Data Protection Policy

Document Status	
Date adopted	7 June 2017
Updated	28 April 2021
Adopted by	SMT
Lead Officer	LK
Date of next review	*May 2026*

Key Statement:

The Yorkshire Dales National Park Authority acknowledges that it holds personal data on trust and that harm may arise if that data is misused.

THEREFORE:-

We will only hold personal data that is relevant to the conduct of our business.

We will employ good practice in all matters concerned with the use of personal data.

We will ensure that personal data is kept secure and is used only for properly authorised purposes.

We will ensure that the rights of data subjects are respected.

1. LEGISLATIVE BACKGROUND

1.1 The **Data Protection Act 2018** (the Act) sets out the framework for data protection law in the UK. It sits alongside and supplements the UK GDPR. The requirements of the Act have also to be seen in the context of other relevant legislation, in particular the Human Rights Act 1998 and the Freedom of Information Act 2000.

2. CONTEXT

2.1 This Policy implements our responsibilities under current legislation, taking guidance from the Information Commissioner's Office (ICO) which is the UK's supervisory authority.

2.2 For the purposes of this Policy, the term "**Data**" means information which is held, processed or recorded ***as part of a relevant filing system or forming part of an accessible record.***

2.3 **"Personal data"** means data held by the Authority *relating* to a living individual who can be identified:

- from the data, or
- from the data and other information which is in the possession of, or is likely to come into the possession of, the Authority (the "data controller"),

and includes any expression of opinion about the individual and any indication of the intentions of the Authority or any other person in respect of the individual.

Note: the definition of what constitutes personal data is not straightforward; sometimes when determining if data is personal data consideration must be given to the impact on an individual, or the reasons for which the data is being processed (so what may constitute personal data for one body may not be personal data for another).

2.4 UKGDPR applies to the processing of personal data wholly or partly by automated means; or the processing other than by automated means of personal data which forms part of, or is intended to form part of, a filing system.

2.5 **"Special Category Data"** as set out in UKGDPR is personal data which is more sensitive and so needs special protection. The categories of Special Data are ethnic origin; politics; religion; trade union membership; genetics; biometrics (where used for ID purposes); health; sex life or sexual orientation. Special Category data must not be processed unless you have identified both a lawful basis and a separate condition for processing this data (Article 9)

2.6 Special Category Data classifications are not the same as the nine protected characteristics of the Equality Act so would not include, for example, financial information or criminal offences. Such details would however be regarded as **sensitive information** and should always be treated with care. [Article 10 of UKGDPR sets out the restrictions on processing details of criminal offences].

3. PRINCIPLES

3.1 The six UKGDPR Principles require 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 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;

(e) retained - 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;

(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.

3.2 Additionally, Article 5 (2) requires that "the controller (ie the Authority) shall be responsible for, and be able to demonstrate, compliance with the Principles".

4. APPLYING THE PRINCIPLES IN PRACTICE

4.1 Data Protection is a shared responsibility between all individual members of staff and the Authority. ***All staff*** *with access to personal data hold a responsibility for understanding and adhering to the requirements of this Policy. The Authority has*

corporate responsibilities to ensure that staff are properly informed, to put in place proper systems and procedures, and to deal properly with any incidents that may arise.

4.2 As a public authority, we have a designated Data Protection Officer (DPO) (as required by Article 37 of the UKGDPR). The DPO is tasked with monitoring the Authority's compliance with data protection legislation; data protection policies, awareness-raising, training, and audits.

4.3 Responsibility for day to day issues, such as advising on data protection and processing subject access requests, rests with the Corporate Services Officer who is the designated Data Protection Co-ordinating Officer (DPCO).

4.4 Responsibility for all IT issues including **computer security** lies with the IT Manager.

4.5 The Authority puts the UKGDPR Principles into practice as follows:

(a) Fair and lawful processing
We will tell persons about whom we are seeking to obtain personal data, or already hold data, how we intend to process their information, explaining what types of information we hold, what we use it for, and what their rights are to access that information.

We will ensure all data subjects have access to our Privacy Notice, explaining what we will use their personal information for, and how we will handle their data. We will normally provide this access on the first occasion that we make contact.

We will identify instances where Consent is needed from data subjects, as a lawful basis for processing their data.

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 a Data Sharing Protocol which explains what procedures need to be followed. Whenever data is provided to a body or individual outside of the Authority, details of the disclosure must be recorded on the appropriate record (computer record, personnel file etc).

Changes to the use of personal data and new arrangements for sharing or providing data may not take place without prior reference to the Section Head and subsequently the DPO or the DPCO, to ensure that Data Protection issues are properly addressed.

(b) Obtained and processed only for specified purposes
We will obtain and process personal data only for the purposes of carrying out Authority business.

(c) Adequate, relevant and not excessive
We will take care to ensure that unnecessary data is not held. When we collect personal data, we will be clear why we need it, and not collect more than we need.

(d) Accuracy and currency
All staff must record information accurately as soon as they receive it, take reasonable steps to validate such information and then apply (and record) any corrections or

alterations as they become known. Where amendments have been made, the other parties who also hold or have received that information must be informed.

(e) Retention
Retention periods for all categories of data are shown in our Document Retention guidance. Guidance periods should be followed, and data should be destroyed once the retention period expires unless legislation or business reasons dictate otherwise.

Where personal data is to be destroyed, this must be done in a secure way. Paper records should be shredded as confidential waste, not sent for recycling. Electronic records should be deleted, or if necessary archived and the appropriate access restrictions applied.

(f) Technical and operational security measures
We will adhere to good practice for the design and security of computer systems, the design and security of working areas, the security of filing systems and the security of premises.

All users of the Authority's computer systems are required to adhere to the ICT Users PolicyAll instances where personal information has been collected and processed are recorded on the Information Asset Register as a means of monitoring and evaluating the personal information we hold. This is checked/updated annually and includes details of where the information is stored and any access restrictions imposed.

Some personal data will be stored on Authority computer systems; some in paper filing systems. Particular care must be taken in the following circumstances:

- Taking hard copy files away from Authority's premises;
- Downloading information to a laptop, or personal computer;
- Downloading information to portable media with the intention that it should be used outside the Authority's premises

Personal data must never be downloaded, removed or copied into any other systems or onto any other devices or media **not covered by the Authority's ICT Users Policy** without the approval of the Chief Executive or a Director, or the SIRO (Richard Burnett) or DPO (Clare Burrows).

Where it is necessary to take such action for operational reasons, the authorising officer will need to be satisfied that the personal data is protected by encryption and/or passwords, as appropriate to the circumstances and with reference to the IT Manager.

This is particularly relevant where officers are working from home; guidance has been issued regarding remote working and this should be followed at all times.

4.6 **Rights of Data Subjects, including Subject Access Requests (SARs)**:
Individuals have a right to know what information we hold about them, and for that information to be accurate, and held for no longer than is necessary or as is required by legislation. Individuals have the right to ask for any personal data we hold about them to be erased. Requests by individuals to know what information we hold about them (Subject Access Requests) can be made verbally or in writing (email is acceptable) and

we should satisfy ourselves as to the identity of the person making the request. All requests must be forwarded to the DPCO for recording. The DPCO will provide advice and guidance as necessary on how to respond to such requests.

4.7 **Transfer of data outside the UK.**

UKGDPR restricts transfers of personal data outside the UK, unless the rights of the individuals in respect of their personal data is protected in another way, or one of a limited number of exceptions applies. These restrictions apply to all transfers, no matter the size of transfer or how often you carry them out. Personal data must not be transferred out of the UK (whether on paper or in electronic form) without the specific written authority of the CEO, SIRO or DPO. Such authority will only be given on a case by case basis and then only where that transfer is necessary for reasons of substantial public interest or is required by statute, and the personal data is protected by the legal framework in that country, territory, sector or international organisation having been assessed as providing 'adequate' protection for individuals' rights and freedoms for their personal data.

4.8 Transfer of data to the UK from EU states: The European Commission has published its draft UK adequacy decisions. If adopted these decisions will allow for continued free transfer of data from the EU. Until adoption of this decision, UK businesses and public authorities will continue to be able to receive data from the EU under the adequacy bridge agreed in the 2020 trade and cooperation agreement.

5. BREACHES OF DATA SECURITY

5.1 Any breaches or suspected breaches of data security should be reported immediately to the DPO (or DPCO) who will consult with 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, have to be reported to the Information Commissioner within 72 hours of becoming aware of the breach. The DPO will make a judgement on whether a reported breach is significant.

6. MONITORING AND EVALUATION

6.1 An internal review of data protection awareness amongst officers will be carried out every five years (or as required by a change in legislation) by the DPCO, and the results will be reported to the Senior Management Team. The audit ensures all officers are kept aware of their data protection responsibilities, and provides an opportunity to identify further training needs.

6.2 In terms of evaluating potential risk of data security breaches, a Data Protection Impact Assessment should be carried out on any new policy or project which might incur risk, both to the Authority as a corporate body or to individuals. Under UKGDPR this requirement is mandatory for certain types of high risk or extensive processing.

6.3 The Authority's approach to data security is regularly audited as part of the Internal Audit schedule. Veritau has most recently carried out an audit on processes and practice in February 2021.

7. STAFF DEVELOPMENT AND TRAINING

7.1 The DPO is responsible for ensuring that staff who deal with personal data receive appropriate training, guidance and information in data protection requirements. The DPCO maintains a log of all training and guidance issued to staff and, where appropriate, to Members. Data protection awareness forms part of the induction process for Officers and Members, and completion of ELMS e-learning on data protection is mandatory for all Officers.