access to AccountNI is obtained from AccountNI. Data on Links is obtained from HR Connect. Data on your access to the CRV is obtained from Causeway.

5. Do you share my personal data with anyone else?

- 5.1. PPS may share data in relation to staff management with NICSHR or HR Connect.
- 5.2. PPS does not normally share personal data collected by CCTV or access control systems with anyone outside the Business Assurance Team, except in line with the PPS Monitoring at Work Policy.
- 5.3. PPS does not normally share Monitoring at Work data outside the PPS ICT team, except in line with the PPS Monitoring at Work Policy. Data obtained from Account NI and Causeway is not normally shared outside the Business

Assurance Team, except in line with the PPS Monitoring at Work Policy. PPS may share monitoring data with PSNI where evidence of criminal offences is detected.

- 5.4. The PPS may share your data with the Northern Ireland Audit Office to carry out data-matching exercises for the purpose of assisting in the prevention and detection of fraud. The powers are contained in Articles 4A to 4H of the Audit and Accountability (Northern Ireland) Order 2003. We do not require your consent to share this data.

6. Do you transfer my personal data to other countries?

- 6.1. PPS does not store your data outside the UK. PPS and Causeway servers are located in the UK. However, your data may be processed outside the UK as PPS systems can be accessed remotely. PPS policy limits remote access to countries which are covered by the UK adequacy regulations (These are noted [here](#)).
- 6.2. DHR, HR Connect, AccountNI, Links and Meta Compliance data is stored in line with their own policies.

7. How long do you keep my personal data?

Staff Management

- 7.1. Personal data related to staff management is retained in line with the PPS Retention and Disposal Policy.
- 7.2. Data mentioned in 3.2 e) is retained on a temporary basis by PPS to facilitate its transfer to HR Connect. After it has been transferred to HR Connect it is deleted.

CCTV

- 7.3. CCTV pictures are retained for a maximum of 30 days but may be deleted sooner depending on the capacity of the recorder.

Proximity Card

- 7.4. Proximity Card data is currently subject to differing retention periods. This is due to limitations within the software. Once the storage is full, the software deletes the oldest transactions to create new ones. PPS is currently working with software providers to set the maximum retention period for any data to one year.

Monitoring Data

- 7.5. Monitoring Data on line of business systems is retained in line with the case file to which it is related. Account NI retain monitoring Data in line with AccountNI Policies. Causeway retain CRV monitoring data in line with Causeway Policies.
- 7.6. Where monitoring data is obtained for the purpose of a data incident investigation, it is retained in line with the PPS Retention and Disposal Policy for data incident files.

CRV Access Data

- 7.7. CRV access data obtained for the purpose of monitoring CRV access is deleted 12 months after the audit is completed.
- 7.8. Where CRV is relevant to a data incident investigation, it is retained in line with the PPS Retention and Disposal Policy for data incident files.
- 7.9. CRV files is retained by Causeway and is managed in line with their retention and disposal policy.

PPS BOX

- 7.10. Your user account data is retained as long as your user account is active. While your user account is active, transactional data is retained for 7 years after the event.
- 7.11. Inactive accounts are retained for six months and then deleted. When your account is deleted any transactional data relating to items in BOX is retained until those items are deleted. Consequently your user data will remain in BOX until all items you interacted with are deleted. Items are deleted once the case is closed.

8. What rights do I have?

- 8.1. Your rights are as follows:

- To obtain confirmation that your data is being [processed, and access to your personal data](#). To have personal data [rectified if it is inaccurate or incomplete](#)
- To have personal data erased and to prevent processing, [in specific circumstances](#).
- To 'block' or suppress processing of personal data, [in specific circumstances](#)
- The right to data portability, [in specific circumstances](#)

- The right to object to the processing, [in specific circumstances](#)
- In relation to [automated decision making and profiling](#). However the PPS does not carry out automated decision making.

9. How do I complain if I am not happy?

- 9.1. If you are unhappy with any aspect of this privacy notice, or how your personal information is being processed, please contact the PPS Data Protection Officer (contact details as shown in paragraph 01).
- 9.2. If you are still not happy, you have the right to lodge a complaint with the Information Commissioner's Office (ICO):

Information Commissioner's Office
Wycliffe House
Water Lane
Wilmslow
Cheshire
SK9 5AF
Tel: 0303 123 1113
Email: casework@ico.org.uk
<https://ico.org.uk/global/contact-us/>