Peak District National Park Authority
Data Protection Policy
September 2020

Version	Author	Approved By	Approval Date	Publication Date	Review Date
1.0	**MS**	**Head of Information Management**	**18/05/2018**	**21/05/2018**	**21/05/2020**
1.1	**MS**	**DPO**	**04/09/2020**	**04/09/2020**	**21/05/2022**

Introduction

We routinely collect process and on occasion, share personal data. This data can identify (directly or indirectly) living individuals and can be found in both paper and electronic files (including databases), as well as visual and audio recordings The data will relate to, our employees, members, casual staff, and volunteers, users of our services, grant recipients and those making donations, consultees and survey responders, suppliers and contractors and members of partner organisations.

We are committed to ensuring that personal data is handled in line with the General Data Protection Regulation. To comply with the law, personal information will be collected and used fairly, stored securely and not disclosed unlawfully.

Processing personal data inappropriately or otherwise failing to protect can result in significant financial and reputation damage as well as the potential to cause damage and distress to individuals.

Contents

Purpose

The aim of this policy is to ensure that everyone handling personal data is fully aware of the requirements and acts in accordance with data protection procedures and that we properly respect the rights of data subjects.

Legislative Background

The General Data Protection Act 1998 (GDPR) and the UK Data Protection Act. The primary objectives of the GDPR are to give individuals more control over their personal data and how it is processed and to simplify the regulatory environment ensuring consistency across the EU member states. The idea behind the Bill is to fill in some of the gaps in the GDPR.

Definitions

This policy implements the requirements GDPR. It also incorporates guidance from the Information Commissioners Office (ICO) which is the UK's supervisory authority with responsibility for enforcement.

For the purpose of the policy the term '**Data**' means personal information which is collected, held, processed or recorded in a manner that is accessible as part of a structured filing system or classed as 'category e' data*[1]

Personal data means data relating to a living individual who can be identified:

- From the data
- From the data and other data which is in the possession of, or is likely to come into the possession of the organisation.
    - Includes any expression of opinion about the individual and any indication of the intentions of the organisation or any other person in respect of the individual

Sensitive personal data means personal data consisting of information relating to:

- Racial or ethnic origin
- Political opinions
- Religious beliefs
- Trade union membership
- Physical or mental health
- Sexual life

[1] The Freedom of Information Act 2000 introduced a right of access for individuals to information held by public bodies. Section 68 of the Act created a new category (e) in the Data Protection Act definition of 'data' in order to provide protection for information about individuals, held by public bodies in paper files or unfiled records, in the face of the FOI access regime.

- Convictions of offences

The GDPR refers to sensitive personal data as **'special category data'**. These categories are broadly similar to those in the Act, with some minor changes:

- Inclusion of genetic and biometric data
- Removal of personal data relating to criminal convictions (similar extra safeguards apply to its processing).

While the data protection principles under the GDPR are similar to those found in in the Data Protection Act, certain concepts are more fully developed.

Lawfulness, fairness and transparency	***We will process personal data lawfully, fairly and in a transparent manner in relation to the data subject***
Purpose limitation	***We will collect personal data for specified, explicit and legitimate purposes and not further process it in a manner that is incompatible with those purposes***
Data minimisation	***The personal data we collect shall be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed***
Accuracy	***The personal data we collect shall be accurate and, where necessary, kept up to date***
Storage limitation	***We shall keep personal data in a form that is necessary for the purposes for which the personal data are processed***
Integrity and confidentiality	***We shall process personal data 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***
Accountability	***As a data controller we will be responsible for, and be able to demonstrate compliance with the GDPR***

The definition of 'processing' is obtaining, using, holding, amending, disclosing, destroying and deleting personal data. This includes some paper based personal data as well as that kept on computer as the GDPR covers manual data too.

A **data controller** determines the purposes for which and the manner in which any personal data are, or are to be, processed. We are a data controller.

A **data processor** is any person (other than an employee of the data controller) who processes data on behalf of the data controller. The data processor operates only on instruction from the data controller.

Types of information processed

We process the following personal information:

- Information on applicants for posts including references;
- Employee and volunteer information – contact details, financial details for payroll, sickness records, training and performance records and JPAR assessments;
- Member contact details;
- Service user information – financial information for payments including planning and grant funding, contact details, date of birth, health information.

Personal information is kept in the following forms:

- Electronic files (including Word, PDF and Excel formats) on a shared network which is maintained as part of a cloud service (Information as a Service via Server Choice);
- Electronic databases and programs located on a shared network (see above);
- Paper files held onsite in an access controlled area, also in files held within locked cabinets within the Finance, CBST, HR, Legal Service and Planning offices;
- Paper files held offsite in Ranger offices and Information Centres – the files are not accessible to members of the public.

Groups of peoples within the organisation who process personal information:

- Employed staff; the following will have access to special category data;
    - HR staff
    - Administrative staff , volunteers and group leaders as part of our outreach work
- Members;
- Volunteers;
- Third parties with whom we've entered into a partnership agreement or have entered into a data sharing agreement.

Records of Processing Activities

Under the GDPR we will no longer be required to register with the ICO and provide them with details about the way we process personal information. Instead we will need to maintain a record of processing activities (ROPA) which should document the purpose(s) for processing, data sharing and retention. The ICO can ask to inspect the ROPA and it will be form an integral part of an ICO investigation in the event of a reported breach.

Scope and Responsibilities

The policy applies to

- All personal data that we process, across all our locations and regardless of format
- All staff as referenced in the Introduction, who have access to and use the information
- All third parties as referenced in the Introduction who have access to the information and may be responsible for processing the information on our behalf

Overall responsibility for personal data processed by the PDNPA rests with the Leadership Team. The Leadership Team delegates tasks to the Data Protection Officer (DPO). The DPO is responsible for:

- Understanding, interpreting and communicating obligations under the GDPR;
- Identifying problem areas or risks;
- Producing clear and effective procedures including advising on data privacy impact assessments;
- Staff training;
- Ensuring that records of processing are accurate and up to date;
- Managing the rights of data subjects – subject access requests, data portability and requests for erasure of personal data;
- Managing potential breaches including liaising with the ICO.

Michele Sarginson is the PDNPA's Data Protection Officer. Contact 01629 816278, email michele.sarginson@peakdistrict.gov.uk.

Responsibility for all IT issues including computer security lies with Head of Information Management.

Breach of this policy could result in disciplinary action, termination of volunteering opportunities, removal of access to specific systems/data and/or removal of all access to all IT services and authority data.

Policy Implementation

All employed staff, Members, volunteers and third parties who process personal data must ensure that they not only understand but also act in line with this policy and the principles set out in the GDPR.

To meet our responsibilities we will:

- Ensure any personal data is collected in a fair and lawful way;
- Explain why it is needed at the start;

- Ensure that only the minimum amount of information needed is collected and used;
- Ensure the information used is up to date and accurate;
- Review the length of time information is held;
- Ensure it is kept safely;
- Ensure the rights people have in relation to their personal data can be exercised.

We will ensure that:

- Everyone managing and handling personal information is trained to do so.
- Anyone wanting to make enquiries about handling personal information, whether a member of staff, volunteer or service user, knows what to do;
- Any disclosure of personal data will be in line with our procedures.
- Queries about handling personal information will be dealt with swiftly and politely.

Gathering and checking information

Before personal information is collected we will consider what details we need to fulfil the purpose and the length of time we may need to retain it for.

We will inform people about our data collection, specifically why we are collecting the information, what we will use it for, who will have access to the information (including any third parties it may be shared with), how long we will keep it for, and their rights regarding the data (for example, making a subject access request or asking for us to delete the data we hold – “the right to be forgotten”) and their rights to complain to the Information Commissioner.

It is important to remember that data is not always collected directly from individuals but may be derived from other data sets, observed by tracking or inferred using algorithms (for example via website cookies and analytics).

We will identify instances where consent is needed from data subjects

Before we share personal data with others (ie persons who are not Members or Officers of the Authority), we will agree with the other party/parties a protocol which explains what procedures need to be followed. Whenever data is provided to an agency or individual outside of the Authority, details of the disclosure must be recorded on the appropriate record

Changes to the use of personal data and new arrangements for sharing or providing data may not take place without prior reference to the DPO to ensure that data protection issues are properly addressed

We will provide this information in various privacy notices that will be published on our website and also in privacy statements included in our various forms.

We will take the following measures to ensure that personal information is kept accurate:

- Send out reminders via email as part of our business as usual process;
- Provision of customer portals where available to allow users to update their own information and preferences.

Special category information will not be used apart from the exact purpose for which permission was given, unless we have sought and received explicit consent, or where special conditions apply, such as to protect the vital interests of the individual (for example in a life threatening situation where the individual is not able to give consent) .

Data Security

This section explains how we will ensure the security of the personal data we process. Unauthorised disclosures can lead to criminal prosecutions and breaches of the principles can result in fines of up to 20 million euros. Breaches can also cause a loss of reputation.

We will take steps to ensure that personal data is kept secure at all times:

- Clear desk policy and Lockable cabinets
- Appropriate electronic security measures including passwords, encryption and access control measures.
- Limit data taken off site
- Shredding of hard copies of personal data – offsite by certified bureau as appropriate
- Security access to buildings
- Frequent password changes
- Implementation of data sharing agreements
- Review of contracts to ensure that where personal data is involved, the supplier can comply with requirements of GDPR
- Offsite back-ups
- Undertake data privacy impact assessments for new systems or processes involving personal data where the nature of the processing and the volume of personal data might pose a risk to the data subject.

Breaches of Data Security

Any breaches or suspected breaches of data security should be reported immediately to the DPO who will work with the Head of Information Management and other relevant officers as required, to decide an appropriate course of action. “Significant” breaches, where the potential harmful impact of such a breach is regarded as high, may have to be reported to the ICO. The DPO and Head of

Information Management will make a judgement on whether a reported breach is significant.

Managing the rights of the data subject

Under the GDPR the data subject (the person to which the data relates) has an enhanced number of rights:

- To know what information we hold and process;
- To know what it is used for;
- To know who it is shared with;
- To know how long it is retained for;
- To ask for it to be deleted;
- To ask for us to provide it in a portable format so that they can transfer it easily to another organisation;
- To ask for us to stop processing in relation to direct marketing;
- To request us to correct, rectify, block or erase information regarded as wrong;
- To ask us not to use an automated decision making process, or have an automated decision reviewed by a person.

They also have a right to have a copy of the information related to them and this must be done within one month. We can no longer charge a fee (unless for additional copies), but we may be able to refuse if it is deemed 'manifestly unreasonable', alternatively we may extend the time for providing the information if the request is complex.

We must advise them of their rights, usually through our privacy notices or as an inclusion on any forms. We may also do this verbally.

Requests should be addressed to the Data Protection Officer; this can be done via Customer and Business Support.

We cannot force them to complete a form, but it will help us to locate the information if they are willing to do so. A copy is available on our website. We will also ask for some forms of ID such as a driving licence, passport or utility bill. We can also accept a request on someone else's behalf; however we will need written authorisation.

Additional Data Policies and guidance

This policy form part of a suite of policies and guidance which are available on the HUB. Their purpose is to explain key elements of the GDPR and how we will implement them into the work that we do. More information is available on:
Clear Desk Policy

Data Sharing Protocol

Managing a Subject Access Request

Role of the Data Protection Officer

Undertaking a Data Protection Impact Assessment

Data Controllers and Processors

Managing Consents

Data Breach Process

Privacy Notices

Records Retention

Information Management Policies Framework

Review

This policy will be reviewed at intervals of 2 years to ensure it remains up to data and compliant with the law.