Data Protection Policy

This policy applies to all NSPCWT Representatives including, but not limited to, directors, employees, representatives, trustees, board members and volunteers.

Statement

North Somerset Parent Carers Working Together (NSPCWT) needs to collect and use certain types of information about people for its day-to-day activities. This personal information must be collected and dealt with appropriately– whether on paper, on a computer, or recorded on other material. This Policy applies to all personal and sensitive or special category data.

NSPCWT will:

- comply with the General Data Protection Regulations (GDPR) in respect of the data held about individuals
- respect individuals' rights
- be open and honest with individuals whose data is held
- ensure that everyone processing personal information understands that they are contractually responsible for following good data protection practice
- protect the organisation's parent carers, volunteers and other individuals
- provide training, support and supervision for volunteers who handle personal data, so that they can act legally, confidently and consistently
- regularly assess and evaluate methods and performance in relation to handling personal information
- protect the organisation from the consequences of a breach of its responsibilities.

NSPCWT's first priority under the GDPR is to avoid causing harm to individuals. Information about volunteers, parent carers and their children will be used fairly, securely and will not be disclosed to any person unlawfully.

NSPCWT aims to ensure that the legitimate concerns of individuals about the ways in which their data may be used are taken into account. In addition to being open and transparent, NSPCWT will seek to give individuals as much choice as is possible and reasonable over what data is held and how it is used.

Disclosure

NSPCWT may share data with other agencies such as the Local Authority and other stakeholders and voluntary agencies on an anonymised basis.

The individual will be made aware of how and with whom their information will be shared. There are circumstances where the law allows us as an organisation to disclose data (including sensitive or special category data) without the data subject's consent.
These are:

1. Processing covered by legal requirements, including safeguarding.
2. Processing for national security.

We regard the lawful and correct treatment of personal information as very important to successful working, and to maintaining the confidence of those with whom we deal.

Data Controller

NSPCWT, a non-profit CIC**,** is the Data Controller under the Act, which means that it determines what purposes personal information held, will be used for. It is also responsible for notifying the Information Commissioner of the data held or likely to be held, and the general purposes that this data will be used for.

Responsibilities

The Directors recognise their overall responsibility for ensuring that NSPCWT complies with its legal obligations.

The Data Protection Officer is Hayley Wyatt, who has the following responsibilities:

- Briefing the Directors on Data Protection responsibilities
- Reviewing Data Protection and related policies
- Advising other volunteers on Data Protection issues
- Ensuring that Data Protection induction and training take place
- Handling subject access requests
- Approving unusual or controversial disclosures of personal data
- Ensuring contracts with Data Processors have appropriate data protection clauses
- Electronic security
- Ensuring that all personal and organisational data is non-recoverable from any computer system previously used within the organisation, which has been disposed of or passed on/sold to a third party
- Approving data protection-related statements on publicity materials and letters.

Each employee, member and volunteer who handles personal data will comply with NSPCWT's operational procedures for handling personal data (including induction and training) to ensure that good Data Protection practice is established and followed.

All employees, members and volunteers are required to read, understand and accept any policies and procedures that relate to the personal data they may handle in the course of their work. Breaches of this policy will be handled under the Code of Conduct.

Confidentiality

In order to signpost to services, NSPCWT may need to share a parent carer's personal data with other agencies. Verbal or written consent will always be sought from a parent carer before data is shared.

Where anyone within NSPCWT feels that it would be appropriate to disclose information in a way contrary to the Code of Conduct, or where an official disclosure request is received, this will only be done after discussions with the Directors or the Data Protection Officer. All such disclosures will be documented.

Data Security

This section of the policy only addresses security issues relating to personal data.

Any recorded information on parent carers, volunteers and employees will be:

- Kept in locked cabinets or password-protected cloud services.
- Protected by the use of passwords if kept on the computer or encrypted if appropriate.
- Destroyed confidentially if it is no longer needed, or if an individual requests.
- If removed from the office for peer support or training purposes, it will be the responsibility of the individual staff member to keep the information secure and the information must be returned to the office as soon as practically possible.

Access to information on the database is controlled by a password and only those needing access are given the password. Directors, employees and volunteers should be careful about the information that is displayed on their computer screens and make efforts to ensure that no unauthorised person can view the data when it is on display.

Notes regarding the personal data of parent carers should be shredded or destroyed confidentially once it is no longer needed.

Data Recording and Storage

NSPCWT holds information stored in the cloud about parent carers, their families, volunteers and professionals.

NSPCWT will regularly review procedures for ensuring that records remain accurate and consistent and, in particular:

- Keep records of how and when information was collected.
- The database system is reviewed and re-designed, where necessary, to encourage and facilitate the entry of accurate data.
- Data on any individual will be held securely and all volunteers will be discouraged from establishing unnecessary additional data sets.
- Effective procedures are in place so that all relevant systems are updated when information about any individual changes.
- Effective procedures are also in place to address requests from individuals for access to, amendments or the erasure of their information.
- Directors, employees and volunteers who keep more detailed information about individuals will be given additional guidance on accuracy in record keeping in compliance with the GDPR.
- Data will be corrected if shown to be inaccurate.

Information will be stored only as long as it is needed or required by statute and will be disposed of appropriately.

As long as you are a member of NSPCWT, we will retain your data on our member database unless you request the removal of your information. If you have provided us with information about your children, once they are aged over 25, we will remove their details from our database and you will be offered the option to join us as a Supporter.

Access to Data

Information and records will be stored securely and will only be accessible to authorised volunteers, and the individual to whom the information relates.

All parent carers have the right to request access to all information stored about them. Any subject access requests will be handled by the Data Protection Officer within the required time limit.

Subject access requests must be in writing or by email. All volunteers are required to pass on anything which might be a subject access request to the Data Protection Officer without delay. In accordance with the GDPR, personal data will be provided in a 'commonly used and machine-readable format' such as a CSV file. Individuals have the right to transfer this information to another Data Controller.

Where the individual making a subject access request is not personally known to the Data Protection Officer, their identity will be verified before handing over any information.

The required information will be provided in permanent form unless the applicant makes a specific request to be given supervised access in person.

Information will be provided unless the information may cause harm to another person.

Employees have the right to access their files to ensure that information is being used fairly. If the information held is inaccurate, the individual must notify the Manager so that this can be recorded on file and updated.

Transparency

NSPCWT is committed to ensuring that in principle Data Subjects are aware that their data is being processed and:

- for what purpose it is being processed
- what types of disclosure are likely; and
- how to exercise their rights in relation to the data.

Data Subjects will generally be informed in the following ways:

- Volunteers: in the volunteer welcome/support pack/ induction
- Parent carers: when they provide their information, consent to retain it is requested, or when they request (on paper, online or by phone) services.
- Members: when they provide their information and consent to retain it is requested, or when they request (on paper, online or by phone) services.
- Staff: in the staff induction

Whenever data is collected, the number of mandatory fields will be kept to a minimum and individuals will be informed which fields are mandatory and why.

Consent

Volunteer details will only be disclosed for purposes unrelated to their work for the organisation (e.g. financial references) with their consent.

Information about volunteers may be made public according to their role, and consent will be sought for (a) the means of contact they prefer to be made public, and (b) any publication of information which is not essential for their role.

Information about parent carers will only be made public with their explicit consent (which includes photographs.) However, in some instances, such as at large-scale events where individuals are captured in an image in the background, it is not always possible to identify individuals and also due to the number of individuals in the image, not feasible for us to contact every individual in the image.

Consent will be obtained from parent carers if children's data is being stored or processed depending on the age of the child/young person, in accordance with legislation.

'Sensitive' data or 'special category' data about parent carers and their families (including health, racial or ethnic origin, religious beliefs and sexual orientation) will be held only with the knowledge and consent of the individual.

Consent should be given in writing, although for some services it is not always practicable to do so. In these cases, verbal consent will always be sought for the storing and processing of data, and records kept of the dates and circumstances. Online consent will be requested when parent carers sign up for mailing lists or message any concerns. In all cases, it will be documented that consent has been given.

All individuals will be given the opportunity to opt out of their data being used in particular ways such as direct marketing, contingent on legitimate use for the organisation.

Once given, consent can be withdrawn by the Data Subject at any time. There may be occasions where NSPCWT has no choice but to retain data for a certain length of time, even though consent for using it has been withdrawn.

Direct Marketing

Some direct communication with parent carers will be considered as unsolicited. This includes:

- promoting NSPCWT services
- promoting NSPCWT events
- promoting membership to supporters
- promoting sponsored events and other fundraising exercises
- seeking donations and other financial support
- marketing on behalf of any other external company or voluntary organisation.

Whenever data is first collected which might be used for any marketing purpose, this purpose will be made clear, and parent carers will be asked to provide their consent. NSPCWT does not have a policy of sharing lists, obtaining external lists or carrying out joint or reciprocal mailings.
NSPCWT will only carry out telephone marketing where consent has been given in advance in the signup form.

Whenever e-mail addresses are collected, any future use for marketing will be identified, and the provision of the address made optional.

Staff training and acceptance of responsibilities

All volunteers, employees and stakeholders that have access to any kind of personal data will be given copies of all relevant policies and procedures during their induction process, including this Data Protection Policy, the Code of Conduct and the operational procedures for handling personal data within NSPCWT drives and database.

Volunteers, employees and stakeholders will be expected to adhere to all these policies and procedures.

Data Protection will be included in Director training and the induction training for all Members of staff and volunteers. To be updated every two years.

We will provide opportunities for all staff to explore Data Protection issues through training, team meetings, and supervision.

Policy Review

This Policy will be reviewed and updated as necessary in response to changes in relevant legislation, changes in the legal structure of NSPCWT, contractual arrangements, and good practice or in response to an identified failing in its effectiveness.

In case of any queries in relation to this policy please contact our Data Protection Officer **Hayley Wyatt:** hayley@nspcwt.org

Appendix One: Legislative Background

The Data Protection Act 1998 gives individuals the right to know what information is held about them. It provides a framework to ensure that personal information is handled properly.

The new General Data Protection Regulations come into effect in the UK on 25 May 2018, and will replace the Data Protection Act 1998.

The Regulations states that anyone who processes personal information must comply with eight principles, which make sure that personal information is:

a) processed lawfully, fairly and in a transparent manner in relation to the data subject ('lawfulness, fairness and transparency');
b) collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes;
c) adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed ('data minimisation');
d) accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay ('accuracy');
e) kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods for statistical purposes, subject to technical and organisational measures to safeguard the rights and freedoms of the data subject ('storage limitation');
f) processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures ('integrity and confidentiality').

The Data Controller shall be responsible for, and be able to demonstrate compliance that the data is ('accountability'):

a) processed fairly and lawfully;
b) obtained only for one or more of the purposes specified in the Act, and shall not be processed in any manner incompatible with that purpose or those purposes;
c) adequate, relevant and not excessive in relation to those purpose(s);
d) accurate and, where necessary, kept up to date;
e) not kept for longer than is necessary;
f) processed in accordance with the rights of data subjects under the Act;

g) kept secure by the Data Controller who takes appropriate technical and other;
h) measures to prevent unauthorised or unlawful processing or accidental loss or destruction of, or damage to, personal information;

Appendix Two: Policy Definitions

Confidentiality: Confidential information is defined as verbal or written information, which is not meant for public or general knowledge, information that is regarded as personal by parent carers, management committee or volunteers.
Consent: of the data subject means any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her;
Data: The GDPR definition of personal data also includes information such as name, an identification number, location data including addresses, emails, phone numbers, online identifiers including IP addresses, information gathered by cookies or factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person (which could include CCTV).

The GDPR reaches further than the current Data Protection Act. It is designed to take into account modern technology and the right of the data subjects to the protection of the personal data being held by an organisation about him/her.' Data is information stored:

a) Electronically i.e. on computer, including word processing documents, emails, computer records, CCTV images, microfilmed documents, backed up files or databases, faxes and information recorded on telephone logging systems.
b) Manually i.e. records which are structured, accessible and form part of a filing system where individuals can be identified and personal data easily accessed without the need to trawl through a file.

Data Controller: The person who (either alone or with others) decides what personal information NSPCWT will hold and how it will be held or used)
Data Protection Act 1998: The UK legislation that provides a framework for responsible behaviour by those using personal information, which will be superseded by the General Data Protection Regulations on 25 May 2018.
Data Protection Officer: The person(s) responsible for ensuring that NSPCWT follows the data protection policy and complies with the General Data Protection Regulations.
Data concerning health: means personal data related to the physical or mental health of a natural person, including the provision of health care services, which reveal information about his or her health status.
Data Subject: any individual whose personal data is being processed. Examples include:

- employees – current and past
- volunteers
- parent carers and their children
- job applicants

- suppliers

'Explicit' consent: is a freely given, specific and informed agreement by an individual to the processing of personal information about them. Explicit consent is needed for processing sensitive or special category data.
Notification: Notifying the Information Commissioner about the data processing activities of NSPCWT, as certain activities may be exempt from notification.
Information Commissioner: The UK Information Commissioner responsible for implementing and overseeing the General Data Protection Regulations.
Processing: means the use made of personal data including any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.
Processor: a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller.
Personal data: means any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.
Personal data breach: means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed.

Appendix Three: Privacy Statement

When you request information from us, sign up as a member or contact us, we obtain information about you. We will ask for your consent to retain this information, and make it clear what your information will be used for.

We have a legal duty under the General Data Protection Regulations (2018) to prevent your information falling into the wrong hands. We must also ensure that the data we hold is accurate, adequate, relevant and not excessive.

Normally information we hold comes directly from you as explicit consent. When we collect information from you, we will ask for your consent to collect this information and make it clear what the purpose of this collection is. You do not have to provide us with any additional information unless you choose to.

We store your information securely on our computer system, we restrict access to those who have a need to know, and we train our staff in handling the information securely.

If you have signed up to an event, when you sign up we will ask you for consent to pass your details to the organisation hosting that event. That organisation may hold additional information about your participation in these activities. In addition, we may disclose your personal information if required to do so by law, in connection with any legal proceedings or prospective legal proceedings, and in order to establish, exercise or defend an organisation's legal rights.

We would also like to contact you in future to tell you about other services we provide, to keep you informed of what we are doing and ways in which you might like to support us. You have the right to ask us not to contact you in this way and to ask us to remove the information which we hold on you.

We will always aim to provide a clear method for you to consent for your information to be stored for this purpose. You can also contact us directly at any time to tell us not to send you any future marketing material or to remove your information by contacting us at:
Email: admin@nspcwt.org
Phone: 01934 440841

You have the right to a copy of all the information we hold about you (apart from a very few things which we may be obliged to withhold because they concern other people as well as you). To obtain a copy please email our Data Protection Officer at the address given above. There may be a charge of £10 for a copy of your data (as permitted by law). We aim to reply as promptly as we can and, in any case, within the legal maximum of 40 days.

NSPCWT's website contains links to other websites. We are not responsible for the privacy policies or practices of any third party.