Data Protection Policy

1. Introduction

Northumberland National Park Authority is committed to protecting the privacy of individuals including its customers, staff and the partners it works with. The organisation has developed policies and procedures to ensure compliance with the new General Data Protection Regulations. These documents, along with this policy, form part of the information governance framework for the organisation.

The new data protection regulations require that organisations are transparent and accountable for management of personal information. This includes publication of a privacy notice, which sets out why the authority collects information and how it is used as well as procedures for managing data breaches and subject access requests. The data protection policy sets out the framework for meeting compliance requirements for GDPR.

2. Background and scope

As part of its day to day business and in order to provide the best service to its customers the authority collects personal and sometimes special categories of information from individuals. This information may be collected via online forms, emails, on paper, by telephone or CCTV, a camera or smartphone. Information is stored electronically and on paper, on camera or uploaded to websites and sometimes personal information may need to be transferred to other organisations or held on external platforms.

The authority takes its responsibility to protect personal information seriously and is committed to ensuring it is collected only for the purposes agreed and also stored securely. The authority may need to hold information for longer periods to comply with financial or employment legislation, or if required for a criminal investigation. A retention schedule is in place to ensure that information is not held longer than necessary.

The policy applies to customers, staff, residents and members of Northumberland National Park.

3. The Data Protection Principles

Article 5 of the GDPR sets out seven key principles for data collection and processing. The first six principles are related to ensuring that personal information is properly collected, stored and processed. The seventh principle, accountability, is linked to demonstrating compliance with the preceding six principles. Northumberland National Park Authority will ensure compliance with the principles as described below:

1. Lawfulness, fairness and transparency – data will be processed lawfully, fairly and in a transparent manner in relation to individuals.
2. Purpose limitation – data will be 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.
3. Data minimisation – data should be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed.

4. Accuracy – data should be 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.

5. Storage limitation – data shall be 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.

6. Integrity and confidentiality (security) – data shall be 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.

7. Accountability – The controller shall be responsible for, and be able to demonstrate compliance with the other data protection principles.

4. Rights of individuals

The GDPR sets out specific rights for individuals in relation to personal information held about them. These rights are detailed in Table 1 below:

Table 1.

| 1. The right to be informed | To be informed why, where and how we use your information |
| 2. The right of access | To ask for access to your personal information |
| 3. The right to rectification | To have any errors about your personal data amended |
| 4. The right to erasure | Asking us to remove personal information about you |
| 5. The right to restrict processing | To ask us to stop processing or restrict use of your personal data |
| 6. The right to data portability | Asking us to move, copy or transfer your personal information in a safe and secure way |
| 7. The right to object | Being able to object about how your personal data is used |
| 8. Rights in relation to automated decision making and profiling. | Being able to challenge decisions made by automated profiling (no human intervention) |
4.1 Policy information relating to individual’s rights

Individuals have the right to be informed about the collection and use of their personal data. This is a key transparency requirement under the GDPR. We will provide you with information including: the purposes for processing your personal data, our retention periods for that personal data, and who it will be shared with. We call this ‘privacy information’.

We will provide privacy information at the time we collect your personal data from you. Our privacy notice is published on our website.

If we obtain your personal data from other sources, we will provide you with privacy information within a reasonable period of obtaining the data and no later than one month after.

There are a few circumstances when we do not need to provide you with privacy information, such as if you already have the information or if it would involve a disproportionate effort to provide it to you.

The information we provide to you will be concise, transparent, easily accessible, and will use plain language.

We will regularly review, and where necessary, update our privacy information. We will bring any new uses of your personal data to your attention before we start the processing and obtain consent from you if it is required.

5. Specified, Explicit, and Legitimate Purposes

Article 6 of the GDPR requires organisations to have a lawful basis for processing personal information. The regulations set out six lawful bases for processing; consent, contract, legal obligation, vital interests, public task and legitimate interests. Northumberland National Park Authority collects and processes information within four of these areas: public task, contract, consent and legitimate interests. Below is further information regarding the lawful basis for processing.

5.1. Public Task

The authority has a requirement to collect and process data for planning purposes. Personal information is collected under the public task basis for the purposes of meeting the statutory obligations relating to its planning functions.

5.2. Contract

The authority has numerous contracts with staff, partners and other organisations. This could be for financial purposes or in relation to land management agreements. For GDPR purposes any personal information collected as part of this process is done within the contract basis.
5.3. Consent

The authority collects personal information for a variety of purposes, from customers signing up for newsletters, to enquiries from volunteers. The GDPR requires that consent is sought for personal information collected in this way. We will provide clear, specific information about why we are asking for your personal information and what we will do with it so that your consent is based on an informed choice.

Where the authority collects personal information relating to children, it will ensure that consent is given by a parent or legal guardian where the child is under 13 years of age. Children over 13 years of age are able to provide their own consent. Children have the same rights as adults in relation to personal information we hold about them. We will ensure that where we are seeking consent to process personal information relating to children we will explain why we are doing so in a way that is clear and easy to understand.

5.4 Legitimate interest

The authority may at times be required to send information to stakeholders including tenants, landowners and others living or working in the national park. For this reason there is a legitimate interest to maintain a database of these individuals. A Legitimate Interests Assessment was undertaken to determine whether this lawful basis was appropriate and that the interests of the organisation did not outweigh those of individuals. A copy of the LIA can be provided on request.

6. Data Protection Impact Assessments

Northumberland National Park Authority will carry out a Data Protection Impact Assessment (DPIA) for all projects where personal information is expected to be collected or processed and for activities involving large scale processing, profiling or monitoring of data. The Data Protection Officer will provide advice and guidance. DPIA’s are carried out to identify and minimise the data protection risks and we will publish DPIA’s on our website.

7. Subject Access Requests

You have the right to request copies of information that we hold about you. This includes:

- confirmation that we are processing your personal data;
- a copy of your personal data;
- other supplementary information – please refer to our privacy notice for details

You are only entitled to information about you; we will not provide you with information about other people. A Subject Access Request can be made using a form which is available on our website. We will ask for proof of identity before we process your request.

We do not normally charge for this service. However where a request for information is excessive or multiple requests for the same or similar information are made we may charge a fee for the administrative costs to comply with your request. We reserve the right to refuse a request for information which is manifestly unfounded or excessive. If this happens we will inform you of our decision.
8. Data Security

Where personal information is collected, held and processed by us, we will take steps to ensure this is carried out securely. We have in place technical and organisational measures to reduce or remove the risk of a data breach or data loss. This applies to information in paper and electronic formats.

In the unlikely event that a data breach or data loss occurs, a procedure is in place to stop, inform, investigate and report the incident. A summary of the process is shown below and a copy of the data breach policy and procedure is available on request.

8.1. Stop

As soon as a breach or data loss has been detected we will take steps to stop the breach. This could include changing passwords for online services, changing locks on doors and cabinets for paper documents or removing access rights for individuals to electronic or manual information.

8.2. Inform

We will inform individuals who may be affected by a personal data loss or data breach as soon as possible. We will provide details of the personal information about them which may have been accessed or lost.

8.3. Investigate

We will carry out an investigation into the data breach or loss and review systems and processes to remove the risk of future breaches.

8.4. Report

We will inform the Information Commissioners Office where necessary and provide them with details relating to the breach.

9. IT Security

The following measures are in place to ensure personal information stored and processed on computers and other devices is securely held:

- all laptops and memory sticks are encrypted
- user passwords are changed every 30 days
- all sites are protected by enterprise-grade firewalls
- all data traffic between offices, home workers and head office, is encrypted
- the website is protected by Cloudflare and Siteground
- the administrator password is changed every 6 months
- website communication to Customer Relationship Management and Electronic Point of Sale systems is encrypted
- the website is encrypted

9.1. Testing
The Authority will undertake regular stress and penetration testing of its network and information systems. The results of the testing will be documented and appropriate safeguards will be implemented accordingly.

9.2. Confidentiality, integrity, availability and resilience

Confidentiality, integrity and availability are three key elements of information security. The information security measures we use seek to guarantee all three for our systems and the personal information we process.

Resilience applies when our systems have to operate under adverse conditions, such as those which may result from a physical or technical incident; and our ability to restore them to an effective state.

A business continuity plan is in place to ensure that the organisation can continue to operate if a technical, operational or other incident occurs.

9.3. Transferring Personal Data

Sometimes the personal information we collect may be stored on servers outside the EU. Where this occurs we will notify you of this. Data processing agreements will be put in place relating to personal information processed by a third party, including outside the EU. More information about this is included in our Privacy Notice.

10. Disposal of data

Our data retention policy outlines the process and schedule for disposal of data, including personal information. All data will disposed of in a secure manner; this includes proper cleansing or destruction of computers and other devices. Information held in paper format will be disposed of by secure shredding.

11. Staff awareness and training

All staff in the organisation will undertake training to ensure they comply with GDPR. Training will also be part of the induction process for new employees. Staff will be trained to ensure the following:

- They understand their obligations under GDPR
- They can identify potential data security risks
- They can identify when a data breach or data loss has taken place
- They can follow procedures should a data breach or loss take place
- They understand the privacy requirements relating to the collection of personal information
- They know the procedure to deal with subject access requests
12. Contact details:

For enquiries relating to this policy please contact our Data Protection Officer as shown below:

Email: dpo@nnpa.org.uk

Telephone: 01434 605555

Address:

Data Protection Officer
Northumberland National Park
Eastburn
South Park
Hexham
NE46 1BX

<table>
<thead>
<tr>
<th>Version</th>
<th>Approved by</th>
<th>Date</th>
</tr>
</thead>
<tbody>
<tr>
<td>Draft version 1 090518</td>
<td>Data Protection Officer</td>
<td>07/08/2018</td>
</tr>
<tr>
<td>V2</td>
<td>Data Protection Officer</td>
<td>28/09/2018</td>
</tr>
<tr>
<td>V2</td>
<td>NNPA Leadership team</td>
<td>02/10/2018</td>
</tr>
<tr>
<td>Final</td>
<td>Data Protection Officer</td>
<td>04/10/2018</td>
</tr>
</tbody>
</table>

Next review date: May 2019