



Workforce Privacy Notice

This privacy notice has been written to inform prospective, current, and former employees of NYNET about how and why we process your personal data, including during the recruitment process.

Who are we?

NYNET is a data controller as defined by the UK GDPR. This means that we determine the purposes for which your personal data is processed and the manner of the processing. We will only collect and use your personal data in ways that are compliant with data protection legislation.

NYNET has appointed Veritau Ltd as its Data Protection Officer (DPO). The role of the DPO is to monitor our compliance with the UK GDPR and the Data Protection Act 2018 and advise on data protection issues. If you would like to discuss this privacy notice or our use of your data, please contact Veritau.

Veritau's contact details are:

Data Protection Officer
Veritau
West Offices
Station Rise
York
North Yorkshire
YO1 6GA
information.governance@veritau.co.uk // 01904 552848



What personal information do we collect?

The personal data we collect about you includes:

- Personal identifiers, including your name, contact details, date of birth, employee number and national insurance number.
- Information about your right to work in the UK, including ID documents.
- Education and qualifications, including copies of certificates.
- Your employment history, including employment references.
- Information about your workplace attendance and reasons for any absences.
- Information about professional development and performance, including reviews and any disciplinary information.

- Information collected during the assessment and/or interview process (such as interviewer notes)
- Relevant criminal history data, including your DBS check.
- Emergency contact information.
- Financial and payroll data, including bank account information, tax, national insurance and pension contributions.
- Information contained in your contract, including your job role and responsibilities, start date, employment location and contracted hours etc.
- Photographs or video images of you, including CCTV footage. We will seek consent to use your photo on our website. Please note you can withdraw this consent at any time and consent will be considered withdrawn should you no longer be employed by NYnet.
- Medical information, which is relevant to your employment, including any disability you disclose.
- Equality monitoring information, such as your ethnicity, religious beliefs, and gender.

Why do we collect your personal information?

We process your information for the purposes outlined below:

- To ensure your right to work and suitability for the role.
- To pay your salary and carry out related payroll functions.
- To monitor and manage staff absence.
- To meet our health and safety obligations.
- To monitor and manage professional development, training and performance.
- To manage additional proceedings in relation to your employment such as our grievance process.
- To make any reasonable adjustments you may need in relation to a health condition or disability.

What is our lawful basis for processing your information?

Under the UK GDPR, it is essential to have a lawful basis when processing personal information. For workforce data processing, we normally rely on the following lawful bases:

- Article 6(1)(b) - contractual obligation
- Article 6(1)(c) - legal obligation
- Article 6(1)(e) - public task

There may be occasions where our processing is not covered by one of the legal bases above. In that case, we may rely on Article 6(1)(f) - legitimate interests. We only rely on legitimate interests when we are using your data in ways you would reasonably expect.

For the processing of personal data relating to criminal convictions and offences, processing meets Schedule 1, Part 2 of the Data Protection Act 2018 as below:

- (10) Preventing or detecting unlawful acts

Some of the information we collect about you is classed as special category data under the UK GDPR. The additional conditions that allow for processing this data are:

- Article 9(2)(b) - employment and social security and social protection law
- Article 9(2)(g) - reasons of substantial public interest

The applicable substantial public interest conditions in Schedule 1 of the Data Protection Act 2018 are:

- Condition 8 – equality of opportunity or treatment
- Condition 10 - preventing or detecting unlawful acts

Who do we obtain your information from?

We normally receive your data directly from you, for example via documents and other records and information supplied by you in the course of your job application and employment period. However, we may also receive some information from the following third parties:

- Your previous employers.
- Your nominated referees.
- Relevant recruitment agencies.

Who do we share your personal data with?

We may share your information with the following organisations:

- Disclosure and Barring Service (DBS).
- HM Revenue and Customs (HMRC).
- Department for Work and Pensions (DWP).
- Your pension provider.
- Staff benefits provider, in relation to any salary sacrifice agreements.
- Your Trade Union, if applicable.
- Our suppliers and advisors, including insurers, lawyers, consultants, and accountant or payroll provider.
- Our IT providers, applications and platforms.
- Prospective future employers, landlords, letting agents, or mortgage brokers where you have asked them to contact us for a reference.
- Relevant recruitment agencies.

We may also share information with other third parties where there is a lawful basis to do so. For example, we sometimes share information with the police for the purposes of crime detection or prevention.

How long do we keep your personal data for?

We will retain your information in accordance with our Retention Schedule below. The retention period for most of the information we process about you is determined by statutory obligations. Any personal information which we are not required by law to retain will only be kept for as long as is reasonably necessary to fulfil its purpose.

Data held	Retention period
PAYROLL	
P45	6 years after leaving NYnet
Personnel file – includes application forms, clearances, contract, HR letters, sick notes	6 years after leaving NYnet
Payroll record	6 years after leaving – retain skeleton record after this time
Payslip and claims information	6 years after leaving NYnet
PENSIONS	
HR CASEWORK	
Casework records	6 years after sanction has been awarded (remove warnings at designated times)
Resolving Issues at Work (including where proven to be unfounded)	6 years from date of last action
OCCUPATIONAL HEALTH	
Occupational Health (OH) Information – includes referrals, medical reports etc.	40 years after leaving NYnet
TRAINING RECORDS	
Training	6 years after leaving NYnet
RECRUITMENT	
Recruitment selection paperwork – unsuccessful applicants	6 months after process
Recruitment selection paperwork – successful applicants	6 years after leaving NYnet
DBS	
DBS positive clearances	Until employee leaves NYnet
DBS negative clearances	Until employee leaves NYnet
PHOTOGRAPHY	
Photos on website	Subject to consent, until employee leaves NYnet or removes consent
CCTV Images	3 years

International transfers of data

Although we are based in the UK, some of the digital information we hold may be stored on computer servers located outside the UK. Some of the IT applications we use may also transfer data outside the UK.

Normally your information will not be transferred outside the European Economic Area, which is deemed to have adequate data protection standards by the UK government. In the event that your information is transferred outside the EEA, we will ensure your data is protected and appropriate safeguards are in place in accordance with the UK GDPR.

What rights do you have over your data?

Under the UK GDPR, individuals have the following rights in relation to the processing of their personal data:

- to be informed about how we process your personal data. This notice fulfils this obligation.
- to request a copy of the personal data we hold about you.
- to request that your personal data is amended if inaccurate or incomplete.
- to request that your personal data is erased where there is no compelling reason for its continued processing.
- to request that the processing of your personal data is restricted.
- to object to your personal data being processed.

If you have any concerns about the way we have handled your personal data or would like any further information, then please contact our DPO using the details provided above.

If we cannot resolve your concerns then you may also complain to the Information Commissioner's Office, which is the UK's data protection regulator. Their contact details are below:

Phone: 0303 123 1113 or via their [live chat](#). Opening hours are Monday to Friday between 9am and 5pm (excluding bank holidays). You can also report, enquire, register and raise complaints with the ICO using their web form on [Contact us | ICO](#).

Changes to this notice

We reserve the right to change this privacy notice at any time. We will normally notify you of changes that affect you. However, please check regularly to ensure you have the latest version.

This privacy notice was last reviewed 17th January 2023.