Data Protection Policy (service users)

This policy applies to PSC staff and volunteers in respect of processing personal data about service users, as well as other stakeholders external to the organisation, such as supporters or representatives of partner organisations.

Parenting Special Children (PSC) needs to collect and store personal information ('data') in electronic format about service users for effective delivery of its services and for monitoring/impact measurement purposes. PSC uses a cloud-based Customer Relationship Management (CRM) system, Charitylog, for this purpose. PSC also needs to collect and store some personal information relating to service uses on paper.

PSC respects the private lives of individuals and recognises the importance of safeguarding personal privacy. PSC appreciates the responsibility of storing personal information and is committed to maintaining a secure environment for this, according to data protection principles as set out in the UK General Data Protection Regulation (UK GDPR) and the Data Protection Act 2018 (DPA 2018). The UK GDPR is implemented in the UK by The Data Protection Act 2018. The DPA 2018 sits alongside and supplements the UK GDPR, for example, by providing exemptions. See https://ico.org.uk/for-organisations/guide-to-data-protection/introduction-to-data-protection/about-the-dpa-2018/#2

This policy provides guidance for PSC staff, trustees and volunteers when handling personal data about service users (or other external stakeholders). A separate policy exists in respect of how PSC manages and protects the personal data of staff and volunteers.

Data Protection Register

PSC registered with the Information Commissioners Data Protection Register in October 2016 following acquisition of its CRM system Charitylog. The registration reference number is ZA213887.

Definition of key terms

This policy relates to the use of personal data, including sensitive personal data, whether it is stored electronically, on paper, or otherwise.

Personal data (or personal information) is information stored in paper form and/or electronically which relates to an individual who can be identified (a 'data subject'). Personal data is protected by data protection legislation. If there is any doubt information should be treated as personal data. Personal data does not include anonymized data.
'Sensitive' personal data is data which reveals the individual's:

- racial or ethnic origin
- political opinions

- religious beliefs
- trade union membership
- physical/mental health or condition
- sexual life and orientation
- criminal record
- genetic and biometric data

PSC is a "data controller" for the purposes of personal data of service users. This means that we determine the purpose and means of processing the personal data of our service users. We use Charitylog, a "data processor", to store our data securely.

Data protection principles

These principles have been established by law. PSC is committed to following these principles relating to personal data. GDPR specifies that personal data must be:

1. processed lawfully, fairly and transparently
2. collected and processed only for specified, explicit and legitimate purposes
3. adequate, relevant and limited to what is necessary for the purposes for which they are processed
4. accurate and kept up to date. Any inaccurate data must be deleted or rectified without delay
5. retained for no longer than is necessary for the purpose(s)
6. kept safe and secure from unauthorised or unlawful processing and accidental loss or damage

In addition, as data controller, PSC is accountable for these principles and must be able to show that it is compliant.

PSC is committed to complying with the principles above at all times. This means that PSC will:

1. inform individuals as to the purpose of collecting any information from them, as and when it is asked for
2. be responsible for checking the quality and accuracy of the information
3. regularly review the records held to ensure that information is not held longer than is necessary, and that it has been held in accordance with PSC's Data Retention Period Schedule
4. ensure that when information is authorised for disposal it is done appropriately
5. ensure appropriate security measures to safeguard personal information whether it is held in paper files or on the PSC computer system
6. share personal information with others only when it is necessary and legally appropriate to do so
7. set out clear procedures for responding to requests for access to personal information known as subject access requests
8. report any breaches of the GDPR in accordance with the procedure set out below (see section below entitled 'How to deal with Data Breaches').

How we define processing

'Processing' means any operation which is performed on personal data such as:

- collection, recording, organisation, structuring or storage
- adaption or alteration
- retrieval, consultation or use
- disclosure by transmission, dissemination or otherwise making available
- alignment or combination
- restriction, destruction or erasure

This includes processing personal data which forms part of a filing system and any automated processing.

Responsibilities of staff, volunteers and trustees

Everyone who works for, or on behalf of, PSC, whether staff or volunteer, has some responsibility for ensuring data is collected, stored and handled appropriately, in line with this policy and PSC's guidelines on Safe use of IT systems and data storage. The trustees are responsible for reviewing this policy. Staff and volunteers should direct any questions in relation to this policy or data protection to the trustees. Equally you should raise it with the trustees if you notice any areas of data protection or security that we can improve upon.

You should only access personal data covered by this policy if you need it for the work you do for, or on behalf of PSC and only if you are authorised to do so. You should only use the data for the specified lawful purpose for which it was obtained.

In addition to the guidelines set out in PSC's 'Safe use of IT systems and data storage' document you must be aware that:

- You should not share personal data informally.
- You should not share personal data with unauthorised people.

How PSC undertakes to store and manage personal data

1. **Processed lawfully, fairly and transparently:**
   PSC will undertake to ensure that:
   - The individual has given consent that is specific to the particular type of processing activity, and that consent is informed, unambiguous and freely given.
   - The processing is necessary for the performance of a contract, to which the individual is a party, or is necessary for the purpose of taking steps with regard to entering into a contract with the individual, at their request.
   - The processing is necessary for the performance of a legal obligation to which we are subject.
   - The processing is necessary to protect the vital interests of the individual or another.
   - The processing is necessary for the performance of a task carried out in the public interest, or in the exercise of official authority vested in us.

- The processing is necessary for a legitimate interest of PSC or that of a third party, except where this interest is overridden by the rights and freedoms of the individual concerned.

Disclosure of personal data
The following list includes the most usual reasons that PSC will authorise disclosure of personal data to a third party:

1. To give a confidential reference relating to a current or former practitioner
2. For the prevention or detection of crime
3. For the assessment of any tax or duty
4. Where it is necessary to exercise a right or obligation conferred or imposed by law upon PSC
5. For the purpose of, or in connection with, legal proceedings (including prospective legal proceedings)
6. For the purpose of obtaining legal advice
7. For research, historical and statistical purposes (so long as this neither supports decisions in relation to individuals, nor causes substantial damage or distress)
8. Any investigation by a statutory authority or regulator.

For PSC, the most likely reason for the disclose of personal data would be in the case of a safeguarding concern in accordance with our safeguarding policy.

2. Collected and processed only for specified, explicit and legitimate purposes:
PSC will obtain data for specific purposes and will not use it for any other purpose. PSC will only use personal data for the specific purposes the individual consented to. These purposes are likely to include:

- Provision and administration of its services
- Promoting its services
- Fundraising
- Monitoring and impact measurement of its services such as is necessary to demonstrate that the charity's work is effective as is required by funding agencies.

Data about PSC service users is collected through online registration using Charitylog web forms. Data is also collected and stored by Mailchimp when users choose to subscribe to the PSC Newsletter via the PSC website. On registration users are asked if they consent to their data being held on Charitylog and used for the purposes of service delivery and impact measurement.

These web forms feature an opt-in consent statement where users may opt to receive communications from PSC on:

1. services
2. fundraising and family activities

Each newsletter or communication has a simple "unsubscribe" option.

Other than for the reasons given in "Disclosure of personal data", above, PSC does not share information on its service users with any other agencies unless service user has given their express permission, ie in the case of a referral to another agency in order for the service user to access further support.

3. **Adequate, relevant and limited to what is necessary for the purposes for which they are processed:**
   To ensure adequate impact measurement as required by funders PSC will collect information, including sensitive personal information, related to service users'
   - family detail
   - lifestyle and social circumstances
   - education and employment details
   - physical or mental health details
   - racial or ethnic origin
   - religious or other beliefs of a similar nature

   PSC staff and volunteers will record only that data which is necessary for effective service delivery and impact measurement, or, in the case of medical or mental health needs, to ensure the health and safety of the service user and the PSC staff or volunteer working with that service user. If data given or obtained are excessive for such purpose, they will be immediately deleted or destroyed.

   We process personal information about:
   - service users
   - complainants, supporters
   - enquirers
   - advisers and representatives of other organisations (partners)

   PSC also processes information about its staff, volunteers, trustees and members of the charity, which is covered by a separate policy.

4. **Accurate and up-to-date:**
   PSC will make every reasonable effort to ensure the data obtained is accurate. PSC will rectify, delete or cease to hold data within a reasonable time of a request by the individual.

5. **Retained for no longer than is necessary for the purpose:**
   PSC will not keep data for longer than is necessary.
   Retention periods are set out in the charity's Data Retention Period Schedule.

6. **Kept safe and secure from unauthorised or unlawful processing and accidental loss or damage:**
   PSC will take all measures to prevent unauthorised or unlawful processing of personal data and accidental loss or damage. All PSC computers have a log-in system and electronic data collected by PSC will be stored on a password-protected CRM system (Charitylog) to which only authorised staff have access. Paper records, where necessary will be kept in a locked, fireproof storage system at the PSC offices to which only authorised staff have access. Staff are trained in data protection and are required to follow PSC's IT Security and Data Storage Guidelines, which should be read in conjunction with this policy.
   PSC's CRM system (Charitylog) is accredited with the Information Security Management Standard ISO 27001 committing it to hosting PSC data in a secure data centre located in the UK. All client data is held on servers operated by Rackspace which are located in the UK.

Subject access request

Data subjects can make a 'subject access request' ('SAR') to find out the information we hold about them. This request must be made in writing. If you receive such a request, you should forward it immediately to the CEO who will coordinate a response without undue delay and at the latest within a calendar month.

Access to records will be refused in instances where an exemption applies, for example, where information sharing may place the individual at risk of significant harm or jeopardise police investigations into any alleged offence(s).

It is a criminal offence to conceal or destroy personal data which is part of a subject access request. This conduct would also amount to gross misconduct under our disciplinary procedure, which could result in your dismissal.

An individual only has the automatic right to access information about themselves, and care needs to be taken not to disclose the personal data of third parties where consent has not been given, or where seeking consent would not be reasonable, and it would not be appropriate to release the information. Particular care must be taken in the case of any complaint or dispute to ensure confidentiality is protected.

All files must be reviewed by the CEO before any disclosure takes place. Access will not be granted before this review has taken place.

Where all the data in a document cannot be disclosed a permanent copy should be made and the data obscured or retyped if this is more sensible. A copy of the full document and the altered document should be retained, with the reason why the document was altered.

How to deal with data breaches

We have robust measures in place to minimise and prevent data breaches from taking place. Should a breach of personal data occur then we must take notes and keep evidence of that breach. Any and all breaches of the DPA, including a breach of any of the data protection principles shall be reported as soon as it is discovered, to the CEO. If you become aware of a data breach you must report this immediately to the CEO (or, in their absence, a trustee) and keep any evidence you have about the breach.

Once notified, the CEO shall assess:

- the extent of the breach
- the risks to the data subjects as a consequence of the breach
- any security measures in place that will protect the information
- any measures that can be taken immediately to mitigate the risk to the individuals.

Unless the CEO concludes that there is unlikely to be any risk to individuals from the breach, it must be notified to the Information Commissioner's Office within 72 hours of the breach having come to the attention of PSC, unless a delay can be justified.

The Information Commissioner shall be told:

- details of the breach, including the volume of data at risk, and the number and categories of data subjects
- the contact point for any enquiries (likely to be the CEO)

- the likely consequences of the breach
- measures proposed or already taken to address the breach

If the breach is likely to result in a high risk to the rights and freedoms of the affected individuals then the CEO or designated authority shall notify data subjects of the breach without undue delay unless the data would be unintelligible to those not authorised to access it, or measures have been taken to mitigate any risk to the affected individuals.

Data subjects shall be told:

- the nature of the breach
- who to contact with any questions; and
- measures taken to mitigate any risks.

The CEO shall then be responsible for instigating an investigation into the breach, including how it happened, and whether it could have been prevented. Any recommendations for further training or a change in procedure shall be reviewed by the trustees and a decision made about implementation of those recommendations.

Staff training

All staff and volunteers will be required to be fully conversant with this policy as part of PSC induction procedures, as well as the Privacy Notice and Safe Use of IT Systems and Data Storage. Data Protection training will be included in Charitylog training sessions and in the Training Manual for PSC staff and administrative volunteers.

Staff leaving the organisation

Staff leaving the organization will be asked to confirm that any paper records containing personal data and all PSC hardware have been returned to the PSC office for safekeeping or disposal, as appropriate.

Breach of this policy

Any breach, deliberate or negligent, by a member of PSC staff, of The Data Protection Act 2018 or this policy, is considered to be an offence and may represent gross misconduct according to the PSC Disciplinary Policy. In that event, disciplinary procedures apply.

In the case of a breach of this policy by a volunteer the matter would be dealt with by offering supervision and training to the volunteer or, where appropriate, ceasing the relationship between PSC and the volunteer, in accordance with the PSC Volunteer Policy.

Associated PSC documents and policies

This policy is to be read in conjunction with the following PSC policies:

- Safe Use of IT Systems and Data Storage
- Data Retention Period Schedule
- Privacy Notice
- Safeguarding Policy
- Confidentiality Policy
- Disciplinary Policy
- Volunteer Policy
- Charitylog Training Manual

Legislation underpinning this policy

Data Protection Act 2018
https://www.legislation.gov.uk/ukpga/2018/12/contents

General Data Protection Regulation 2018
https://www.legislation.gov.uk/ukpga/2018/12/contents/enacted

Resources used to draw up this policy

As well as the relevant legislation, this policy was drawn up with reference to:

- The RVA Data Protection Policy and the Data Control Sheets (with reference to length of time retaining personal data)
- Information Commissioners Office guidance on retaining personal data https://ico.org.uk/for-organisations/guide-to-data-protection/principle-5-retention/
- The PSC Diagnosis Support Service Confidentiality Policy
- Information Commissioners Office guidance on the use of cloud computing https://ico.org.uk/media/1540/cloud_computing_guidance_for_organisations.pdf
- ISO 27001 CERTIFICATION SUMMARY http://www.british-assessment.co.uk/services/iso-certification/iso-27001-certification/?gclid=COO7ucKdq9ECFY0aGwodpc0Bhw

Review of this policy

This policy will be reviewed by the PSC board of trustees every two years.

This policy was adopted by the trustees in July 2016
Amended September 2018, January 2021
Reviewed January 2024 no changes

Review date: January 2026