Data Protection & GDPR Policy

Service: Chestnut Lodge

Organisation: Willow Family Care

Policy Owner / Designated Data Protection Lead: Jamie Harrocks

Jamie Harrocks – Responsible Individual (RI)

Date Approved: September 2025

Review Cycle: Annual or following legislative change / data breach

---

1. Purpose of the Policy

This policy sets out how Willow Family Care ensures compliance with the UK General Data Protection Regulation (UK GDPR) and the Data Protection Act 2018, and how personal data relating to children, families, staff, professionals, and visitors is collected, stored, used, shared, and protected.

Chestnut Lodge recognises that children in residential care are a particularly vulnerable group and that the protection of their personal and sensitive information is fundamental to safeguarding, trust, and lawful practice.

---

2. Scope

This policy applies to:

- All employees, agency staff, volunteers, and contractors
- All personal and special category data held in paper or electronic form
- All systems used to record, store, or share information (including ClearCare, SharePoint, email, and hard copy files)

---

3. Legal Framework

This policy is informed by:

- UK General Data Protection Regulation (UK GDPR)
- Data Protection Act 2018
- Children Act 1989 & 2004
- Care Standards Act 2000
- The Children's Homes (England) Regulations 2015
- Regulation 44 & Regulation 45 requirements
- ICO guidance on children's data

---

4. Data Protection Principles

Willow Family Care adheres to the seven GDPR principles. Personal data must be:

1. Lawful, fair, and transparent
2. Collected for specified, explicit purposes
3. Adequate, relevant, and limited
4. Accurate and kept up to date
5. Kept no longer than necessary
6. Processed securely
7. Accountable

All staff are expected to work within these principles at all times.

---

5. Designated Data Protection Lead

Willow Family Care has appointed a named Designated Data Protection Officer (internal lead):

Jamie Harrocks

Role: Responsible Individual (RI)

Responsibility: Strategic oversight of GDPR and data protection compliance across the service.

Strategic Responsibilities include:

- Oversight of data protection compliance and governance
- Decision-making regarding data breaches and ICO notification
- Oversight of Subject Access Requests (SARs)
- Ensuring policies, systems, and training are in place
- Monitoring compliance through QA, audits, and RI oversight
- Liaison with external agencies where required

---

6. Operational Responsibility

The Registered Manager is responsible for:

- Day-to-day data protection practice
- Ensuring staff follow procedures
- Secure storage and access to records
- Immediate escalation of breaches or concerns to the RI
- Supporting staff with GDPR queries in practice

This split ensures clear accountability without duplication, and mirrors safeguarding governance arrangements.

---

7. Lawful Basis for Processing Data

Chestnut Lodge processes personal data under the following lawful bases:

- Legal obligation (e.g. statutory records, safeguarding duties)
- Public task (children's care and protection)
- Vital interests (safeguarding and welfare)
- Contract (employment and service provision)

Special category data (e.g. health, mental health, safeguarding records) is processed in line with Schedule 1 of the Data Protection Act 2018.

---

8. Data Security & Storage

Willow Family Care ensures:

- Electronic records are password-protected and access-restricted
- Role-based access to systems (e.g. ClearCare)
- Locked storage for paper records
- Clean desk policy
- Secure disposal of confidential waste
- No use of personal devices for work data unless authorised

Staff must never:

- Share passwords
- Access records without a legitimate reason
- Remove records from the home without authorisation

---

9. Data Sharing

Information is shared:

- On a need-to-know basis
- In line with safeguarding duties
- With local authorities, professionals, and regulators where lawful and necessary
- Securely and proportionately

Information sharing decisions are always guided by the child's welfare and statutory duties.

---

10. Subject Access Requests (SARs)

Individuals have the right to request access to their personal data.

All SARs must:

- Be referred immediately to the Registered Manager
- Escalated to Jamie Harrocks (RI) for oversight
- Be responded to within one calendar month
- Be carefully reviewed where safeguarding exemptions apply

---

11. Data Breaches

A data breach includes:

- Loss of data
- Unauthorised access
- Accidental disclosure
- Cyber incidents

Procedure:

1. Immediate containment by staff
2. Report to Registered Manager without delay
3. Escalation to Jamie Harrocks (RI)
4. Risk assessment and decision on ICO notification
5. Actions logged and reviewed as part of QA

Staff must report concerns immediately — delay increases risk.

---

12. Training & Awareness

- GDPR training is included in staff induction
- Refresher training is provided periodically
- Managers reinforce good practice through supervision
- Compliance is monitored through audits and RI oversight

---

13. Monitoring & Review

Compliance is monitored through:

- Audits
- Incident reviews
- Regulation 44 and RI oversight
- QA visits and inspections

This policy is reviewed annually or following significant changes or incidents.

---

14. Failure to Comply

Failure to follow this policy may result in:

- Disciplinary action
- Safeguarding concerns
- Legal or regulatory consequences

---

15. Linked Policies

- Safeguarding & Child Protection Policy
- Information Sharing Policy
- Records Management Policy
- ICT & Systems Use Policy
- Whistleblowing Policy

Approval

Approved by: Jamie Harrocks

Role: Responsible Individual / Director

Signature: _____

Date: _____