



Peak District National Park Authority Guidance note – Ad hoc data disclosure

Version	Author	Approved By	Approval Date	Publication Date	Review Date
1.0	MS	Head of Information Management	05/11/2019	05/11/2019	05/11/2021

Introduction

Occasionally we may receive requests to disclose data (including personal data) to a third party organisation, including the police in cases of criminal investigation etc. Also, we may wish to make a request for information (including personal data) from an external organisation in connection with law enforcement.

Contents

Introduction..... 2

Purpose..... 3

Where the guidance applies..... 3

Legislative Background..... 3

Conditions for the disclosure 4

Managing Requests 4

Documentation of Decisions 4

Disclosure of information..... 5

Duty of Care 5

Subject Access Requests (SAR) 5

Making a request to an external organisation..... 5

Review 5

Purpose

The aim of this guidance note is to ensure that staff in receipt of a request, or who wish to make a request understand the conditions under which personal and/or special category data can be disclosed. The guidance does not cover situations where we have already entered into an overarching agreement with partners. Please refer to the data sharing protocol that can be found on the HUB under [Information Management](#) for guidance on the disclosure of personal data outside of the law enforcement purposes. This guidance is not concerned with the disclosure of information to external organisations or other persons in an emergency, e.g. details of medical conditions, next of kin etc.

Where the guidance applies

The guidance note applies to all requests made by the Police, or other authorised agencies for personal data held by the National Park Authority, where the requestor seeks that information for law enforcement purposes, and where it is not appropriate for the requestor to seek that information from the individual(s) concerned, or is unable to obtain it from any other source.

Legislative Background

Part 3 of the DPA 2018 regulates the processing of personal data for law enforcement purposes.

The law enforcement purposes are defined under section 31 of the DPA 2018 as:

'The prevention, investigation detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security.'

Part 3 only applies to a **competent** Authority's processing for law enforcement purposes.

A **competent** authority means:

- a person specified in Schedule 7 of the DPA 2018 (this includes the police, HMRC, the FCA and HSE); or
- any other person if, and to the extent that, they have statutory functions to exercise public authority or public powers for the law enforcement purposes (this includes local authorities who prosecute trading standards offences and planning contraventions or the Environment Agency when prosecuting environmental offences).

Planning enforcement function falls within S31 of DPA 2018 - we have the powers to take non-compliance with an enforcement notice all the way through to prosecution. If we are looking at alterations to or demolition of a listed building without the necessary consent, under another regime this is a criminal offence. Our 'basis in law' is set out in the Town and Country Planning Act 1990 Part VII.

Conditions for the disclosure

The Authority will only consider disclosing personal data for law enforcement purposes under the following conditions:

- Not supplying the information would jeopardise the requestor's ability to undertake a lawful duty, as defined in the law enforcement purposes; and
- The requesting body could not obtain the information requested from a source other than the National Park Authority; and
- Release of the information would not conflict with other legal obligations with which the National Park Authority is required to comply.

Or:

- Where a Court Order is made that requires we release the requested information.

Managing Requests

Organisations wishing to make a request for personal information held by the National Park Authority should complete a Data Request Form. A copy of the form is included at the end of the guidance and is also available on our website by following the link to [Information Management/GDPR](#)

A request should be for specific information relating to one of the law enforcement purposes, it should not be used for 'trawling' information. Any request of this nature will be refused.

Requests for data should initially be discussed with the [Data Protection Officer](#).

Documentation of Decisions

All requests to disclose information will be documented. Such documentation will include a copy of the request, the initial assessment and a summary of the actions taken by the Authority. Access to the information will be restricted and records of the request will be retained for 24 months following receipt of the request. After this period they will be securely destroyed.

Details of information requests are to be kept strictly confidential.

Where a breach of the GDPR or DPA is deemed to have occurred, and where the potential harm to individuals has become an overriding consideration, the Data Protection Officer will report the matter to the Information Commissioners Office (ICO).

Disclosure of information

Where the Authority makes an assessment that it is obliged to disclose information then it will disclose only the minimum information necessary to enable the requestor to conduct their lawful duties.

Duty of Care

On receipt of a request the Authority may become aware of events/circumstances where it may wish to act so that it can address its duty of care and other responsibilities. The Authority will not act on any knowledge gained from the receipt of such a request without first seeking guidance and as necessary, permission from the requestor. Such communications between the Authority and the requestor will be documented for audit purposes.

Subject Access Requests (SAR)

An individual can make a SAR to an organisation requesting copies of all personal information that the organisation holds on them. This is a right under the GDPR 2016, however, this right may be restricted or removed in cases where the relevant information has been provided for law enforcement purposes and responding to the SAR may prejudice the purposes or be detrimental to public safety, national security or the rights and freedoms of others.

Making a request to an external organisation

Following discussions with Staff Committee, Unison and Strategic Leadership Team regarding how we might be able to obtain information from external organisations to assist with our own investigations, or for the purpose of staff protection, the options have been reviewed and it has been concluded that there is no over-arching data sharing agreement that we could sign up to that will facilitate this.

However, that doesn't mean that we cannot obtain information for these purposes, only that it would have to be on an ad-hoc basis, completing a form which the organisation in question should be able to provide or which you may be able to download from their website. If no form is available then the recommendation is that you complete our form in order that we retain a formal record of the request. Requests for information should be handled sensitively and should not be done without consultation with our Data Protection Officer.

Review

This policy will be reviewed at regular intervals. Any significant change to relevant legislation, Authority policy or procedures primarily concerned with information confidentiality, integrity and accessibility may trigger an earlier review.