



Job Applicant Privacy Notice

Applies to: All job applicants, candidates, and prospective employees of Northridge Care Group

1. Purpose of this Notice

This Privacy Notice explains how Northridge Care Group ("the Company", "we", "us") collects, uses, stores, and protects personal information about individuals applying to work with us.

We are committed to handling your personal data fairly, lawfully, and transparently, in line with the UK General Data Protection Regulation (UK GDPR) and the Data Protection Act 2018.

2. Data Controller

Northridge Care Group Ltd
No.3 South Preston Office Village, Bamber Bridge, Preston, Lancashire, PR5 6BL
Email: DPL@northridge.uk
Tel: 01772 346825

We are the data controller for all personal information you provide during the recruitment and selection process.

3. What Information We Collect

We collect and process the following types of information from job applicants:

a. Personal Identification

- Name, address, contact details (email, phone number)
- Date of birth (where required for safeguarding or identification purposes)
- Proof of identity (passport, driving licence, birth certificate)

b. Recruitment Information

- Application forms, CVs, and cover letters
- Interview notes, assessment results, and correspondence
- Employment history, qualifications, skills, and experience
- References provided by you or third parties

c. Safeguarding and Compliance Information

- Right to work documentation (e.g. visas, share codes)
- Criminal record and DBS check information (where relevant to the role)
- Information about professional registration or safeguarding declarations

d. Equal Opportunities and Diversity Monitoring

- Information on gender, ethnicity, disability, or health (collected voluntarily for monitoring and reporting purposes only)

We do not require or process irrelevant personal data (e.g. marital status, political opinions, or unrelated medical details) as part of our recruitment process.

4. Lawful Basis for Processing

We process your personal data under one or more of the following lawful bases:

- Legitimate interests: to assess your suitability for employment and manage the recruitment process.
- Contractual necessity: to take steps at your request prior to entering into an employment contract.
- Legal obligations: to meet safeguarding, right-to-work, or equality monitoring requirements.
- Consent: where we collect optional information (e.g. equal opportunities data) or retain your details for future vacancies.

For special category data (e.g. health or DBS information), processing is carried out under:

- Article 9(2)(b) - employment, social security, and social protection law (DPA 2018 Schedule 1); and
- Article 9(2)(g) - substantial public interest, including safeguarding of children and vulnerable individuals.

5. How We Use Your Information

We use your information to:

- Manage recruitment and selection processes;
- Assess your skills, qualifications, and suitability for employment;
- Verify identity, right to work, and safeguarding compliance;

- Contact you about your application or potential future vacancies (where consent is given);
- Meet our legal and regulatory obligations (e.g. Ofsted, safeguarding authorities).

We will not use your information for marketing or unrelated purposes.

6. Who We Share Your Data With

Your data may be shared, where necessary, with:

- Recruitment panel members and authorised managers;
- DBS and safeguarding authorities (for regulated roles);
- Occupational health professionals (where health information is required for role suitability);
- External HR or legal advisers (where relevant to the recruitment process).

We do not sell or share your data for marketing purposes.

7. Data Retention

- Unsuccessful applicant data will normally be retained for 6 months after the recruitment process ends, unless you consent to a longer period for future opportunities.
- Successful candidates' data will be transferred to their employee personnel file and managed in accordance with the Employee Privacy Notice.
- Data is securely deleted or anonymised when no longer required.

8. How We Protect Your Information

We have strong physical, digital, and organisational safeguards to protect your data, including:

- Encrypted IT systems and password protection
- Restricted access to confidential HR and safeguarding files
- Staff confidentiality agreements and GDPR training
- Secure disposal of paper and digital records

9. Your Rights

You have the following rights under UK GDPR:

- Access - to request copies of your personal data
- Rectification - to correct inaccurate or incomplete data
- Erasure - to request deletion (where lawful)
- Restriction - to limit processing

- Data portability - to request data in a reusable format (where applicable)
- Objection - to certain types of processing

Requests should be made in writing to the Data Protection Lead. We will respond within one month.

10. Data Breaches

Any suspected data breach must be reported immediately to your manager or the Data Protection Lead.

We will assess and, where required, report relevant breaches to the Information Commissioner's Office (ICO) within 72 hours, and to affected individuals if there is a risk to their rights or freedoms.

11. Updates to This Notice

We may update this notice periodically to reflect changes in law or internal practices. The latest version will be available on our website or provided upon request.

12. Contact

If you have any questions or concerns about how we handle your data, please contact:

Data Protection Lead: Kendal Hulme (HR Director)

Email: DPL@northridge.uk

Address: No.3 South Preston Office Village, Bamber Bridge, Preston, Lancashire, PR5 6BL

If you are not satisfied with our response, you have the right to contact the Information Commissioner's Office (ICO) at www.ico.org.uk or 0303 123 1113.