STROUD DISTRICT COUNCIL
www.stroud.gov.uk

Data Protection Policy

April 2018

Legal Services

CONTENTS

Section

Last updated: April 2018

Reviewed by: Legal & Democratic Services

1. POLICY STATEMENT

1.1 Everyone has rights with regard to the way in which their personal data in handled. We (or more generally) the Council, collect and are required as part of the Council's activities and service provision to store and process personal data about its constituents, members, employees, customers, suppliers, contractors and other third parties.

1.2 Data users (as defined at section 3.6) are obliged to comply with this policy when processing personal data on our behalf. Any breach of this policy may result in disciplinary action.

2. ABOUT THIS POLICY

2.1 The personal data we hold, which may be held on paper or on a computer or other media, is subject to certain legal safeguards specified in data protection legislation e.g. General Data Protection Regulation 2016 and the Data Protection Act 2018.

2.2 This policy and any other documents referred to in it set out the basis on which we will process any personal data we collect from data subjects, or that is provided to us by data subjects or other sources.

2.3 This policy does not form part of any employee's contract of employment and may be amended at any time, particularly in the light of changes to the law.

2.4 This policy sets out rules on data protection and the legal conditions that must be satisfied when we obtain, handle, process, transfer and store personal data.

2.5 The Head of Legal Services (who acts as the Council's Data Protection Officer) oversees compliance with data protection legislation and Council policy. Any questions about the operation of this policy or any concerns that the policy has not been followed should be referred in the first instance to the Head of Legal Services at:

data.protection@stroud.gov.uk or Legal Services, Council Offices, Ebley Mill, Ebley Wharf, Stroud, Gloucestershire, GL5 4UB.

3. DATA PROTECTION TERMS

3.1 Comprehensive definitions of relevant data protection terms are set out in the General Data Protection Regulations 2016 ("**GDPR"**) and these regulations and any other legislation applicable to England should be applied to this policy. The following definitions are simply provided to help explain in plain English what the various terms mean although any dispute would need to be determined with reference to the legislation.

3.2 **Data** is information which is stored electronically, on a computer, or in certain paper-based filing systems.

3.3 **Data subjects** for the purpose of this policy include all living individuals about whom we hold personal data. A data subject need not be a UK national or resident. All data subjects have legal rights in relation to their personal information.

3.4 **Personal data** means data relating to a living individual who can be identified from that data (or from that data and other information in our possession or otherwise accessible). Personal data can be factual (for example, a name, address or date of birth) or it can be an opinion about that person, their actions and behaviour. Please see Article 4 GDPR

3.5 **Data controllers** are the people who or organisations which determine the purposes for which, and the manner in which, any personal data is processed. They are responsible for establishing practices and policies in line with the UK law. The Council (via its Chief Executive and Directors in respect to their relevant service areas) is the data controller of all personal data used for Council purposes.

3.6 **Data users** are those of our employees or agency staff whose work involves processing personal data as part of the Council's work. Data users must protect the data they handle in accordance with relevant law and Council policy such as this data protection policy and any applicable data security procedures at all times.

3.7 **Data processors** include any person or organisation that is not a data user that processes personal data on the Council's behalf and on our instructions. Employees of data controllers are excluded from this definition but it could include suppliers which handle personal data on the Council's behalf.

3.8 **Processing** is any activity that involves use of the data. It includes obtaining, recording or holding the data, or carrying out any operation or set of operations on the data including organising, amending, retrieving, using, disclosing, erasing or destroying it. Processing also includes transferring personal data to third parties.

3.9 **Special Category Data (or 'sensitive' personal data)** includes information about a person's racial or ethnic origin, political opinions, religious or similar beliefs, trade union membership, physical or mental health or condition, sexual life, genetic and biometric data or information about the commission of, or proceedings for, any offence committed or alleged to have been committed by that person, the disposal of such proceedings or the sentence of any court in such proceedings. Special Category Data can only be processed under strict conditions, including a condition requiring the express permission of the person concerned.

4. **DATA PROTECTION PRINCIPLES**

4.1 Anyone processing personal data must comply with the six statutory data protection principles. They set out how personal data must be dealt with and in particular that data must be:

THE PRINCIPLES	EXPLANATION
1. Processed lawfully, fairly and in a transparent manner in relation to individuals	The Council's Privacy Notice sets out how personal data provided will be used to promote compliance with these principles. Please also see sections 5 to 6 below.
2. Collected for specified, explicit and legitimate purposes and not further processed in a manner incompatible with those purposes	
3. Adequate, relevant and limited to what is necessary for the purposes	
4. Accurate and where necessary kept up-to-date	We will check the accuracy of any personal data at the point of collection and at regular intervals afterwards. We will take all reasonable steps to destroy or amend inaccurate or out-of-date data.
5. Not kept longer than necessary for the purpose (unless processed solely to achieve in the public interest or for research purposes etc).	Reference should be made to the document retention periods set out in the Council's Privacy Notice (see section 5 below) for determining how long a document should be retained. Personal data should not be retained longer than the relevant retention periods unless the reason for doing so is clearly documented and most importantly, necessary.
6. Processed in a manner which involves taking appropriate security measures to keep the personal data confidential to those who need it for a valid purpose.	Please see Privacy Notice paragraph 6.

5. PRIVACY NOTICE

5.1 The Council has a **general** Privacy Notice which **sets out data subjects rights** regarding their personal data (see paragraph 5 of the Privacy Notice). It also **explains who is going to process the information, what is going to happen with the information, when and with whom the information will be shared and how it will be used**. Specific council services may need to use information differently and will have different reasons for collecting information. Paragraphs 10 onwards of the Privacy Notice provide data subjects with relevant details of how each service area will use information they collect.

5.2 As explained in the notice, if we receive personal data about a data subject from other sources, we will provide the data subject with this information as soon as possible thereafter as and when required by law.

5.3 We will **only request personal data to the extent that it is required for the specific purpose notified to the data subject**. There may be occasions where a data subject provides more information than is needed (e.g. a long letter providing details which are not relevant to the Council's services). In these cases, when dealing with pertinent matters, we should (i) inform the data subject that such is not required and it will be deleted or (ii) otherwise obtain their express consent to processing the information.

5.4 When obtaining **information from children** under the age of 13, the Council must obtain consent from a parent or guardian to process the child's data. The same data subject rights apply to children as they do to adults, although it is even more important that information provided to children about how their information will be used etc. is transparent and clear so it can be readily understood by the data subject; or where the Council is satisfied that the child is not competent, to the person who has approached the Council and holds parental responsibility for the child and as such to whom the Council will respond in appropriate cases.

6. PROCESSING CONDITIONS

6.1 Neither the legislation nor this policy is intended to prevent the processing of personal data. For personal data to be processed lawfully, it must be processed for a valid purpose. Such **purposes are set out in paragraph 3 of the Council's Privacy Notice**.

6.2 Express consent (which should be documented) from the data subject to process their personal data is a valid purpose, but it should not be used as a first resort. Consent requires a positive opt-in and must be clearly given. Consent must be easily withdrawn and the data subject must be clearly informed how to withdraw their consent. The consent must also be regularly reviewed and obtained again if anything relevant changes.

6.3 When Special Category Data is being processed, additional conditions must be met (see definition of Special Category Data in paragraph 2 of the Council's Privacy Notice). In cases concerning this type of data, where consent is sought, it should be obtained in writing wherever possible.

7. DEALING WITH SUBJECT ACCESS REQUESTS

7.1 Data subjects may make a formal request in writing for information we hold about them. Any member of staff of the Council who receives a written request should forward it to their Information Management Champion or Head of Service / Director **immediately** as requests must be responded to in full within 1 month of the request and will potentially require the Information Management Champion to contact a variety of services within the Council in order to meet the request.

7.2 When receiving telephone enquiries, we will only disclose personal data we hold on our systems if the following conditions are met:

(a) We will check the caller's identity to make sure that information is only given to a person who is entitled to it.

(b) We will request that the caller put their request in writing if we are not sure about the caller's identity and where their identity cannot be checked.

7.3 A record should be retained of Subject Access Requests for 12 months. Thereafter they should be destroyed unless upon review it is considered necessary to retain the record for some longer period given the particular circumstances of the case.

8. DATA PROTECTION IMPACT ASSESSMENTS (DPIA)

8.1 These are also known as DPIAs or privacy impact assessment (not to be confused with Privacy Notices). They are required when the Council uses new technologies and the processing is likely to result in a high risk to the rights and freedoms of individuals.

8.2 They must be completed by Directors or Heads of Service. They must contain a description of the processing operations and the purposes, including where applicable the legitimate interests pursued by the Data Controller; an assessment of the necessity and proportionality of the processing in relation to the purpose; an assessment of the risk to individuals; the measures in place to address risk, including security and to demonstrate that the Council complies.

8.4 Heads of Service / Directors must submit a written record of their DPIA to the Head of Legal Services for the Council's records.

9. POTENTIAL OR ACTUAL BREACHES OF DATA PROTECTION

9.1 If a breach of data protection law comes to the attention of a member of staff or is suspected by them, they must notify their team's Information Champion, Head of Service / Director immediately.

9.2 **Action must be taken to resolve any breach ASAP and prevent the situation reoccurring**. Further the Head of Service / Director is required to notify the Head of Legal Services of the issue as soon as possible and certainly within 72 hours of the incident occurring.