AYLESBURY
TOWN COUNCIL

Data Protection Policy

1. Introduction

We process personal data about our employees, clients, customers and other individuals for a variety of business purposes and in the exercise of official authority. This might include names, addresses, telephone numbers etc.

This policy sets out how we seek to protect personal data and ensure that staff and council members understand the rules governing their use of personal data to which they have access in the course of their work.

This policy is underpinned by the Data Protection Act 2018 and the UK General Data Protection Regulation, and is informed by guidance from the Information Commissioner's Office (ICO).

2. Scope

This policy applies to all staff, volunteers, council members, contractors, suppliers and anyone working on behalf of the Town Council, and covers electronic and manual records.

3. Definitions

3.1 Personal Data

Personal data is any information relating to an identified or identifiable living person. Identified means that the information directly identifies a person, such as a database of names and addresses. Identifiable means that a person could be identified by matching two or more sets of data, e.g. one database may hold a list of staff names and their employee numbers, while a separate database may hold employee ID numbers and addresses; it would not be difficult to match the two and identify someone. Encrypted personal data is also covered because people are identifiable when the password is used;

this is known as pseudonymous data. This does not apply to anonymous data unless the data collected is so detailed or specific so as to allow identification.

This definition includes online and electronic identifiers such as internet protocol (IP) addresses, which can uniquely identify a computer or mobile device, cookies, which may uniquely identify website visitors, and GPS data, such as from mobile phones, which may be used to locate an individual.

3.2 Special Categories of Personal Data

Previously known as Sensitive Data, these categories may only be processed in special circumstances:

- Racial or ethnic origin
- Political opinions
- Religious or philosophical beliefs
- Trade Union membership
- Health
- Sex life or sexual orientation
- Genetic and biometric data, such as fingerprints, photographs and DNA swabs.

3.3 Data Subject

The data subject is an individual whose personal data is being processed.

3.4 Processing

Processing any operation performed on 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.

3.5 Data Controller/Processor

The data controller is the body which determines the purposes and means of processing personal data; this is the Town Council for the purposes of this policy. Aylesbury Town Council is the data controller only for activities directly related to Aylesbury Town Council business. Aylesbury Town Council business is defined as work carried out on behalf of the Town Council as a corporate body, which has first been approved by the Town Clerk. Where a councillor is a member of a political party, that political party may act as the data controller for activities directly related to that political party. Councillors are advised to register themselves as a data controller with the ICO for any data processing activities which fall outside the remit of Aylesbury Town Council business or the remit of their political party, if any.

The data processor processes personal data on behalf of the data controller, e.g. processing payroll. In most cases, the Town Council will also be the data processor.

4. Principles of Processing Personal Data

When processing personal data, we will adhere to all of the following principles:

4.1 Lawfulness, Fairness and Transparency

We must have a legal basis for processing personal data (see 5. Lawfulness of Processing Personal Data) and inform the data subject at the point of collecting their personal data exactly how and why it will be used (see 9. Privacy Notices). The data protection register describes the legal basis for each area of the council's work.

4.2 Purpose Limitation

We will collect personal data for specified, explicit and legitimate purposes, and not process it further in a manner that is incompatible with those purposes. The data protection register lists which information we collect and how and why we use it.

4.3 Data Minimisation

Personal data we process must be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed. The data protection register describes the reasons why each piece of information is needed and whether or not it is legally required.

4.4 Accuracy

Personal data we process must be accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that is inaccurate, having regard to the purposes for which they are processed, is erased or rectified without delay. The data protection register describes how this is accomplished for each area of the Town Council's work.

4.5 Storage Limitation

We must keep personal data for no longer than is necessary for the purposes for which the personal data is processed, unless there is a legal obligation to do so. The data protection register contains a retention schedule for each area of the Town Council's work.

4.6 Integrity and Confidentiality

We must process personal data in a manner that ensures appropriate security, including protection against unauthorised or unlawful processing and against accidental loss,

destruction or damage, using appropriate technical or organisational measures; these are listed in the data protection register.

4.7 Accountability

Compliance with these principles is documented in the data protection register.

5. Lawfulness of Processing Personal Data

The Town Council may only process personal data when at least one of the following legal bases are true:

- The data subject has given consent to the processing of their personal data for one or more specific purposes.
- Processing is necessary for the performance of a contract or in order to take steps at the request of the data subject prior to entering into a contract.
- Processing is necessary for compliance with a legal obligation.
- Processing is necessary in order to protect the vital interests of the data subject or of another person.
- Processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority.
- Processing for the purposes of the pursuing legitimate interests is not available to the Town Council as a public authority.

The legal basis for each area of the Town Council's work is documented in the data protection register.

6. Conditions for Consent

Where the Town Council relies on consent as its legal basis for processing personal data, consent must be clear, affirmative, freely given, specific, informed and unambiguous. Silence, pre-ticked boxes or inactivity do constitute consent. Consent should cover all processing activities carried out. When the processing has multiple purposes, consent should be given for all of them. Any request for consent must be written in plain English and clearly distinguishable from other information provided. Consent may be withdrawn at any time, as easily as it was given, and the data subject will be informed of this right beforehand.

7. Processing Special Categories of Personal Data

The Town Council will only process special categories of data in at least one of the following circumstances:

- The data subject has given explicit consent to the processing for one or more specified purposes.
- Processing is necessary for the Town Council to carry out obligations and fulfil specific rights to itself or the data subject in the fields of employment, social security and social protection law.
- Processing is necessary to protect the vital interests of the data subject or of another person where the data subject is physically or legally incapable of giving consent
- Processing is carried out in the course of the Town Council's legitimate activities as a not-for-profit body with a political and philosophical aim. We will ensure that such processing relates solely to members, former members and people who have regular contact in connection with these aims, and that the personal data are not disclosed outside the Town Council without the consent of the data subjects.
- Processing relates to personal data which are manifestly made public by the data subject.
- Processing is necessary for the establishment, exercise or defence of legal claims.
- Processing is necessary for reasons of substantial public interest, which shall be proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject.
- Processing is necessary for the purposes of preventive or occupational medicine, for the assessment of the working capacity of employees, medical diagnosis, the provision of health or social care or treatment or the management of health or social care systems and services.
- Processing is necessary for reasons of public interest in the area of public health, such as pandemic planning.
- Processing is necessary for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes.

Any processing of special categories of personal data will be documented in the data protection register.

8. Rights of the Data Subject

The Town Council must uphold the following rights afforded to data subjects, when processing personal data:

8.1 Information

Data subjects must be informed about how and why their personal data is being processed, as well as their rights detailed below. The Town Council will provide this information by way of a privacy notice the point of collection (see 9. Privacy Notices).

8.2 Access

Data subjects are entitled to request access to information held about them, providing this does not adversely affect the rights and freedoms of others. This is known as a subject access request. The following information must also be provided:

- The purposes of the processing.
- The categories of personal data concerned.
- The recipients of the personal data.
- The envisaged period for which the personal data will be stored.
- The right to request the rectification or erasure of personal data and the right to object to or request restriction of processing of personal data.
- The right to lodge a complaint with the ICO.
- Where the personal data are not collected from the data subject, any available information as to the source.
- the existence of automated decision-making, including profiling, and meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject.

Any written request counts as a subject access request and should be referred to the DPO, to be actioned within one month from receipt.

8.3 Rectification

Data subjects have the right to rectification of inaccurate data and the completion of incomplete data. Request should be referred to the DPO.

8.4 Erasure

Known as “the right to be forgotten”, a data subject may request that any information held on them is deleted or removed, and any third parties who process or use that data must also comply with the request. An erasure request can only be refused if one of the following exemptions applies:

- To exercise the right of freedom of expression and information.
- To comply with a legal obligation or for the performance of a public interest task or exercise of official authority.
- For public health purposes in the public interest.
- Archiving purposes in the public interest, scientific research historical research or statistical purposes.
- The exercise or defence of legal claims.

Requests should be referred to the DPO, to be actioned within one month from receipt.

8.5 Restriction

A data subject has the right to restrict processing of their personal data in the following cases:

- When the data subject contests the accuracy of their personal data, processing will be restricted for a period enabling the Town Council to verify the accuracy as rectify as necessary.
- The processing is unlawful and the data subject opposes the erasure of their personal data and requests restriction instead.
- The Town Council no longer needs the personal, but the data subject requires it for the establishment, exercise or defence of legal claims.
- When the data subject objects to the processing of their personal data (see 8.7 Objection), processing will be restricted while the Town Council verifies whether its legitimate grounds override those of the data subject.

Requests should be referred to the DPO. Any third parties who process or use that data must also comply with the request.

8.6 Portability

Data subjects have the right to request a copy of their personal data in a structured, commonly used and machine-readable format, and to request that their data is transferred directly to another system, in the following cases:

- Where the processing is based on the individual's consent or for the performance of a contract; and
- When processing is carried out by automated means.

This right does not apply to processing necessary for the performance of a task carried out in the public interest or in the exercise of official authority, or if doing so would adversely affect the rights and freedoms of others.

Requests should be referred to the DPO, to be actioned within one month from receipt. Data will be provided in Comma Separated Value (.CSV) format.

8.7 Objection

A data subject has the right to object where the Town Council processes personal data in the performance of a task carried out in the public interest or in the exercise of official authority, or for direct marketing. The Town Council must stop processing the personal data unless there are compelling legitimate grounds which override the interests, rights and freedoms of the data subject or for the establishment, exercise or defence of legal claims. Requests should be referred to the DPO.

9. Privacy Notices

At the point of personal data being collected, the following information will be provided to the data subject in the form of a privacy notice:

- The Town Council is identified as the data controller, together with contact details.
- The contact details of the DPO.
- The purposes and legal basis for the processing of the personal data.
- The recipients of the personal data.
- The period for which the personal data will be stored, or if that is not possible, the criteria used to determine that period.
- The rights of access, rectification, erasure, restriction and portability of their personal data
- Where the processing is based on consent, the right to withdraw consent at any time.
- The right to lodge a complaint with the ICO.
- Whether the provision of personal data is a statutory or contractual requirement, or necessary to enter into a contract, as well as whether the data subject is obliged to provide the personal data and of the possible consequences of failure to provide such data.
- The existence of any automated decision-making, and meaningful information about the logic involved, as well as the significance and the envisaged consequences for the data subject.

Samples of all forms used to collect data, which will include appropriate privacy notices, are available in the data protection register.

10. Privacy Impact Assessments

A privacy impact assessment (PIA) identifies privacy risks and risk reduction strategies. The Town Council will assess all new projects to ensure risks to privacy are effectively managed. PIAs are also useful for reviewing existing systems; all current areas of the

Town Council's work have been assessed, and these can be found in the data protection register.

The process for conducting a PIA is as follows:

10.1 Identify the need for a PIA

A PIA will be necessary the following cases:

- New personal information will be processed.
- Existing personal information will be processed for a different purpose to that for which it was collected.
- Personal information will be made available to different bodies.
- The use of potentially intrusive technology such as biometrics.
- Decisions or actions may be taken which could impact on individuals.
- Special categories of data or otherwise sensitive data will be processed.
- Contacting individuals in ways they may find intrusive.

10.2 Describe Information Flows

Describe how information is collected, stored, used and deleted, what information is used, what it is used for and who will have access to it.

10.3 Identify Privacy and Related Risks

The PIA process is a form of risk assessment and management. Risks will broadly fall into three categories: risks to individuals e.g. inappropriate sharing of personal data; corporate risks e.g. bad publicity; and compliance risks e.g. non-compliance with legislation relating to data protection.

10.4 Identify and Evaluate Privacy Solutions

Privacy solutions are steps which can be taken to reduce the privacy impact. The aim of this stage of the process is to balance the project's outcomes with the impact on individuals' privacy. The costs and benefits of possible privacy solutions should be assessed. Some costs will be financial, for example purchasing additional software to give greater control over data access and retention. The costs should be balanced against the benefits, for example the increased assurance against a data breach, and the reduced risk of regulatory action and reputational damage.

10.5 Sign off and record the PIA outcomes

It is important to keep a record of the process. This will ensure that the necessary measures are implemented. It can also be used to assure the public, the ICO, and other stakeholders that the project has been thoroughly assessed. PIAs should be checked and signed off by the DPO.

11. The Data Protection Officer (DPO)

As a public authority, the Town Council is obliged to appoint a DPO, who must be involved in all issues which relate to the protection of personal data. The DPO is responsible for the following:

- Inform and advise the Town Council of its data protection obligations, monitor compliance with this policy, raise awareness and arrange training.
- Provide advice on privacy impact assessments and monitor their performance.
- Act as a contact point and co-operate with the ICO.
- Act as a contact point for data subjects regarding all issues related to processing of their personal data and to exercise their rights.

12. Records of Processing

The Town Council maintains a data protection register, under the supervision of the DPO, which details the following information:

- The Town Council's contact details as the data controller and contact details of any data processors working on the Town Council's behalf.
- The DPO's contact details.
- The purposes of the processing.
- The categories of data subjects and categories of personal data.
- The categories of recipients of personal data.
- The data retention schedule.
- Technical and organisation data security measures.

Data processors working on behalf of the Town Council must also maintain their own records of processing.

13. General Security Measures

13.1 Computer security

- All computers must have a firewall, virus-checking and anti-spyware software installed and activated.
- Operating systems must be set to receive automatic updates.
- Staff must only have access to the information they need to their job.
- Special categories of data, bank details or otherwise sensitive information must be encrypted.

- Personal data must be removed before disposing of old computers (by using technology or destroying the hard disk).
- Strong passwords must be used - at least eight characters and have a combination of upper- and lower-case letters, numbers and the special keyboard characters like the asterisk or currency symbols.

13.2 Email security

- Email is not a secure medium hence personal data must not be sent by email, unless it is sent as an encrypted, password-protected attachment, with the password relayed using a verified telephone number.
- Care must be taken to enter the correct email address, bearing in mind autocomplete features could fill in an incorrect address.
- Blind carbon copy (bcc) should be used where necessary to avoid revealing email addresses to all recipients.
- Work email addresses must only be used for Town Council related business. Councillors should use an email account separate from their personal account.
- Spam must not be opened and should be deleted immediately.

13.3 Other security measures

- Hard copies of personal data must be disposed of in the confidential waste, to be securely shredded.
- The physical premises must be secure and protected with an alarm.

14. Personal Data Breaches

A personal data breach is a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data.

A record of personal data breaches is kept in the data protection register.

If a breach is likely to cause a risk to a data subject's rights and freedoms then the ICO must be notified of the following information within 72 hours:

- The nature of the personal data breach including where possible, the categories and approximate number of data subjects concerned and the categories and approximate number of personal data records concerned.
- The name and contact details of the data protection officer or other contact point where more information can be obtained.
- The likely consequences of the personal data breach.
- Measures taken or proposed to be taken to address the personal data breach, including, where appropriate, measures to mitigate its possible adverse effects.

If a breach is likely to cause a high risk to a data subject's rights and freedoms, then the data subject must also be notified, unless appropriate measures were taken before or after the breach to mitigate the high risk.

15. Review

This policy will be reviewed at least annually or sooner following a personal data breach or when there is a change to data protection legislation.

Adopted by Policy Committee	Ratified by Town Council	Reviewed	Amended	Next Review Date
11 July 2018	13 September 2018			January 2020
26 January 2021	11 February 2021	January 2021	January 2021	January 2022