Data Protection Policy

CONTENTS

APPENDIX

Approved by Governance & Resources Committee March 2018

DATA PROTECTION POLICY

1. POLICY

1.1. The processing of personal data is essential to many of the services and functions carried out by local authorities. Derbyshire Dales District Council ('the Council') recognises that compliance with the Data Protection legislation will ensure that processing is carried out fairly and lawfully.

1.2. The Data Protection Act, and Article 8 of the Human Rights Act 1998, both stress that the processing of personal data needs to strike a balance between the needs of the organisation to function effectively and efficiently, and respect for the rights and freedoms of the individual. This policy sets out how the Council intends to safeguard those rights and freedoms.

1.3. The Data Protection Act 1998 will be replaced by a revised Act in 2018. The new legislation will build on existing legislation and incorporate the new General Data Protection Regulation, which will be implemented across Europe. Derbyshire Dales District Council recognises the need to abide by the new legislation and associated guidance issued by the Information Commissioner's Office.

1.4. This policy replaces any previous data protection policy statement.

2. SCOPE

2.1 The policy is applicable to all employees, Elected Members, apprentices, agency workers, unpaid volunteers and those on work experience. In certain circumstances it will apply to contractors working for the Council.

2.2 This policy applies to the collection and processing of all personal data as defined by the legislation as that of a 'natural person'. It covers all formats including paper, electronic, audio and visual formats. The policy will only deal with the personal data of a living person and does not apply to the data of a deceased person.

2.3 The policy applies to all employees working within Elections although the post of Electoral Registration Officer is registered, for the processing of elections data, with the Information Commissioners Office separately.

2.4 Key delivery partners who process data on our behalf, such as Arvato Public Services, will have their own policy statements in respect to data protection. These, however, will be in line with the Council's policy

3. POLICY PRINCIPLES

3.1 The policy is a statement of what the Council is doing to ensure compliance with the legislation. It is not a statement of how compliance will be achieved as this will be a matter for operational procedures.

3.2 The policy has been produced to ensure compliance with the relevant legislation and to ensure customers gain appropriate access to data and information on request. As such the policy will be made available to the public

4. DATA PROTECTION STATEMENT

4.1 The Data Protection Act applies to the processing of personal data wholly or partly by automated means as well as that in filing systems or intended to form part of a filing system at a later date. To be applicable the data has to be stored in a structured way to enable retrieval. '**Filing system**' means any structured set of personal data, whether centralised, decentralised or dispersed on a functional or geographical basis.

4.2 '**Personal data'** means any information relating to an identified or identifiable natural person (data subject). As defined by the legislation an identifiable natural person is one who can be identified directly or indirectly in particular by reference to an identifier such as a name, a number, location data etc. This may also include online identifiers provided by their devices, applications, tools and protocols, such as internet protocol addresses, cookie identifiers or radio frequency identification tags. Such identifiers may leave traces which combined with other information may be used to create profiles of the natural person and identify them.

4.2 Derbyshire Dales District Council is the **'Controller'** who determines the purposes and means of processing personal data. Processing means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaption or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

4.3 The new legislation applies to **'Processors'** who act on the controller's behalf and places further obligations on both parties. The 'Processor' means a natural or legal person, public body, agency or other body which processes personal data on behalf of the Council. Any processing of personal data in the context of the activities of an establishment of a controller or a processor shall be carried out in accordance with the legislation.

5. DATA PROTECTION PRINCIPLES

5.1. The following **principles** relate to the processing of personal data and set out the main responsibilities for the Council under the legislation. Article 5 of the legislation requires that personal data shall be:

(a) Processed lawfully, fairly and in a transparent manner in relation to the data subject. This will commonly be known as – **lawfulness, fairness and transparency.**

(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, scientific or historical research purposes or statistical purposes shall not be considered incompatible with the initial purposes. This will be commonly known as – **purpose limitation**.

(c) Adequate, relevant and limited to what is necessary in relation to the purpose for which they are processed. This will be commonly known as – **data minimisation.**

(d) 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**.** This will be commonly known as – **accuracy**.

(e) 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 this legislation in order to safeguard the rights and freedoms of the data subject. This will be commonly known as – **storage limitation**.

(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. This will be commonly known as – **integrity and confidentiality.**

6. DATA PROTECTION COMPLIANCE

6.1. In order for processing to be lawful the Council must meet one or more conditions, not all of which apply to local government. The conditions

for **lawful processing** are detailed in Appendix 1. In general terms the Council will rely on the conditions of 'legal obligation' or 'public task' as the basis of processing for statutory services and 'performance of a contract' for services which are discretionary and allow customer choice. There will however be circumstances where personal data is highly sensitive and **consent** may form an additional legal basis for processing.

6.2 The Council will explain the reasons for processing personal data through the use of **Privacy Notices. D**epending on the method of contact these may be written as part of a data capture form or verbal. Further details can be found on the Council website.

6.3 In order to deliver services the Council has been regularly processing 'sensitive personal data' such as that relating to the health of an individual or ethnic origin. The new legislation has amended the original list and renamed these **Special Categories**. Personal data which, by their nature, which are particularly sensitive merit specific protection as the context of their processing could create significant risks to the data subject. These are also detailed in Appendix 1.

6.4 The Council has a duty to retain personal data whilst it is legally required to do so. **Security measures** are in place to ensure data is safely stored both in electronic and paper format. The Council has an Information Security Policy to ensure that all staff are aware of their responsibilities. Personal data will be retained in line with the Councils Guidelines on Retention and Disposal of Data, a copy of which is available on request. When data is no longer required it will be safely destroyed or deleted from electronic equipment.

6.4 In order to provide an effective public service the Council may need to share data with third parties and delivery partners who process data on our behalf. Any **sharing of data** will be in line with legislation and where applicable data subjects will be notified as part of the privacy notice. Under certain circumstances where legislation applies the Council will share data with other bodies without consent, for instance for data matching or to prevent fraud or detect crime. A number of Information Sharing Agreements are also in place to ensure effective transfer of data to other bodies, such as the County Council for emergency planning situations and child protection. Such sharing agreements have also been put in place with certain government departments.

6.5 The Council has a duty to ensure that all employees that come into contact with personal data have been adequately trained. This will involve **training** as part of the induction process and throughout the course of their employment. All employees will receive basic data protection and information security training which will be in proportion to the job role undertaken. Refresher training will be mandatory every 2 years for office based employees. Additional on-the-job training may

also be necessary in areas processing sensitive or high risk data, such as those containing Special Categories, financial data or using high risk technology. With the assistance of the Data Protection Officer, Human Resources will maintain an accurate record of all data protection training undertaken. Apprentices, unpaid volunteers and those on work experience will receive basic information on the importance of data protection in line with their job role. Elected members will receive regular training on data protection and information security. Delivery partners who process data on our behalf will also have to demonstrate that they train their employees.

6.6 As stated the Council will ensure measures are in place to protect data, however data breaches may occur. A **data breach** is defined as a breach of security leading to the destruction, loss, alteration, unauthorised disclosure of, or access to, personal data. The Council will investigate all data breaches and establish the risk to individuals such as discrimination, damage to reputation, financial loss, loss of confidentiality or other significant economic or social disadvantage. The Council will maintain a register of data protection breaches and near misses. Where a risk is likely to have a significant detrimental impact the Council will notify the Information Commissioners Office within 72 hours of identification. Under such circumstances the Council also has a duty to notify those concerned directly. If a breach occurs, the Council and where appropriate its delivery partners, will decide the most appropriate method of communication. This may include placing messages on the website, sending letters or notifying the data subject by telephone. Any breaches reported to the Information Commissioners Office will be done so in accordance with their guidance.

7. DATA SUBJECT'S RIGHTS

7.1. The Council will have operational processes in place to ensure the following data subject's rights apply:

a. The right to be informed
b. The right of access
c. The right of rectification
d. The right of erasure
e. The right to restrict processing
f. The right of data portability
g. The right to object
h. Rights in relation to automated decision making and profiling.

7.2. Under the legislation individuals have a right to obtain confirmation that their data is being processed, have access to their personal data and be provided with other supplementary information on how their data is being used through the use of a privacy notice. The request for access will commonly be done through a Subject Access Request.

7.3 The identity of the individual making the Subject Access Request must be verified using two forms of formal identification which includes both the name and address. This is to ensure that the Council only releases information to the correct data subject. This verification could be a bank statement, passport, utility bill, driving license etc. If visual information is being requested e.g. CCTV images, photographic identification of the data subject will also be needed. If Officers have any reasonable doubt about the identity of an individual they have a right to refuse the request. The Council will take every care to redact any information on other data subjects within the documents before release.

7.4 The personal data requested will be provided **free of charge**. A 'reasonable fee' (based on administrative cost) can be charged if a request is manifestly unfounded or excessive in nature, or repetitive. In such circumstances a refusal notice will be issued without undue delay and at the latest within one month. The legislation permits the Council to seek clarification from the requestor if necessary.

7.5 The Council will have **one month** from receipt of request to provide the information, ideally however the information will be provided without delay. Complex requests can be extended for a further 2 months, although the requester will be informed within the original one month period. The Council has an operational procedure in place to deal with subject access requests. Information for members of the public wishing to make a Data Subject Access Request can be found on the website. Employees wishing to make a Data Subject Access Request for access to their own personal data should contact Human Resources.

7.6 The Council will have in place operational procedures for the additional rights of rectification, erasure, restricting processing, data portability, objection and rights in respect to automated decision making/profiling. Some of these rights will depend on the original condition for processing and may not apply.

7.7 Should any member of the public wish to make a complaint about the processing of their data by the Council then they should use the Councils Complaints Procedure which is available on the website. The public also have a right to contact the Information Commissioners Office who are the supervisory authority for data protection matters under the legislation.

8. ACCOUNTABILITY AND GOVERNANCE

8.1 The Council will implement appropriate technical and organisational measures to ensure that they are compliant with the legislation and have good governance arrangements in place. The Council will:

- Maintain relevant documentation on processing activities.

- Have a designated Data Protection Officer at an appropriate level within the organisation and provide suitable resources to support the role.
- Implement measures to meet the principle of data protection by design and default, through the use of Data Protection Impact Assessments.
- Ensure transparency and pseudonymisation of data where appropriate.
- Create and improve security measures on an on-going basis.

8.2. The Council has an Information Governance Board which monitors and implements data protection compliance. Reports are also taken to senior management and to elected members. Internal Audit periodically conduct checks on data protection compliance. External inspection and support has also been sought on compliance issues to ensure effective implementation of the legislation.

9. RESPONSIBILITY FOR IMPLEMENTATION

9.1 Keeping the policy under review and updating the policy is the responsibility of the Data Protection Officer for the Council. Corporate Leadership Team are responsible for implementing this policy and the legislation in general.

9.2 Managers at all levels are responsible for ensuring that employees, agency workers, apprentices, unpaid volunteers and work placements for whom they are responsible are aware of and adhere to this policy. Managers are also responsible for ensuring that employees are updated in regard to any changes in this policy and receive regular training.

9.3 All Employees need to be aware that a breach of the legislation could result in disciplinary action being taken.

DDDC Data Protection Policy: Appendix 1 **CONDITIONS FOR LAWFUL PROCESSING**

Processing of personal data by the Council will only be lawful if at least **one** of the following applies:

(a) the data subject has given **consent** to the processing of their personal data for one or more specific purposes;
(b) processing is necessary for the performance of a **contract** to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract;
(c) processing is necessary for compliance with a **legal obligation** to which the controller is subject;
(d) processing is necessary in order to protect the **vital interests** of the data subject or of another natural person;
(e) processing is necessary for the performance of a **task** carried out in the public interest or in the exercise of official authority vested in the controller;
(f) processing is necessary for the purposes of **legitimate interests** pursued by the controller or by a third party, except where such interest are overridden by the interest or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child.*

Additional conditions apply to the processing of **Special Category** data that would reveal:

- racial or ethnic origin
- political opinions
- religious or philosophical beliefs
- trade union membership

and the processing of:

- genetic data
- biometric data for the purpose of uniquely identifying a natural person
- data concerning health
- data concerning a natural person's sex life or sexual orientation.

Processing of the above are prohibited unless one of the following applies:

(a) the data subject has given **explicit consent** to the processing for one or more specified purposes;

(b) processing is necessary for the purpose of carrying out an obligation such as employment and social security and social protection law;

(c) processing is necessary to protect the vital interests of the data subject and the natural person is physically or legally incapable of giving consent;

(d) processing is carried out in the course of its legitimate activities of a foundation, association or not-for-profit organisation

(e) processing relates to personal data which are manifestly made public by the data subject;

(f) processing is necessary for the establishment, exercise or defence of legal claims or whenever courts are acting in their judicial capacity;

(g) processing is necessary for reasons of substantial public interest;

(h) processing is necessary for the purposes of preventive or occupational medicine, for the assessment of the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment of the management of health or social care systems and services;

(i) processing is necessary for reasons of public interest in the area of public health, such as cross border threats to health;

(j) processing is necessary for archiving purposes in the public interest, scientific or historical research.

February 2018