# NEW FOREST NATIONAL PARK AUTHORITY (NPA)

# Data Protection Policy

| | |
|---|---|
| Author: | Information and Data Protection Officer |
| Approved by: | Resources, Audit and Performance Committee |
| Approval date: | 9 September 2024 |
| Review date: | September 2028 |
| Version: | 2.0 |
| Distribution list: | Internal and External (website) |
| Classification level | Public |

## 1. Introduction

1.1 This Policy sets our how the New Forest National Park Authority (NPA) meets its obligations under the UK General Data Protection Regulation (UK GDPR) and the Data Protection Act 2018 (DPA 18).

1.2 This policy applies to all the processing of personal data carried out by the NPA, including processing carried out by joint controllers, contractors and processors.

1.3 We take the key principles of data protection very seriously. These six principles require that personal data is:

- processed lawfully, fairly and in a transparent manner;
- collected for limited, specified, purposes and not further processed in a manner that is incompatible with those purposes;
- adequate, relevant and limited to what is necessary;
- accurate and, where necessary, kept up to date;
- not kept for longer than is necessary; and
- kept safe and secure.

1.4 In addition, the accountability principle requires us to be able to evidence our compliance. We have in place policies and procedures to ensure compliance with the legislation.

1.5 We need to collect and use information about individuals in order to carry out our day to day operations. In general, we hold individuals' contact and other information in order to help us to achieve our two purposes, as well as our socio-economic duty. There are also more specific reasons why we need to use individuals' information, and these vary depending on the service or project in question. For example, some processing of personal data is necessary for the performance of our statutory functions such as planning and enforcement.

1.6 When individuals supply any personal information to us, we have some legal obligations in the way we handle it. The starting point is that people's personal data belongs to them and not to us, and privacy and security need to be at the heart of everything we do. In brief, we must collect the information fairly – for example, we must collect it only on the bases set out in the legislation, we must hold it securely, we must explain how we will use it to the individuals(s) in question, and we must comply with individuals' rights over their information.

## 2. What is personal data?

2.1 The UK GDPR definition of "personal data" includes any information relating to an identified or identifiable natural living person.

2.2. Pseudonymised personal data is covered by the legislation, but anonymised data is not regulated by the UK GDPR or DPA 18 providing that the anonymisation has not been done in a reversible way.

2.3 Some personal data is more sensitive and is afforded more protection, this is known as special category personal data and is related to:

- Race or ethnic origin;
- Political opinions;
- Religious or philosophical beliefs;
- Trade union membership;
- Genetic data;
- Biometric ID data;
- Health data;
- Sexual life and/or sexual orientation; and
- Criminal data (convictions and offences)

## 3. Good data protection principles and practices

3.1 Personal information must be dealt with properly however it is collected, recorded and used, whether on paper, or in electronic or other format. This is not only because we need to comply with the relevant law, but also because the fair and lawful treatment of personal information is important to the successful operation of our business and to maintaining the confidence of our staff and the individuals and organisations with whom we have contact.

3.2 Public authorities must appoint a Data Protection Officer (DPO). The DPO is primarily responsible for advising on and assessing our compliance with the DPA 18 and UK GDPR and making recommendations to improve compliance. Staff must discuss any proposed new processing or changes to processes that involve personal data with the DPO. Our DPO can be contacted at dpo@newforestnpa.gov.uk or by telephone on 01590 646653.

3.3 We have a process for considering any data breaches and a reporting process for assessing whether we need to report the breaches to the Information Commissioner and / or notify the affected data subjects.

3.4 We require all staff to undertake mandatory data protection and cyber security training. All new starters receive an in-person data protection induction from the DPO.

3.5 We have a process for handling subject access requests and other information rights requests or queries. These are undertaken by our DPO.

## 4. What personal data do we process?

4.1 We collect information from individuals in these categories, among others:

- users of the planning service;
- people who complain about enforcement matters, and the people who own the relevant sites;
- other users of particular services, such as people interested in the work of the New Forest Land Advice Service, people complaining or asking for information, and those who subscribe to newsletters;
- volunteers;
- people who use our website (see 'cookies' section below);
- parish and town councillors;
- job applicants, employees and members of the NPA;
- people who work for other stakeholders in the New Forest who contact us, such as employees of Forestry England or New Forest District Council;
- people with whom we collaborate on shared projects;
- people who use and respond to our social media pages and posts;
- people we meet at our outreach events, including the work we do with schools, at the New Forest Show, the Volunteering Fair, or in connection with particular projects; and
- people who fill in surveys and consultations.

4.2 Personal data is more than just the names, contact details and signatures of individuals. It is any information that relates to an individual even if, on its own, it is not enough to identify them. It includes personal opinions, images biometric data, IP addresses and computer cookies.

4.3 Information can be collected in a variety of ways, such as via the website, social media, through specific forms, at our offices, by phone or email, or at events.

## 5. How we hold and process information

5.1 We must ensure that we:

- build in good data protection as a default in everything we do;
- fully observe the conditions regarding fair collection and use of information and meet the principles of good data protection practices set out in the UK GDPR and DPA 18;
- ensure that we fully assess the privacy implications of our personal data processing, establish and – importantly – audit our lawful basis for this processing, and keep people informed using privacy notices;
- seek consent where necessary and file it with the relevant records, and ensure we comply with the conditions of consents we have obtained;
- train our staff and members on data protection;
- collect and process appropriate information only to the extent that it is needed to fulfil operational needs or to comply with any legal requirements;
- ensure the quality of information used;
- keep our retention schedule up to date and apply checks to determine the length of time information is held;

- ensure that we comply with individuals' personal data rights as detailed in the legislation;
- seek continuous improvement in our records management practices;
- deal with all enquiries about the handling of personal information promptly and courteously;
- take particular care when dealing with information that is categorised as special category data in the relevant legislation, and information that relates to children and vulnerable adults;
- take appropriate technical and organisational measures to safeguard personal information; and
- ensure that personal information is not transferred abroad without suitable safeguards.

5.2 In more detail, we must always determine our lawful basis for all processing prior to collecting or undertaking the processing. In some cases, we need individuals' contact information so that we can provide services or information that have been requested, such as when we determine planning applications or respond to information requests. In some cases, we might need some information that goes beyond contact details – for example, if someone is making a planning application, we might need some information on how they use or intend to use their home. There may also be times when we ask for this sort of information in a formal capacity – for example, during an enforcement investigation we might issue a Planning Contravention Notice. Where we need to use individuals' information for reasons of this type (to allow someone to access a service or respond to an investigation), we do not need to ask for consent to collect and use this information. This is because we must use it in our capacity as the local planning authority or because we have another good reason why we need to use the information. In these cases, staff need to make sure they are clear that this is the case and if necessary, consult the DPO.

5.3 There may also be times when we do not need individuals' contact information but we would like to use it in order to keep people informed about and/or invite them to participate in events and services that might interest them, or to share e-news with them. Occasionally we also collect information from individuals that goes beyond contact details – for example, volunteering interests or availability. In all these circumstances we will let the relevant individuals know that that is how their information will be used when we collect it, and where necessary we will ask for consent for this. Again, staff are encouraged to consult the DPO for help and guidance on how to do this.

5.4 We take individuals' privacy very seriously. Personal data must never be supplied to anyone outside the NPA without first obtaining the relevant individuals' consent, unless we are obliged by law to disclose it, or it would otherwise be fair to do so and we are permitted by law to use it in this way. An example of when we might be legally obliged to disclose individuals' data would be if the police ask to see some information to help them to solve a crime or to protect someone. An example of where it might otherwise be

lawful for us to disclose data would be if someone made a request for information under the Freedom of Information Act 2000. In these circumstances we would carefully consider whether it would be appropriate and fair to disclose individuals' data, including factors such as what we think the individual in question might expect us to do with their data and whether they have consented to its release. If we would like to share individuals' information with third parties for reasons such as that it would be useful to us or them – for example, sharing with other stakeholders on a joint project, or with planning consultants, or with bodies to which we might outsource types of administration such as payroll – we will always let the individuals know, and where necessary we will ask for explicit consent. Staff should consult the DPO as necessary.

5.5 Personal data must be collected for a specified, explicit and legitimate purpose and we will not further share information internally in a manner that is incompatible with the initial purpose. Staff should seek the advice of the DPO if internal sharing between departments or projects is being considered.

5.6 Staff are reminded to keep personal data secure at all times. This means complying with the ICT Policy, introducing good filing practices such as locking paper copies away, and deleting or securely destroying data when the purpose for collecting it is fulfilled. There are confidential (blue) waste bins provided on every floor for staff use.

5.7 Any requests received from individuals for the exercise of their information rights must be forwarded to the Information and Data Protection Officer as soon as possible.

## 6. Cookies

6.1 We need permission to save non-essential cookies on users' machines when they use our website. Cookies are small files which are sent to the browser (for example Internet Explorer) and stored on the computer's hard disk. They only identify the computer and not individual.

6.2 We use cookies to measure site usage such as entry and exit points of visitors, how many people visit a certain section or page, and details of searches performed and related information. More information regarding Cookies is available on our website Privacy and cookies - New Forest National Park Authority (newforestnpa.gov.uk)

## Glossary of terms

**Personal data** - Any information relating to an identifiable living individual who can be identified from that data or from that data and other data. This includes not just being identified by name but also by any other identifier such as ID number, location data or online identifier, or being singled out by any factors specific to the physical, physiological, genetic, mental, cultural or social identity of the individual.

**Processing** - Anything that is done with personal data, including collection, storage, use, disclosure, and deletion.

**Special category personal data** - Personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying an individual, data concerning health or data concerning an individual's sex life or sexual orientation.

**Controller** - The organisation (or individual) which, either alone or jointly with another organisation (or individual) decides why and how to process personal data. The controller is responsible for compliance with the DPA and GDPR.

**Processor** – An organisation (or individual) which processes personal data on behalf of a controller.

**Personal Data Breach** - 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.

**Pseudonymisation** - The processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organisational measures to ensure that the personal data are not attributed to an identified or identifiable natural person.

**Version history**

| Version | Changes made | Date | Made by | Sign off / adopted |
|---|---|---|---|---|
| 2.0 | Complete revamp and format of Policy | 9 Sept 2024 | Jo Murphy (DPO) | RAPC |
| | | | | |