STOTFOLD TOWN COUNCIL

INFORMATION AND DATA PROTECTION POLICY

1. PURPOSE

1.1 Stotfold Town Council takes the security and privacy of data seriously and is committed to being transparent about how it collects and uses personal data and meets its data protection obligations. The Town Council is registered as a “data controller” with the Information Commissioner’s Office (“ICO”) and will comply with our legal obligations under the Data Protection Act 2018 (the “Legislation") and the UK Data Protection Regulation 2018 (“ UK GDPR”).

1.2 This Policy sets out the Town Council’s commitment to data protection and individual rights in relation to personal data and sensitive personal data. This Policy explains how the Town Council will hold and process personal information and explains the individual’s rights as a “data subject.”

1.3 This Policy replaces any earlier Policy under previous legislation.

2. DATA PROTECTION OFFICER

2.1 The appointed Data Protection Officer for Stotfold Town Council is the Town Clerk. Their role is to inform and advise the Town Council of obligations under the Data Protection Act 2018 and to monitor the Town Council’s compliance.

2.2 The Data Protection Officer acts as the single point of contact for the Information Commissioner’s Office (“ICO”) and provides advice and assistance on Data Protection Impact Assessments.

2.3 The Town Clerk can be contacted at:

Email: enquiries@stotfoldtowncouncil.gov.uk
Telephone at 01462 730 064
Correspondence: The Town Clerk, Stotfold Town Council, The Greenacre Centre, Valerian Way, Stotfold, Hitchin, Herts, SG5 4HG

3. DATA PROTECTION DEFINITIONS

3.1 There are two types of data under the Legislation:

- “personal data” which is information relating to a living individual who can be identified from that information (a “data subject”) on its own or when taken together with other information. This may include both facts and expressions of opinion about the person and indication of the intentions of the Council or others in respect of that person. It does not include anonymised data.
- “special category data” which is information about an individual’s racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, health, sex life or sexual orientation and genetic and biometric data.

3.2 Other definitions relevant to data protection:

- “criminal records data” means information about an individual’s criminal convictions and offences and information relating to criminal allegations and proceedings.
- “data processing” means any use that is made of personal data, including collecting, recording, organising, combining, structuring, storing, amending, retrieving, or consulting, disclosing (by transmission, dissemination or otherwise making available) or restricting or destroying data. This includes processing personal data held in manual form in a relevant filing system, accessible record or processed automatically.

3.3 More detailed definitions for ‘personal data’ ‘special category data’ ‘criminal records data’ ‘data processing’ ‘data subject’ ‘data controller’ and ‘data processor’ are set out in the Legislation.

4. DATA PROTECTION PRINCIPLES

4.1 There are six data protection principles that govern the processing of data to ensure compliance with the Legislation and to protect the interests of individuals. Under these principles personal data:

- Be processed fairly, lawfully, and transparently (*Fairness, lawfulness, and transparency);*
- Be collected and processed only for specified, explicit and legitimate purposes (*Purpose limitation);*
- Be adequate, relevant, and limited to what is necessary for the purposes for which it is processed (*Data minimisation);*
- Be accurate and kept up to date. Any inaccurate data must be deleted or rectified without delay (*Accuracy);*
- Not be kept for longer than is necessary for the purposes for which it is processed (*Storage limitation);*
- Be processed securely. To that end the Council adopts appropriate measures to make sure that personal data is secure and protected against unauthorised or unlawful processing and accidental loss, distribution, or damage (*Integrity and confidentiality).*

In addition, there is an overarching principle of accountability

- To be responsible for complying with the UK GDPR and being able to demonstrate this (Accountability).

4.2 Lawfulness of Processing

4.2.1 Personal data can only be lawfully processed if one or more of the following conditions apply:

- The data subject has given consent to the processing;
- Processing is necessary for the performance of a contract with the data subject;
- Processing is necessary for compliance with a legal obligation to which the data controller is subject;
- Processing is necessary to protect the vital interests of the data subject or another person;
- Processing is necessary for the performance of a task carried out in the public interest;

- Processing is necessary for the purposes of the legitimate interests pursued by the data controller or a third party; (This ground is not available to public authorities such as the Council).

4.2.2 Special category data can only be lawfully processed if one or more of the following conditions apply:

- The data subject has given explicit consent to the processing for one or more specified purpose/s;
- Processing is necessary for the purposes of carrying out the obligations and exercising specific rights of the controller or of the data subject in the field of employment and social security and social protection law;
- Processing is necessary to protect the vital interests of the data subject or of another natural person where the data subject is physically or legally incapable of giving consent;
- Processing is carried out in the course of its legitimate activities by a foundation, association or any other not for profit body with a political, philosophical, religious or trade union aim and on condition that the processing relates solely to the members or to former members of the body or to persons who have regular contact with it in connection with its purposes and that the data is not disclosed outside that body without the consent of the data subjects;
- Processing relates to personal data which is manifestly made public by the data subject;
- Processing is necessary for the Town Council to exercise or defend legal claims or whenever courts are acting in their judicial capacity;
- Processing is necessary for reasons of substantial public interest;
- Processing is necessary for the purposes of preventative or occupation medicine, for the assessment of the working capacity of the employee or medical diagnosis;
- Processing is necessary for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes.

4.2.3 Criminal records data can only be lawfully processed if in accordance with the Appropriate Policy for the processing of special category data and criminal record data as required by Schedule 1 Part 4 and Sections 38, 39 and 40 of Data Protection Act 2018.

4.2.4 Once the Town Council has established that it has the right to process an individual's personal data it will do so only within the framework of the 6 Data Protection Principles.

5. INDIVIDUAL RIGHTS

As a data subject individuals have a number of rights in relation to their personal data as defined within the Data Protection Principles.

5.1 Data Subject Access Requests

5.1.1 Individuals have the right to request a copy of their personal data being processed by the Town Council under a "Subject Access Request" ("SAR"). This will usually be in electronic form if the individual has made the request electronically unless they agree otherwise.

5.1.2 A SAR does not necessarily extend to all records or correspondence containing the individual's name or personal identifier. To be included in a response to a SAR the information needs to relate to, be about or be linked to, the named individual. The Town Council may ask an individual to specify the information to which the request relates.

5.1.3 The Town Council will respond within one calendar month unless the request is complex or if there are a number of requests. Should this be the case, , in which case the period can be extended by a further two months. If an extension is necessary the Town Council will write to the individual within one month of receiving the original request to explain why an extension may be necessary.

5.1.4 If a SAR is manifestly unfounded, excessive, or unreasonable, the Town Council is not obliged to comply with it. Alternatively, the Town Council may charge a fee based on the administrative cost of responding to the request as set out in more details within the Publication Scheme 2025.

5.1.5 The Town Council will explain to an individual the circumstances of any refusal to respond to a request and of their right to complain to the Information Commissioner's Office.

5.1.6 Requests can be made by submitting a request to enquiries@stotfoldtowncouncil.gov.uk. The Town Council will need to ask for identification from the requestor before the request can be processed. If the SAR is being requested on behalf of a third party, written permission will need to be supplied to the Town Council from the individual named in the SAR, with their relevant identification included stating the third party is acting on their behalf.

5.2 Other rights

5.2.1 Individuals have a number of other rights in relation to their personal data:

- The right to information about what personal data the Council processes, how and on what basis;
- To request that inaccurate data is rectified;
- With some exceptions, individuals have the right to request that the Town Council stops processing or erases their personal data that is no longer necessary to process for the purpose if was collected;
- The right to object to data processing;
- With some exceptions the right to intervene and not be subject to automated decision making;
- The right to be notified of a data security breach concerning their personal data where there is a high risk of harm;
- Where consent is relied upon as a lawful ground to process data the right to not consent or withdraw consent later;
- The right to have their information moved to another provider following a written request.

5.2.2 To ask the Council to take any of these steps an individual should send the request to enquiries@stotfoldtowncouncil.gov.uk.

6. DATA SECURITY

6.1 The Council takes the security of personal data seriously. The Council has internal policies and controls in place to protect personal data against loss, accidental destruction, misuse, or disclosure and to ensure that data is not accessed, except by those who have lawful authority in connection with the proper performance of their duties.

6.2 The Council recognises that the personal data it holds is valuable and must be managed properly as accidental loss, unlawful destruction or damage may cause distress to individuals concerned.

6.3 Examples of our security processes include:

- Encryption - meaning that information is hidden so that it cannot be read without special knowledge such as a password.
- Pseudonymisation - meaning that information will be recorded with alternative naming conventions to ensure personal information is not accessible by all.
- Controlling access to systems and networks based on functions within the Town Council which allows sonal information from getting access to it.
- Regular testing of technology and upgrading security measures, including keeping up to date on the latest security updates for software and information technology devices the Town Council manages.
- Training of staff on handling of personal information and reporting any data breaches or data concerns.

6.4 Where the Town Council engages third parties to process personal data on its behalf, such parties do so on the basis of written instructions and are obliged to implement appropriate technical and organisational measures to ensure the security of data in accordance with the Town Council's policies, the outcome of any Data Processing Impact Assessment and the standards required by the Legislation.

7. DATA PROTECTION IMPACT ASSESSMENTS

7.1 The processing of some data that the Town Council carries out may result in risks to privacy. Where processing would result in a high risk to an individual's rights and freedoms the Town Council will carry out a Data Protection Impact Assessment to determine the necessity and proportionality of processing.

7.2 This will include considering the purposes for which the activity is carried out, an assessment of necessity, proportionality and compliance measures, the risk for individuals and the measures that can be put in place to mitigate those risks.

7.3 The Data Protection Officer will be consulted in relation to all Data Protection Impact Assessments.

8. DATA BREACHES

8.1 If the Council discovers that there has been a breach of personal data that poses a risk to the rights and freedoms of individuals we will report it to the Information Commissioner's Office within 72 hours of discovery. The Council will record all data breaches regardless of their effect.

8.2 If the breach is likely to result in a high risk to the rights and freedoms of individuals we will tell affected individuals that there has been a breach and provide them with information about its likely consequences and the mitigation measures we have taken.

8.3 The Town Council has policies and procedures for handling suspected data breaches to ensure compliance with the Legislation.

8.4 Any suspected data breach should be reported immediately to townclerk@stotfoldtowncouncil.gov.uk.

9. STAFF TRAINING AND GUIDANCE

9.1 All Town Council staff have a responsibility to ensuring data is collected, stored, and processed appropriately in line with the Legislation and relevant policy.

9.2 Induction training for all new members of staff will include compulsory training on information management and data protection. Regular data protection updates or refresher training will be provided to all staff and managers. All staff are required to complete a mandatory e-learning module on UK GDPR.

9.3 Failure to observe data protection requirements can amount to a disciplinary offence by a member of staff and can be dealt with under the Council's disciplinary procedure.

9.4 Significant negligent or deliberate breaches of Town Council policies such as accessing employee or customer data without authorisation or a legitimate reason to do so may constitute gross misconduct and could lead to dismissal without notice.

10. INTERNATIONAL DATA TRANSFERS

There are strict rules regarding the transfer of personal data to other countries. The Town Council will not transfer personal data outside of the UK without having appropriate contractual, security and privacy arrangements in place.

11. DATA SHARING

11.1 The Town Council may need to share an individual's personal data with third parties. When this is done it will be carried out in compliance with the Legislation including the 6 data protection principles.

11.2 The Town Council will only share personal data if it follows those principles and is justified on the basis that the benefits (after taking into account any relevant safeguards) outweigh the risks of any possible negative effect on the data subject concerned. Where sharing is justified, the Town Council will take all reasonable steps to minimise any negative impact on the data subject. The amount of information shared, and the extent of sharing will be limited to that which is necessary to carry out a particular function.

11.3 The threshold for sharing special category data is higher than for other sorts of personal information. Therefore, the Council will only share this type of information where there is an overriding need to do so and/or where there is a specific provision to do so within the Legislation.

12. INFORMATION COMMISSIONER'S OFFICE (ICO)

12.1 The ICO is responsible for upholding information rights in the public interest. The ICO can take action to change the behaviour of organisations and individuals that collect use and keep personal information. The ICO may use criminal prosecution, non-criminal enforcement and audit depending upon the circumstances.

12.2 The ICO maintains a public register of data controllers. Stotfold Town Council is registered as a data controller with the ICO.

12.3 Independent advice regarding data protection and freedom of information can be obtained from the ICO at www.ico.org.uk.

13. CRIMINAL OFFENCES

13.1 Breaches of the Legislation through loss or mishandling of personal data can result in large fines and significant reputational damage.

13.2 Officers and Councillors can also face disciplinary and/or enforcement action for misusing, unlawfully or recklessly accessing personal data which they have access to as part of their employment or appointment with the Town Council.

13.3 The Town Council recognises that its residents value their privacy and is committed to achieving high levels of compliance with all relevant data protection legislation.

14. POLICIES AND PROCEDURES

The Town Council's relevant Policies and Procedures governing data protection and freedom of information include:

- This Policy;
- Business Continuity Plan 2024;
- CCTV Code of Practice 2024;
- Councillor IT Device Usage Policy 2024;
- Data Breach Policy 2018;
- Document Retention Policy 2018;
- Freedom of Information Procedure;
- Privacy Notice 2025;
- Privacy Consent Form;
- Publication Scheme 2024;
- Disclosure Log 2024;
- Risk Management Strategy 2024;
- Subject Access Request Procedure 2025;
- Standing Orders 2025;
- Privacy Statement 2018 which can be accessed from the Town Council's website. This provides details regarding why the Town Council collects and uses personal information, how the Council will use personal information and who we may need to share personal information with.

15. COMPLAINTS

15.1 In the event of a complaint regarding the way personal data has been processed by the Town Council, individuals are able to refer their complaint to the Town Council Data Controller at enquiries@stotfoldtowncouncil.gov.uk / Tel: 01462 730 064 or to the ICO at casework@ico.org.uk / Tel: 0303 123 1113.

Revision History:

Date Adopted	March 2025	Replaced the previous policy - Information and Data Protection Policy – 2018
Date reviewed		