



Families Growing Together
Heidi Pannell

Families Growing Together General Data Protection Regulation (GDPR) Policy

I am committed to being transparent about how I collect and the personal data of its service users and any other individuals.

I am committed to treating data lawfully and meeting my data protection obligations. This policy sets out my commitment to data protection and to respecting individual rights in relation to personal data.

Scope of policy

This policy applies to all personal data handled by Heidi Pannell

Personal data refers to any information that relates to an individual who can be identified from that information.

The processing of data widely includes every form of action that could be taken in relation to it such as obtaining, recording, amending, storing, keeping, or using it in any way; sharing or disclosing it; erasing and destroying it.

As long as the processing of data is carried out on Heidi Pannell's behalf it applies to any individual who processes that data; regardless of where the data is held (mobile devices, electronic notebooks, laptops or memory sticks) and regardless of who owns the PC/device.

Introduction to Data Protection legislation

The General Data Protection Regulation (GDPR) came into force on 25 May 2018. It is intended to strengthen and unify data protection for individuals within the European Union (EU). The GDPR replaces the 1998 Data Protection Act and is supported by the UK's Data Protection Act 2018, which became law on the same date. In addition, the Privacy & Electronic Communications Regulation 2003 (and a new ePrivacy Regulation which will eventually replace it) makes additional rules about direct marketing by phone, email or text.

Key points of the legislation are:

- Any use of personal data must have a recognised '**legal basis**' and comply with '**Data Protection Principles**'.
- Individuals must be given clear information about why and how their data is used.
- Individuals have the right to know what information an organisation holds about them. See appendix 1

Information Commissioners Office

I am registered with the Information Commissioners Office and am governed by their regulations.



Policy Objectives

I collect, hold, use and share personally identifiable information about the people I am in contact with, for the purposes of delivering services and meeting needs. I am committed to ensuring that personal data will be collected, used and held, lawfully and appropriately.

Transparency

I will fulfil my obligation to be transparent about its data processing activities.

Disclosure of service user data

Consent for processing service user data will be sought at the earliest opportunity. If an individual does not consent, appropriate action must be taken to ensure that the processing does not take place.

Service user information will not normally be disclosed to any third party without the informed consent of the service user unless the matter is regarded as a child protection or similar serious issue e.g. prevention of crime.

Whenever data is collected from individuals, key information from the Privacy Notice will be communicated.

Keeping Data Secure

Scope

Keeping personal data secure is part of data protection and I take the security of personal data seriously. I have controls in place to protect against loss, accidental destruction, misuse or disclosure

Where I engage third parties to process personal data on its behalf, such parties do so on the basis of a contract in writing that meets GDPR requirements, including a duty of confidentiality and – in particular – an obligation to implement appropriate technical and organisational measures to ensure the security of data.

Special Category Data

Special category data carries additional restrictions due to the increased threat it poses from misuse. Special category data includes racial or ethnic origins, political opinions, TU membership, religious or philosophical beliefs, genetic data, health, sex life, sexual orientation. Similar restrictions also apply to the use of data about an individual's criminal record, to criminal allegations and proceedings.

Individuals should give their explicit consent to processing their special category data or criminal records data and it will only be held without consent as a result of legal obligations (e.g. health and safety), to protect the individual's vital interests, or in limited other circumstances.

Enforcement

The ICO has a range of corrective powers and sanctions to enforce the GDPR. These include issuing warnings and reprimands, imposing a temporary ban on data processing and ordering the rectification, restriction or erasure of data, or fines.



Families Growing Together General Data Protection Regulation Procedure

Records with respect to Service Users

Each child and their family where individual work has been commissioned has an electronic case file which is stored confidentially in password-protected files. The files contains;

- Basic biographical information
- Contracts
- Notes of sessions
- Assessments and reports
- Information provided by the commissioning agency and the family
- Correspondence
- Outcome monitoring

Retention of Service Users Records

Once an intervention is completed any 3rd party information in relation to a Service User will be deleted. Records and reports will be kept for a period of 6 years.

Video records

Video footage of service user sessions is filmed only with their consent and is secured safely.

Retention of Video records

Video records will be kept until the end of the intervention, and following this the file will be wiped unless special consent has been given to use the tapes for supervision/training purposes. In these circumstances the files will be continued to be stored securely without identifying information.

Subject Access Request

Under GDPR individuals can make a data subject access request (SAR) in relation to information that is held about them.

The information will be provided either in the form of hard copy or electronically or occasionally a service user may be invited in to view their file, under supervision.

Service users should be made aware that information may be excluded from access if it would infringe the confidentiality of another individual.

Requests for information about children

Children have the same rights as adults over their personal data, including the right of access.

Before responding to a subject access request for information held about a child, I will consider factors;

- The child's level of maturity and their ability to make decisions like this;
- The nature of the personal data and how it will be interpreted;
- Any court orders relating to parental access or responsibility that may apply;
- Any duty of confidence owed to the child or young person;



- Any consequences of allowing those with parental responsibility access to the child's or young person's information.
- Any detriment to the child or young person if individuals with parental responsibility cannot access this information; and
- Any views the child or young person has on whether their parents should have access to information about them.

Under GDPR it is not permissible to charge for subject access unless the request is manifestly unfounded or excessive, particularly if it is repetitive.

Keeping Data Secure

Guidance to ensure data security includes;

- Nondisclosure of any personal data either verbally, in writing or accidentally to an unauthorised third party
- Confidential paper files kept in locked cabinets in locked premises. Files should be transported in a locked case
- Users must ensure that they always log off from their computer when away from it.
- Keeping data and devices secure (password protection, encryption, secure file storage and destruction);
- Password protection for any electronic files/documents containing confidential personal data.
- Taking particular care when transferring personal data onto a memory stick, laptop or any other mobile device and using password protection and encryption.
- Securing the sharing of personal data by email by using Egress or password protection on documents if they contain more than one piece of identifying information.
- Not storing personal data on local drives or on personal devices that are used for work purposes.
- Avoiding copying confidential personal data unless it is strictly necessary.

Reporting Security breaches

If there is a data breach, a possible breach or a "near miss" I will record are required to record this and discuss immediately with peer therapeutic practitioners so remedial action can be taken promptly.

See Reporting Data Protection and Security Information Incidents Policy..

Responsibility for Policy Heidi Pannell

Policy Operational 1.2..24

Policy review date 2.8.27

Appendix 1



Legal basis

No processing of personal data may take place unless it is within the scope of one of the six legal bases set out in GDPR. They include;

- (a) Freely given, specific, informed and unambiguous consent of the individual.
- (b) Contractual necessity.
- (c) Legal obligation.
- (d) Necessity for protecting the vital interests of an individual.
- (e) Public functions.
- (f) In the legitimate interests of Families Growing Together or a third party, provided that the Data Subject's rights, freedoms and legitimate interests are given due consideration.

Data Protection Principles

I am required to process personal data in accordance with the six data protection principles:

- Personal data must be processed lawfully, fairly and in a transparent manner.
- Personal data must be collected only for specified, explicit and legitimate purposes.
- Personal data must be adequate, relevant and limited to what is necessary for the purposes for which it is to be processed.
- Personal data must be accurate and where necessary up to date. I will take all reasonable steps to ensure that inaccurate personal data is rectified or deleted without delay
- Personal data must be retained no longer than necessary.
- Appropriate measures to ensure that personal data is secure and protected against unauthorised or unlawful processing, and accidental loss, destruction or damage must be taken.