

FamilyCare

Healing pasts • Building futures

An abstract graphic consisting of several overlapping, rounded, organic shapes in various colors: orange, red, pink, brown, green, and blue. The shapes are layered, creating a sense of depth and movement. The colors are vibrant and the overall composition is modern and artistic.

Data Protection Policy

www.family-care.co.uk

Data Protection Policy

Implemented/Reviewed: September 2026

Date of Next Review: September 2027



1. Introduction

Family Care Group is committed to ensuring that personal data is processed lawfully, fairly, and transparently in accordance with:

- The **UK General Data Protection Regulation (UK GDPR)**
- The **Data Protection Act 2018**
- Relevant ICO guidance and safeguarding legislation

These are collectively referred to as **“data protection legislation.”**

The organisation has appointed a Data Protection Lead. Current details are maintained separately and available upon request.

2. Roles and Responsibilities

2.1 Board of Directors

The Board of Directors has overall responsibility for ensuring that appropriate arrangements are in place to support compliance with data protection legislation across Family Care Group.

2.2 Managers

Managers must:

- Ensure personal data is processed in accordance with this policy and applicable data protection legislation.
- Promote good data protection practices within their service area.
- Ensure staff complete mandatory data protection training.
- Escalate actual or suspected data breaches immediately in accordance with organisational procedures.
- Support the management of Subject Access Requests, data breaches and other data protection matters where required.

2.3 Employees

All employees must:

- Follow this policy and any related organisational procedures.
- Maintain the confidentiality and security of personal data.
- Only access, use or share personal data where authorised and necessary for their role.
- Report actual or suspected data breaches immediately.
- Complete mandatory data protection training.
- Co-operate with data protection investigations, audits and compliance activities.

Failure to comply with this policy may result in disciplinary action.

3. Data Protection Principles

The Company adheres to the **six UK GDPR principles**:

1. Personal data shall be processed lawfully, fairly, and transparently
2. Collected for specified, explicit, and legitimate purposes
3. Adequate, relevant, and limited to what is necessary (data minimisation)
4. Accurate and kept up to date
5. Kept no longer than necessary (storage limitation)
6. Processed securely with appropriate technical and organisational measures

The organisation also complies with the **accountability principle**, demonstrating compliance through policies, training, and monitoring.



4. Lawful Basis for Processing

The Company processes personal data under one or more of the following lawful bases:

- Consent
- Legal obligation
- Vital interests (e.g. safeguarding)
- Public task
- Legitimate interests (where applicable)

For **special category data** (including health, safeguarding, and care records), processing is carried out under:

- UK GDPR Article 9 conditions
- Data Protection Act 2018 Schedule 1 – including safeguarding and health/social care purposes

5. Data Subject Rights

Individuals have the following rights:

- Right of access (Subject Access Request – SAR)
- Right to rectification
- Right to erasure (where applicable)
- Right to restrict processing
- Right to data portability
- Right to object
- Rights relating to automated decision-making

The Company will respond to requests within **one calendar month**, unless an extension is permitted.

6. Data Access – Children, Young People, and Parents

Children and Young People

Children and young people with sufficient understanding have the right to access their personal data.

The Company will:

- Support access requests without unnecessary delay
- Ensure records are not altered or damaged
- Supervise access where appropriate

Access may be restricted where disclosure could:

- Cause serious harm
- Reveal information about another person without consent

Parents and Those with Parental Responsibility

Parents do **not have an automatic right** to access their child's data

The Company will:

- Seek the child's consent where they have capacity
- Consider the child's wishes and best interests
- Conduct a balancing test where consent is not given

Disclosure may occur without consent where necessary to:

- Prevent serious harm
- Safeguard a child or others

- Comply with legal obligations

7. Information Sharing

Information will only be shared where:

- It is lawful and proportionate
- There is a safeguarding need
- There is a legal obligation
- There is an overriding public interest
- Information sharing for safeguarding purposes may take place without consent where permitted by law and necessary to protect a child or vulnerable person

All disclosures must be documented, including reasons for decisions.

8. Data Security

The Company implements appropriate security measures, including:

- Access controls and role-based permissions
- Secure storage (physical and electronic)
- Password protection and encryption where appropriate
- Staff training in data protection
- Confidentiality agreements

9. Data Retention

Personal data will be retained in line with the organisation's **Retention Schedule**, ensuring:

- Data is not kept longer than necessary
- Legal, regulatory, and safeguarding requirements are met

10. Data Breach Management

All staff must report all actual or suspected data breaches must be reported immediately to a manager and Business Support

Business Support will:

- Assess risk and impact via DPO
- Record all breaches in a breach log
- Notify the Information Commissioner's Office (ICO) within **72 hours** where required
- Notify affected individuals where there is high risk

11. International Data Transfers

Personal data will only be transferred outside the UK where:

- There is a **UK adequacy decision**, or
- Appropriate safeguards are in place (e.g. International Data Transfer Agreement – IDTA)

12. Data Protection Impact Assessments (DPIAs)

DPIAs will be carried out where processing is likely to be high risk, particularly where:

- Children's data is involved
- Sensitive or special category data is processed

13. Record Keeping (Accountability)

The Company maintains records of processing activities, including:

- Types of data held
- Purpose and lawful basis
- Recipients of data
- Retention periods



- Security measures

14. Legislative References

- UK GDPR
- Data Protection Act 2018
- Children's Homes (England) Regulations 2015
- ICO Children's Code (Age Appropriate Design Code)

