JIGSAW FAMILY SUPPORT

Data Protection Policy and Procedure

1. Purpose of This Policy

This policy outlines how Jigsaw Family Support collects, stores, processes, shares, and protects personal data in accordance with:

- UK General Data Protection Regulation (UK GDPR)
- Data Protection Act 2018
- Information Commissioner's Office (ICO) guidance

The policy ensures:

- Lawful and ethical handling of personal information
- Transparency for children, families, staff, and partners
- Protection of privacy and confidentiality
- Compliance with statutory safeguarding responsibilities

2. Policy Statement

Jigsaw Family Support is committed to:

- Protecting all personal data we hold
- Maintaining confidentiality and privacy
- Ensuring lawful and secure data processing
- Only collecting information that is necessary for our work
- Being open and transparent about how personal data is used

All staff, volunteers, contractors, and third parties must follow this policy.

3. Scope

This policy applies to all data relating to:

- Children and young people
- Parents/carers and families
- Staff, volunteers, and contractors
- Referrers, professionals, and partner agencies

It covers all forms of data:

- Digital records
- Paper files
- Email and electronic communication
- Photographs, videos, and audio
- Case notes, assessments, and reports

4. Definitions

- **Personal Data:** Any information relating to an identifiable person (e.g., name, address, ID number).

- **Special Category Data:** Sensitive data requiring extra protection (e.g., health, ethnicity, safeguarding records).
- **Data Subject:** The individual the data refers to.
- **Data Controller:** Jigsaw Family Support (decides how/why data is processed).
- **Data Processor:** Any person or organisation processing data on behalf of Jigsaw Family Support.
- **Processing:** Any action involving data (collecting, storing, sharing, deleting).

5. Lawful Basis for Processing Data
Under UK GDPR, Jigsaw Family Support relies on the following lawful bases:

5.1 Legal Obligation - To comply with the law (e.g., safeguarding children).
5.2 Public Task / Legitimate Interests - To deliver educational and support services.
5.3 Vital Interests - Where life or safety is at risk.
5.4 Consent - Used for optional activities (e.g., photos or media) where appropriate.
5.5 Contract - Where contractual arrangements apply (e.g., staff employment).

Special category data is processed under:
- Substantial Public Interest (safeguarding)
- Health or Social Care provision

6. Data Protection Principles
Jigsaw Family Support adheres to the seven principles of UK GDPR.

Personal data must be:
1. Lawfully, fairly, and transparently processed
2. Collected for specific, explicit, and legitimate purposes
3. Adequate, relevant, and limited to what is necessary
4. Accurate and kept up to date
5. Stored no longer than necessary
6. Processed securely
7. Accountable, with evidence of compliance

7. Collecting Personal Data
Jigsaw Family Support collects data:
- Directly from children and families
- From schools, local authorities, and referring agencies
- During assessments or outreach sessions
- Through incident logs, reports, and observations

Only information essential for providing safe and effective services is collected.

8. Storing Data Securely
8.1 Physical Records

- Kept in locked cabinets
- Accessed only by authorised personnel
- Not left unattended or in vehicles

8.2 Digital Records

- Stored on secure, password-protected systems
- Not held on personal devices
- Backed up regularly
- Access restricted by role

8.3 Portable Devices

- Must be encrypted
- Not to leave premises unless authorised and necessary

9. Data Sharing

Personal data will be shared only when:

9.1 Safeguarding and Legal Requirements

Sharing with:

- Social care
- Police
- Health services
- Schools
- Multi-agency partners

9.2 Service Delivery

Where it is necessary for:

- Assessments
- Monitoring progress
- Support planning

9.3 Consent

For situations where consent is appropriate (e.g., photos).

Jigsaw Family Support will **never**:

- Sell data
- Share data unnecessarily
- Share data with unauthorised individuals

10. Data Breaches

A data breach includes:

- Loss of personal data
- Unauthorised access
- Unauthorised disclosure

- Cyber-security incidents

If a breach occurs:

1. Notify the Data Protection Lead immediately
2. Assess the severity and risk
3. Record the incident
4. Inform the ICO within 72 hours if required
5. Inform affected individuals where necessary

11. Rights of Data Subjects

Under UK GDPR, individuals have the right to:

- Be informed about data collection
- Access their data
- Rectify inaccurate information
- Erasure (in specific circumstances)
- Restrict processing
- Data portability
- Object to certain processing
- Not to be subject to automated decision-making

Requests must be responded to within one month.

12. Data Retention

Data is kept only for the required duration.

Jigsaw Family Support follows a Data Retention Schedule, including:

- Safeguarding records: Until the subject is 25 years old
- Personnel files: Six years after employment ends
- General records: According to statutory and operational need

When no longer needed, records are:

- Shredded (physical)
- Permanently deleted (digital)

13. Staff Responsibilities

All staff, volunteers, and contractors must:

- Follow this policy and confidentiality rules
- Only access information required for their role
- Keep data secure at all times
- Report data breaches immediately
- Complete data protection and safeguarding training

Misuse of personal data may result in disciplinary action.

14. Data Protection Lead (DPL)

Jigsaw Family Support appoints a Data Protection Lead responsible for:

- Ensuring compliance
- Managing data breaches
- Responding to subject access requests
- Overseeing data storage and retention

Data Protection Lead:
Operational Lead/ Designated Safeguarding Lead and Director

15. Review of the Policy
This policy will be reviewed:

- Annually, or
- Following significant data protection changes, or
- After any data breach

Policy Title	Data Protection Policy and Procedure
Approved By	**S. Whitehouse**
Date Approved	**1.09.25**
Review Date	**31.08.26**
Version	**2.0**

JIGSAW FAMILY SUPPORT

Data Breach Procedure

1. Purpose

This procedure outlines how Jigsaw Family Support will respond to any actual or suspected data breach to ensure:

- Immediate containment of the breach
- Protection of affected individuals
- Compliance with UK GDPR and Data Protection Act 2018
- Accurate recording and investigation
- Prevention of recurrence

A data breach may involve personal information relating to children, families, staff, or partners. All breaches must be treated with urgency and seriousness.

2. Definition of a Data Breach

A data breach is any incident where confidential or personal data is:

- Lost
- Stolen
- Accessed without authorisation
- Disclosed in error
- Destroyed unintentionally
- Altered without permission
- Processed in breach of data protection policies

Breaches may be:

- **Accidental** (human error)
- **Deliberate** (malicious attacks)

3. Examples of Data Breaches

- Emailing personal information to the wrong recipient
- Losing paper files or notebooks containing personal data
- Theft or loss of a work laptop or phone
- Sharing documents with unauthorised individuals
- System hacking or malware attack
- Sending unencrypted sensitive information
- Posting confidential information publicly
- Staff accessing records without legitimate reason
- Accidental destruction of records
- Safeguarding information shared inappropriately

ANY breach—big or small—must be reported.

4. Immediate Actions When a Breach Is Identified

4.1 Staff Responsibilities

Any staff member who discovers or suspects a breach must:

1. **Report it immediately** to the Data Protection Lead (DPL).
2. If safeguarding-related → also inform the **DSL**.
3. Provide all known details (who, what, when, how).
4. Take immediate steps to contain the breach if possible (e.g., recall email, recover documents).
5. Not delete evidence.
6. Not attempt to handle the breach alone.

4.2 If IT Equipment Is Involved

Staff must:

- Disconnect device from the internet
- Secure the device
- Inform the DPL immediately

5. Data Protection Lead (DPL) Response

The DPL will:

5.1 Contain the Breach

- Secure systems or records
- Prevent further unauthorised access
- Retrieve data where possible
- Contact IT support if necessary

5.2 Assess the Risk

Assess:

- Type and sensitivity of data
- Number of individuals affected
- Whether children are involved
- Potential harm caused
- Whether the information could be exploited
- Whether data is protected (encrypted/passworded)

5.3 Decide Whether to Report to the ICO

The DPL must report serious breaches to the **Information Commissioner's Office (ICO)** within **72 hours** if the breach is likely to result in:

- Risk to individuals' rights or freedoms
- Harm, distress, or danger
- Loss of control over personal data

If reporting is needed, the DPL will:

- Submit the ICO breach notification
- Record justification and details

- Provide updates to ICO as required

6. Informing Affected Individuals

Individuals must be informed **without delay** if the breach poses a high risk of:

- Emotional distress
- Identity theft or fraud
- Exposure of sensitive data
- Safeguarding risk

Notification must include:

- What happened
- What data was affected
- Steps taken by the organisation
- What the individual can do to protect themselves
- Contact details for further support

Where the breach involves children, communication must consider:

- Age and understanding
- Parental rights
- Safeguarding guidance

7. Safeguarding Considerations

If the data breach involves safeguarding records, children's information, or creates risk of harm:

- DSL must be involved immediately
- Social care or police may need to be consulted
- A safeguarding referral may be required
- Confidentiality rules must be strictly followed

8. Investigation

The DPL will lead a full investigation including:

- Timeline of events
- What data was affected
- Root cause analysis
- Whether procedures were followed
- Staff actions and training needs
- Whether disciplinary procedures are required

The DPL will produce a report for:

- Senior Leadership
- Directors
- Safeguarding team (if relevant)
- ICO (if required)

9. Documentation & Record Keeping

All breaches must be documented, including:

- Description of breach
- How it occurred
- Who was involved
- What data was affected
- Risk assessment
- Decisions made
- Notifications sent
- Actions taken
- Measures to prevent recurrence

Records must be stored securely and retained according to the Data Retention Schedule.

10. Preventing Future Breaches

Following an investigation, the organisation may:

- Update policies
- Provide additional training
- Improve system security
- Introduce new monitoring processes
- Adjust staff permissions and access
- Change how sensitive data is stored or transferred

Continuous improvement is part of the Quality Assurance process.

11. Staff Training

All staff must receive:

- Data protection and confidentiality training
- Cybersecurity and phishing awareness
- Training on secure communication
- Updates whenever procedures change

12. Policy Review

This procedure will be reviewed:

- Annually
- After any serious breach
- Following ICO guidance updates
- As part of the Quality Assurance cycle

Policy Title	Data Breach Procedure
Approved By	**S. Whitehouse**
Date Approved	**1.09.25**
Review Date	**31.08.26**
Version	**2.0**

Putting All The Pieces Together