Nidderdale Plus Partnership Company No 5331403; Registered Charity No 1163998

DATA PROTECTION POLICY

Last updated and approved by the Board of Trustees: 11 June 2024

Definitions

GDPR means the General Data Protection Regulation

Responsible person means Helen Flynn

Register of systems means a register or contexts in which personal data is processed by Nidd Plus

---

The Board and staff of the Nidderdale Plus Partnership are committed to ensuring compliance with the General Data Protection Regulation 2018 (GDPR) which aims to promote high standards in the handling of personal information and so protect the individual's right to privacy and are registered with the Information Commissioner. This policy reflects all personal information of living people held by Nidd Plus in an electronic format and, in some cases, on paper, for example name, address, date of birth, opinions about the individual or any other information from which the individual can be identified. The policy will also recognize the importance of gaining consent when obtaining and processing personal information.

1. Data protection principles

Nidderdale Plus is committed to processing data in accordance with its responsibilities under the GDPR. Article 5 of the GDPR requires that personal data shall be:

a. processed lawfully, fairly and in a transparent manner in relation to individuals;
b. collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving

purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be considered to be incompatible with the initial purposes;
c. adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed;
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;
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 insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes subject to implementation of the appropriate technical and organisational measures required by the GDPR in order to safeguard the rights and freedoms of individuals; and
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.
g. taking responsibility for complying with the UK GDPR at the highest management level which means Trustees and senior staff. We are accountable for ensuring we put in place appropriate technical and organisational measures.

2. General provisions

a. This policy applies to all personal data processed by Nidderdale Plus.
b. The Responsible Person shall take responsibility for Nidderdale Plus's ongoing compliance with this policy and ensure that staff receive training when necessary to ensure that they are aware of our responsibilities and procedures regarding data protection.
c. This policy shall be reviewed at least annually.
d. Nidderdale Plus shall register with the Information Commissioner's Office (ICO) as an organisation that processes personal data.

3. Lawful, fair and transparent processing

a. To ensure its processing of data is lawful, fair and transparent, Nidderdale Plus shall maintain a Data Protection Action Plan.
b. The Data Protection Action Plan shall be reviewed at least annually.
c. A Data Privacy Notice has been written and is displayed on the Nidderdale Plus website and a physical copy is also be displayed in the front office. All staff, volunteers and customers both current and future will be provided with a copy upon request.
d. Nidderdale Plus is aware that individuals have a right under the General Data Protection Regulation 2018 to get a copy of the information we hold about them online and in some manual filing systems. This is known as right of subject access. The Procedure for Subject Access Requests is at Appendix 1. Nidderdale Plus will respond promptly to any such request, within 40 working days, and may charge a fee of £10 for responding to the request.

4. Lawful purposes

a. All data processed by Nidderdale Plus must be done on one of the following lawful bases: consent, contract, legal obligation, vital interests, public task or legitimate interests (see ICO guidance for more information).
b. Nidderdale Plus shall note the appropriate lawful basis in the Register of Systems.

c. Where consent is relied upon as a lawful basis for processing data, evidence of opt-in consent shall be kept with the personal data.
d. Where communications are sent to individuals based on their consent, the option for the individual to revoke their consent should be clearly available and systems should be in place to ensure such revocation is reflected accurately in Nidderdale Plus's systems.

5. Data minimisation

a. Nidderdale Plus shall ensure that personal data are adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed.

6. Accuracy

a. Nidderdale Plus shall take reasonable steps to ensure personal data is accurate.
b. Where necessary for the lawful basis on which data is processed, steps shall be put in place to ensure that personal data is kept up to date.

7. Artificial Intelligence (AI)

a. Should we apply AI to personal date we will explain our purposes for using it.
b. Whilst it is unlikely we would use AI to make solely automated decisions about people, should this be necessary, we will advise an individual what information we may use and why it is relevant and what the likely impact is going to be.

8. Archiving / removal

a. To ensure that personal data is kept for no longer than necessary, Nidderdale Plus shall put in place an archiving policy for each area in which personal data is processed and review this process annually. The responsible person shall determine the archiving policy for each area, and be in charge of communicating this to each member of staff who is handing personal data
b. The archiving policy shall consider what data should/must be retained, for how long, and why. The archiving policy needs to be added to each database area, so that members of staff who are using the databases daily are sure about when they can delete or archive personal data that is no longer needed.

9. Security

a. Nidderdale Plus uses the Microsoft cloud data storage system, incorporating SharePoint and OneDrive, and shall ensure that personal data is stored securely on the Microsoft system and is kept-up-to-date.
b. Access to personal data shall be limited to personnel who need access and appropriate security should be in place to avoid unauthorised sharing of information. Access to areas where personal data is stored is restricted to members of paid staff who each are assigned a personal log in. No sharing of personal data is allowed with trustees, unless there is a legitimate reason for sharing specific personal data, eg recruitment purposes. Volunteers offering their time to carry out services for Nidderdale Plus, will have access to personal data only at the time of carrying out the specific tasks they are performing, for example, the volunteer drivers are given the names and addresses of the passengers who need community transport. The Register of Systems describes in more detail the processes for sharing information with volunteers when it is needed.
c. When personal data is deleted this should be done safely such that the data is

irrecoverable.

d. Appropriate back-up and disaster recovery solutions shall be in place.

10. Breach

In the event of a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data, Nidderdale Plus shall promptly assess the risk to people's rights and freedoms and if appropriate report this breach to the ICO (more information on the ICO website).

This policy will be monitored and reviewed by the trustees on an annual basis. A copy is available on our website, in our office and to our partner organisations, as required.

Appendix 1

Procedure to be followed upon receipt of Subject Access Requests (SARS)

(*Information adapted from ico.org.uk/for-organisations/advice-for-small-organisations/how-to-deal-with-a-request-for-information-a-step-by-step-guide/)*

What is a Subject Access Request?

Nidderdale Plus holds information about people stored as contacts on our computers, in notes and other documents.

By law, people can ask us for a copy of any information that's to do with them. It might be saved on our system, but if it's about them, it's their personal data, and they have a right to see it. If they ask us for a copy of it, by phone, in person, or in writing, they have made a Subject Access Request (SAR), and we need to take action.

1. Inform the data protection lead

The Nidderdale Plus Data Protection Lead is Helen Flynn; in her absence Richard Bruce, Chair of Board of Trustees should be informed.

2. Confirm the identity of the person making the request if necessary

If the requester is unknown to staff members, check their identity quickly. Do not ask for formal ID unless it's necessary and proportionate. Instead, ask questions that only they would know – for example about services they have used. Or ask for ID that we can actually verify. There's little point insisting on photo ID if we don't know what the requester looks like – it should be proportionate.

3. Check the request is valid

If the SAR is made by someone other than the person the data is about (such as a friend, relative or solicitor), check they're allowed to have it. Request to see that they have written authority to act on behalf of the person concerned, or a document showing general power of attorney.

Note: In most cases, children over 12 are capable of making their own SARs. If asked for personal data about a 12-year-old by their parent or carer, permission should be obtained from the child first. Contact the Information Commissioner's Office on 0303 123 1113 to speak to a member of the team if not sure.

4. Set reminder

Set a reminder in the calendar to complete the SAR and send it to the relevant person within 28 days. If an ID check is required or other information, the one month time limit can be extended until their reply is received. Any additional information must be requested as soon as possible.

There are three important things to remember about the one calendar month timeframe:

1. It doesn't matter if the day we receive the request isn't a working day. For example, if we receive a request on Saturday 7 March, we should respond by Tuesday 7 April.

2. If the SAR's due date falls on a weekend or a public holiday, we have until the next working day to respond. For example, if we receive a request on 25 November, we should respond by 27 December.
3. We can't add extra days when the calendar month is shorter. For example, if we receive a request on the 31 January, we should respond by the 28 February.

If it's a very complex request, or if the requester has made a lot of requests, an extra two calendar months can be taken to respond. The requester must be advised there will be a delay before the end of the first calendar month. For further info, check https://ico.org.uk/for-organisations/advice-for-small-organisations/frequently-asked-questions/right-of-accesssubject-access-requests-and-other-rights/#howdoi

5. Check what exact data they have asked to see

Read written requests carefully. Do not assume they're asking for everything we've got, when in fact they've only asked for data relating to one particular thing. They might even be able to give us advice on how to find it.

6. Search for the relevant information

Use the search functions on computers (including archived files), and email folders to find information relating to the person. Think creatively about all the places where this information might be held. Check tablets, portable memory sticks, call recordings and social media posts. Keep looking until satisfied all areas have been checked.

7. Check what may need to be redacted

Carefully read through the information identified to make sure it really is their information.

Redact (black out) any information which **doesn't** relate to the person making the SAR. Alternatively copy and paste sections relevant to the SAR into a separate document for issue instead.

Note: If using a computer to redact information, to avoid the risk of the blacked-out sections being deleted and the text underneath being read, cut and paste in a separate document and ensure the final version is saved as a pdf.

8. Consider the impact of releasing data about other people

In the event of the personal data including information that is closely linked to someone else, the personal data must still be released as requested. But if we may disclose data about someone else as a result, the impact of that must be considered.

When responding to a SAR in these situations there can be lots to consider, contact the ICO on 0303 123 1113 for support.

9. Prepare the reply

If the SAR was received via by email, the reply should also be sent by email, unless the requester has said otherwise. Ascertain what format they'd like it sent in and ensure steps 7 and 8 have been considered.

10. Send the reply securely and keep a record of what has been sent

In addition to the requester's personal data, the Nidd Plus privacy information document should also be included. The individual has a right to know why we hold their data, how we got it, how long we're planning on keeping it, who we share it with, and how they can ask for it to be changed (such as updating their address) or deleted. Record the date and the information sent as we may need to refer to it again, for example if they're unhappy with our response or make another request soon after.