	DATA PROTECTION POLICY STATEMENT	**Document Control** Reference: Data Protection Policy Statement Issue No: 2 Issue Date: June 2020

1. Introduction:

1.1 The General Data Protection Regulation 2016 (GDPR) replaces the EU Data Protection Directive of 1995. The principles of the GDPR are enshrined within UK law under the Data Protection Act 2018. The purpose of both GDPR and DPA 2018 are to protect the "rights and freedoms" of natural persons (i.e. living individuals) and to ensure that personal data is not processed without their knowledge and (wherever possible) that it is processed with their consent.

2. Definitions used by Uttlesford District Council:

i) Material scope (Article 2) - GDPR applies to the processing of personal data wholly or partly by automated means (i.e. by computer) and to the processing other than by automated means of personal data (i.e. paper records) that form part of a filing system or are intended to form part of a filing system.

ii) Territorial scope (Article 3) - GDPR will apply to all controllers that are established in the European Union (EU) who process the personal data of data subjects, in the context of that establishment. It will also apply to controllers outside of the EU that process personal data in order to offer goods and services, or monitor the behaviour of data subjects who are resident in the EU.

2.1 Article 4 Definitions:

a. Establishment - the main establishment of the controller in the EU will be the place in which the controller makes the main decisions as to the purpose and means of its data processing activities. The main establishment of a processor in the EU will be its administrative centre. If a controller is based outside the EU, it will have to appoint a representative in the jurisdiction in which the controller operates to act on behalf of the controller and deal with supervisory authorities.

b. Personal data - any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

c. Special categories of personal data - personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade-union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation.

d. Controller - the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data; where the purposes and means of such processing are determined by Union or Member State law, the controller or the specific criteria for its nomination may be provided for by Union or Member State law.

e. Data subject - any living individual who is the subject of personal data held by an organisation.

f. Processing - 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, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

g. Profiling - is any form of automated processing of personal data intended to evaluate certain personal aspects relating to a natural person, or to analyse or predict that person's performance at work, economic situation, location, health, personal preferences, reliability, or behaviour. This definition is linked to the right of the data subject to object to profiling and a right to be informed about the existence of profiling, of measures based on profiling and the envisaged effects of profiling on the individual.

h. Personal data breach - a breach of security leading to the accidental, or unlawful, destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed. There is an obligation on the controller to report personal data breaches to the supervisory authority and where the breach is likely to adversely affect the personal data or privacy of the data subject, an obligation to inform the subject themselves.

i. Data subject consent - means any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data.

j. Child - GDPR defines a child as anyone under the age of sixteen (16) years old, although this may be lowered to thirteen (13) by Member State law. The processing of personal data of a child is only lawful if parental or custodian consent has been obtained. The controller shall make reasonable efforts to verify in such cases that consent is given or authorised by the holder of parental responsibility over the child.

k. Third party - a natural or legal person, public authority, agency or body other than the data subject, controller, processor and persons who, under the direct authority of the controller or processor, are authorised to process personal data.

l. Filing system - any structured set of personal data which are accessible according to specific criteria, whether centralised, decentralised or dispersed on a functional or geographical basis.

3. Policy Statement:

3.1 The Corporate Management Team of Uttlesford District Council, located within the Council Offices at London Road, Saffron Walden, Essex, CB11 4ER, are committed to compliance with all relevant EU and Member State laws in respect of personal data, and the protection of the “rights and freedoms” of individuals whose information the Council collects and processes in accordance with the General Data Protection Regulation (GDPR).

3.2 Compliance with the GDPR is described by this policy and other relevant policies such as the Council’s Information Security Policy, along with connected processes and procedures.

3.3 The GDPR and this policy apply to all of Uttlesford District Council’s personal data processing functions, including those performed on customers’, clients’, employees’, suppliers’ and partners’ personal data, and any other personal data the organisation processes from any source.

3.4 The Data Protection Officer is responsible for reviewing the Record of Processing Activity (ROPA) annually in the light of any changes to the Council's activities and any additional requirements identified by data protection impact assessments. This register will be made available on the supervisory authority's (Information Commissioner's Office) request.

3.5 This policy applies to all Uttlesford District Council staff and all interested parties of the Council such as outsourced suppliers. Any breach of the GDPR will be dealt with under the Council's disciplinary policy and may also be a criminal offence, in which case the matter will be reported as soon as possible to the appropriate authorities.

3.6 Partners and any third parties working with or for or on behalf of Uttlesford District Council and who have, or may have access to personal data, will be expected to have read, understood and to comply with this policy. No third party may access personal data held by the Council without having first entered into a data confidentiality agreement which imposes on the third party obligations no less onerous than those to which Uttlesford District Council is committed and which gives the Council the right to audit compliance with the agreement.

4. Responsibilities and Roles under the General Data Protection Regulations:

4.1 Uttlesford District Council is a data controller under the GDPR.

4.2 Corporate Management Team and all those in managerial or supervisory roles throughout the Council's various service departments are responsible for developing and encouraging good information handling practices within the Council.

4.3 The Data Protection Officer (DPO) is a mandated role specified within the GDPR for all Public Authorities. The Data Protection Officer is accountable to the Corporate Management Team for the management of personal data within the Council and for ensuring that compliance with data protection legislation and good practice can be demonstrated.

This accountability includes:

- development and implementation of the GDPR as required by this policy and
- security and risk management in relation to compliance with the policy.

4.4 The Data Protection Officer, who the Corporate Management Team considers to be suitably qualified and experienced, has been appointed to take responsibility for Uttlesford District Council's compliance with this policy on a day-to-day basis and, in particular, has direct responsibility for ensuring that the Council complies with the GDPR. The responsibility for data processing that takes place within various service areas throughout the Council is equally shared by the individual service heads for their specific area of responsibility.

4.5 The Data Protection Officer has specific responsibilities in respect of procedures such as the Subject Access Request Procedure and is the first point of call for staff seeking clarification on any aspect of data protection compliance.

4.6 Compliance with data protection legislation is the responsibility of all Council staff who may have access to personal data.

4.7 Uttlesford District Council's Training Policy sets out training and awareness requirements for staff.

4.8 All Council staff are responsible for ensuring that any personal data about them and supplied by them to the Council is kept accurate and up-to-date.

5. Data Protection Principles:

5.1 All processing of personal data must be conducted in accordance with the data protection principles as set out in Article 5 of the GDPR. Uttlesford District Council's policies and procedures are designed to ensure compliance with the principles.

5.1.1 ***1st Principle: Personal data must be processed lawfully, fairly and transparently***

a. ***Lawful*** - identify a lawful basis before you can process personal data. These are often referred to as the "conditions for processing", for example consent.

b. ***Fairly*** - in order for processing to be fair, the data controller has to make certain information available to the data subjects as practicable. This applies whether the personal data was obtained directly from the data subjects or from other sources.

The GDPR has increased requirements about what information should

be available to data subjects, which is covered in the 'Transparency' requirement.

c. ***Transparently***- the GDPR includes rules on giving privacy information to data subjects in Articles 12, 13 and 14. These are detailed and specific, placing an emphasis on making privacy notices understandable and accessible. Information must be communicated to the data subject in an intelligible form using clear and plain language.

5.1.2 Uttlesford District Council's Privacy Procedure and our Privacy Notices are both available on our website. The specific information that must be provided to the data subject, as a minimum, must include:

- the identity and the contact details of the controller and, if any, of the controller's representative;
- the contact details of the Data Protection Officer;
- the purposes of the processing for which the personal data are intended as well as the legal basis for the processing
- the period for which the personal data will be stored;
- the existence of the rights to request access, rectification, erasure or to object to the processing, and the conditions (or lack of) relating to exercising these rights, such as whether the lawfulness of previous processing will be affected;
- the categories of personal data concerned;
- the recipients or categories of recipients of the personal data, where applicable;
- where applicable, that the controller intends to transfer personal data to a recipient in a third country and the level of protection afforded to the data;
- any further information necessary to guarantee fair processing.

5.2 ***2nd Principle: Personal data can only be collected for specific, explicit and legitimate purposes.***

5.2.1 Data obtained for specified purposes must not be used for a purpose that differs from those formally notified to the supervisory authority as part of the Council's GDPR register of processing. The Council's Privacy Procedure sets out the relevant procedures.

5.3 ***3rd Principle: Personal data must be adequate, relevant and limited to what is necessary for processing.***

5.3.1 The Data Protection Officer is responsible for ensuring that the Council does not collect information that is not strictly necessary for the purpose for which it is obtained.

5.3.2 All data collection forms (electronic or paper-based), including data collection requirements in new information systems, must be include a fair processing statement or link to privacy statement and should be approved by the Data Protection Officer.

5.3.3 The Data Protection Officer will ensure that, on an annual basis all data collection methods are reviewed by internal audit experts to ensure that collected data continues to be adequate, relevant and not excessive.

5.4 ***4th Principle: Personal data must be accurate and kept up to date with every effort to erase or rectify without delay.***

5.4.1 Data that is stored by the data controller must be reviewed and updated as necessary. No data should be kept unless it is reasonable to assume that it is accurate.

5.4.2 The Data Protection Officer is responsible for ensuring that all staff are trained in the importance of collecting accurate data and maintaining it.

5.4.3 It is also the responsibility of the data subject to ensure that data held by the Council is accurate and up to date.

5.4.4 Council staff, agency employees, customers, residents and all associated partners should be required to notify the Council of any changes in circumstance to enable personal records to be updated accordingly. It is the responsibility of all Council staff to ensure that any notification regarding change of circumstances is recorded and acted upon.

5.4.5 The Data Protection Officer is responsible for ensuring that appropriate procedures and policies are in place to keep personal data accurate and up to date, taking into account the volume of data collected, the speed with

which it might change and any other relevant factors.

5.4.6 On at least an annual basis, the Data Protection Officer will work with Service Managers to review the retention dates of all the personal data processed by the Council by reference to the Record of Processing Activity and will identify any data that is no longer required in the context of the registered purpose. This data will be securely deleted/ destroyed in line with the Councils Document Retention Policy.

5.4.7 The Data Protection Officer is responsible for responding to requests for rectification from data subjects within one month. This can be extended to a further two months for complex requests. The controller shall inform the data subject of any extension within one month of receipt of the request together with reasons for the delay. If the Council decides not to comply with the request, the Data Protection Officer must respond to the data subject to explain its reasoning and inform them of their right to complain to the supervisory authority and seek judicial remedy.

5.4.8 The Data Protection Officer is responsible for making appropriate arrangements that, where third-party organisations may have been passed inaccurate or out-of-date personal data, to inform them that the information is inaccurate and/or out of date and is not to be used to inform decisions about the individuals concerned; and for forwarding any correction to the personal data to the third party where this is required.

5.5 ***5th Principle: Personal data must be kept in a form such that the data subject can be identified only as long as is necessary for processing***

5.5.1 Personal data will be retained in line with the Council's Document Retention Policy and once its retention date is passed it must be securely destroyed as set out in this procedure.

5.5.2 Service area managers are responsible for ensuring that their staff comply with the Councils Document Retention Policy and any departure or extension out-with the policy must be justified and documented in line with the requirements of the data protection legislation. This approval must be documented and retrievable for audit purposes.

5.6 ***6th Principle: Personal data must be processed in a manner that ensures the appropriate security***

5.6.1 The Data Protection Officer will carry out a risk assessment taking into account all the circumstances of the Council's controlling or processing operations.

5.6.2 In determining appropriateness, the Data Protection Officer should also consider the extent of possible damage or loss that might be caused to individuals (e.g. staff or customers) if a security breach occurs, the effect of any security breach on the Council itself, and any likely reputational damage including the possible loss of customer/ residents trust.

5.6.3 When assessing appropriate technical measures, the Data Protection Officer will consult with Information Communications Team manager before giving consideration to the following:

a. Password protection;
b. Automatic locking of idle terminals;
c. Restrict use of USB sticks and ensuring encryption to the specific user;
d. Virus checking software and firewalls;
e. Role-based access rights including those assigned to temporary staff;
f. Encryption of devices that leave the organisations premises such as laptops;
g. Security of local and wide area networks;

5.6.4 When assessing appropriate organisational measures the Data Protection Officer will consider the following:

a. The appropriate training levels throughout the Council;
b. The inclusion of data protection in employment contracts;
c. Identification of disciplinary action measures for data breaches;
d. Physical access controls to electronic and paper based records;
e. Adoption of a clear desk policy;

5.6.5 These controls have been selected on the basis of identified risks to personal data, and the potential for damage or distress to individuals whose data is being processed.

5.7 The controller must be able to demonstrate compliance with the GDPR's other principles (accountability).

5.7.1 The GDPR includes provisions that promote accountability and governance. These complement the GDPR's transparency requirements. The accountability principle in Article 5(2) requires the Council to demonstrate that we comply with the principles and states explicitly that this is our responsibility.

5.7.2 The Council will therefore demonstrate compliance with the data protection principles by implementing data protection policies, adhering to codes of conduct, implementing technical and organisational measures, as well as adopting techniques such as data protection by design, DPIA's, breach notification procedures and incident response plans.

6. Data Subjects' Rights:

6.1 Data subjects have the following rights regarding data processing and the data that is recorded about them:

- To make subject access requests regarding the nature of information held and to whom it has been disclosed;
- To prevent processing likely to cause damage or distress;
- To prevent processing for purposes of direct marketing;
- To be informed about the mechanics of automated decision-taking process that will significantly affect them;
- To not have significant decisions that will affect them taken solely by automated process;
- To seek compensation if they suffer damage by any contravention of the GDPR;
- To take action to rectify, block, erase, including the right to be forgotten, or destroy inaccurate data;
- To request the supervisory authority to assess whether any provision of the GDPR has been contravened;
- To have personal data provided to them in a structured, commonly used and machine-readable format, and the right to have that data transmitted to another controller.
- To object to any automated profiling that is occurring without consent.

6.2 Uttlesford District Council ensures that data subjects may exercise these rights:

i) Data subjects may make data access requests as described in Subject Access Request Procedure; this procedure also describes how the Council will ensure that its response to the data access request complies with the requirements of the GDPR.

ii) Data subjects have the right to complain to Uttlesford District Council related to the processing of their personal data, the handling of a request from a data subject and appeals from a data subject on how complaints have been handled in line with the Council's complaints procedure.

7. Consent:

7.1 Uttlesford District Council understands 'consent' to mean that it has been explicitly and freely given, and a specific, informed and unambiguous indication of the data subject's wishes that, by statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her. The data subject can withdraw their consent at any time.

7.2 The Council understands 'consent' to mean that the data subject has been fully informed of the intended processing and has signified their agreement, while in a fit state of mind to do so and without pressure being exerted upon them. Consent obtained under duress or on the basis of misleading information will not be a valid basis for processing.

7.3 There must be some active communication between the parties to demonstrate active consent. Consent cannot be inferred from non-response to a communication. The Council in our role as data controller must be able to demonstrate that consent was obtained for the processing operation.

7.4 For sensitive data, explicit written consent of data subjects must be obtained unless an alternative legitimate basis for processing exists.

7.5 In most instances, consent to process personal and sensitive data is obtained routinely by Uttlesford District Council using standard consent documents e.g. when a new resident or customer signs a contract, or during induction process for new

employees.

7.6 Where Uttlesford District Council provides services to children, parental or custodial authorisation must be obtained. This requirement applies to children under the age of sixteen (16) years.

8. Security of Data:

8.1 All Council staff are responsible for ensuring that any personal data that the Council holds and for which they are responsible is kept secure and under no circumstances disclosed to any third party unless that third party has been specifically authorised by the Council to receive that information and has entered into a confidentiality agreement.

8.2 All personal data should be accessible only to those who need to use it to enable the delivery of Public Service as required by the Council. All personal data should be treated with the highest security and must be retained:

- in a lockable room with controlled access; and/or
- in a locked drawer or filing cabinet; and/or
- if computerised, password protected in line with the Council's ICT policy and/or
- stored on (removable) computer media which are encrypted in line with the Council's ICT Policy.

8.3 Care must be taken to ensure that personal computer screens and terminals are not visible except to authorised staff of the Council. All members of staff are required to enter into an Acceptable Use Agreement before they are given access to organisational information of any sort, which details rules on screen time-outs.

8.4 Manual records containing personal data may not be left where they can be accessed by unauthorised personnel and must not be removed from Council premises without explicit authorisation. As soon as manual records which contain personal data are no longer required for day-to-day client support, they must be removed from secure archiving.

8.5 Personal data may only be deleted or disposed of in line with the Document Retention Policy. Manual records which have reached their retention date are to be shredded and disposed of as 'confidential waste'. Hard drives of redundant personal computers (PC's) are to be removed and immediately destroyed as required by the

Council's IT security policy before disposal.

8.6 Processing of personal data 'off-site' presents a potentially greater risk of loss, theft or damage to personal data. Staff must be specifically authorised by their Service Manager to process personal data off-site external to any Council premises.

9. Disclosure of Data:

9.1 Uttlesford District Council has a responsibility to ensure that personal data is not disclosed to unauthorised third parties which includes family members, friends, and government bodies. All staff should exercise extreme caution when asked to disclose personal data held on another individual to a third party. It is equally important to bear in mind whether or not disclosure of the information is relevant to, and necessary for, the conduct of the Council's business.

9.2 All requests to provide data for one of these reasons must be supported by appropriate paperwork and all such disclosures must be specifically authorised by the Manager of the service area concerned.

10. Retention and Disposal of Data:

10.1 Uttlesford District Council shall not keep personal data in a form that permits identification of data subjects for longer a period than is necessary, in relation to the purpose(s) for which the data was originally collected.

10.2 The Council may store data for longer periods if the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes, subject to the implementation of appropriate technical and organisational measures to safeguard the rights and freedoms of the data subject.

10.3 The retention period for each category of personal data will be set out in the Document Retention Policy along with the criteria used to determine this period including any statutory obligations which the Council has to retain the data.

10.4 Personal data must be disposed of securely in accordance with the sixth principle of the GDPR – processed in an appropriate manner to maintain security, thereby protecting the "rights and freedoms" of data subjects.

11. Record of Processing Activity / Data Flowcharts:

11.1 Uttlesford District Council has established a Record of Processing Activity (ROPA) and data flow process as part of its approach to address risks and ensure compliance with GDPR. The Council's' ROPA and data flow charts determines:

- business processes that use personal data;
- source of personal data;
- volume of data subjects;
- description of each item of personal data;
- processing activity;
- categories of personal data processed;
- the purpose(s) for which each category of personal data is used;
- recipients, and potential recipients, of the personal data;
- the role of the Council throughout the data flow;
- key systems and repositories;
- any data transfers; and
- retention and disposal requirements.

11.2 The Council is aware of any risks associated with the processing of particular types of personal data.

11.3 The Council assesses the level of risk to individuals associated with the processing of their personal data. A Data Protection Impact Assessment procedure (DPIA) is carried out in relation to the processing of personal data by the Council and in relation to processing undertaken by other organisations on behalf of the Council.

11.4 The Council manages any risks identified by the risk assessment in order to reduce the likelihood of a non-conformance with this policy.

11.5 Where a type of processing, in particular using new technologies and taking into account the nature, scope, context and purposes of the processing is likely to result in a high risk to the rights and freedoms of natural persons, the Council shall, prior to the processing, carry out a DPIA of the impact of the envisaged processing operations on the protection of personal data. A single DPIA may address a set of similar processing operations that present similar high risks.

11.6 Where, as a result of a DPIA it is clear that the Council is about to commence processing of personal data that could cause damage and/or distress to the data subjects, the decision as to whether or not the Council may proceed must be reviewed by the Data Protection Officer.

11.7 If there are significant concerns either as to the potential damage or distress or the quantity of data concerned the Data Protection Officer may escalate the matter to the supervisory authority (the Information Commissioners Office).

Document Owner:
The Data Protection Officer is the owner of this document and is responsible for ensuring that this procedure is reviewed in line with the requirements of the GDPR.

Change History Record:

Issue	Reason for change	Approval	Date of Issue
1	New document - (1st publication)	Simon Pugh (Assistant Director Governance & Legal)	23rd May 2018
2	Biennial review by DPO to ensure currency and compliance with Data Protection Legislation - June 2020	Simon Pugh (Assistant Director Governance & Legal)	June 2020