Children and Young Person's Data Protection Policy

Contents

1. Scope

This policy applies to all children and young people placed in our registered homes, as well as any personal data about their families, advocates, or professionals that we process. It applies to all employees, agency staff, volunteers, and contractors who may handle or access children's data.

This policy should be read in conjunction with:

- GDPR & Data Protection Policy (Company-wide)
- Safeguarding and Child Protection Policy
- Confidentiality and Information Sharing Policy
- Data Breach Response Procedure
- Privacy Notices (Children, Families, Employees)

2. Legislative Framework and Guidance

This policy is informed by the following laws, regulations, and guidance:

- UK General Data Protection Regulation (UK GDPR)
- Data Protection Act 2018
- Children's Homes (England) Regulations 2015
- Children Act 1989 and 2004
- Care Standards Act 2000
- Working Together to Safeguard Children (2023)
- Ofsted Social Care Common Inspection Framework (SCCIF)
- Information Sharing: Advice for Practitioners (DfE, 2018)
- Human Rights Act 1998
- Equality Act 2010

3. Definitions

"Personal data" - Information relating to an identifiable child, directly or indirectly (e.g. name, date of birth, photo, care plan, or social care records).
"Special category data" - Sensitive data requiring extra protection, including health, ethnicity, religion, sexual orientation, and behavioural or emotional information.
"Data processing" - Any action performed on data, including collection, recording, storage, sharing, use, and deletion.
"Children's data" - Any information held by Northridge Care Group about a child or young person placed in our care or referred for placement.

4. Principles

Northridge Care Group Ltd is committed to protecting the privacy and dignity of all children and young people. In line with UK GDPR, all data will be:

- Processed fairly, lawfully, and transparently
- Collected for specific, explicit, and legitimate purposes
- Adequate, relevant, and limited to what is necessary
- Accurate and up to date, with inaccuracies corrected promptly
- Retained only as long as necessary for its purpose
- Processed with appropriate technical and organisational security measures
- Not transferred outside the UK/EEA without adequate safeguards

5. Outcomes

In order to provide effective residential care and meet our statutory obligations under the Children's Homes (England) Regulations 2015, UK GDPR, and Data Protection Act 2018, Northridge Care Group Ltd must collect, use, and store personal information about children and young people in our care. This includes information shared by local authorities, families, schools, health professionals, and other agencies. All personal data will be obtained, processed, transported, and stored lawfully, fairly, and securely in accordance with data protection principles.

6. Policy and process

Lawful Basis for Processing Children's Data

Personal and special category data about children is processed under the following lawful bases:

- Legal obligation - To comply with the Children's Homes (England) Regulations 2015, safeguarding law, and Ofsted requirements
- Public task - To carry out official care and safeguarding functions in the public interest
- Vital interests - To protect a child's life, safety, and welfare
- Consent - For limited cases, such as photographs, external publications, or optional activities (where age and understanding allow)

For special category data, processing also meets the conditions under:

- Article 9(2)(g) UK GDPR - Substantial public interest
- Schedule 1, Part 2 DPA 2018 - Safeguarding of children and vulnerable people

Types of Data Held

Information we may hold about children and young people includes:

- Personal identifiers (name, date of birth, NHS number, contact details)
- Care plans, placement agreements, and risk assessments
- Health, education, and therapeutic information
- Legal documentation (court orders, LAC status, parental responsibility)
- Family and contact details
- Incident and safeguarding reports
- Behavioural, emotional, and psychological records
- Images, videos, and recordings (where appropriate and lawful)

Data Storage and Security

- Records are stored electronically in secure systems or in locked cabinets.
- Access is strictly controlled and limited to staff with a legitimate need to know.
- Information is only removed from the premises or shared electronically using encrypted systems.
- Paper documents are disposed of confidentially and securely.
- Access rights are regularly reviewed to ensure compliance.

Sharing of Information

We may share children's data lawfully and proportionately with:

- Local authority social workers and commissioners
- Education, health, and therapy professionals
- Police, safeguarding partners, and regulatory bodies (including Ofsted)
- Families and legal representatives (where appropriate)

Data will always be shared:

- On a need-to-know basis
- In line with safeguarding duties and information-sharing guidance (Working Together 2023)
- Securely, using authorised systems

Retention of Data

Records relating to children are kept in accordance with statutory guidance and our data retention schedule. Typically, children's social care records are retained until the individual reaches 75 years of age, or longer if required by safeguarding or legal proceedings.

Children's Rights

Children and young people have the same data protection rights as adults, including:

- The right to be informed (via the Children's Privacy Notice)
- The right of access (to view records, with support and safeguards)
- The right to rectification (to correct inaccuracies)
- The right to erasure or restriction (where lawful and appropriate)
- The right to object to processing (where applicable)

Requests from children, parents, or local authorities will be handled by the Registered Manager and Data Protection Lead, ensuring that decisions consider age, understanding, best interests, and safeguarding.

Data Breaches

All staff must report any suspected or actual data breach immediately to the Registered Manager and Data Protection Lead. A breach includes unauthorised access, accidental disclosure, loss, or destruction of personal data.

The Data Protection Lead will:

1. Contain and assess the breach.
2. Determine the risk to the child's rights and freedoms.
3. Report the breach to the Information Commissioner's Office (ICO) within 72 hours if necessary.
4. Notify the affected individual(s), local authority, and Ofsted where required.
5. Record all incidents and outcomes in the data breach log.

Training and Responsibilities

All staff must complete annual GDPR and data handling training specific to children's records.
Registered Managers are responsible for ensuring compliance in their homes.
The Data Protection Lead oversees monitoring, auditing, and reporting on data security across the group.

Failure to comply with this policy or with data protection requirements may result in disciplinary action.

7. Revision History

Version	Date	By whom
1.0	21.10.2025	Kendal Hulme (HR)