2018

SHAFTESBURY TOWN COUNCIL

General Data Protection Regulations

22nd May 2018

SHAFTESBURY TOWN COUNCIL

General Data Protection Regulations Policy

Adopted on: 22nd May 2018

Review date: 2019

1. Introduction

An essential activity of Shaftesbury Town Council is the requirement to gather, process and store information about its employees, people in the community, suppliers, business contacts and other sources in order to operate efficiently.

The Town Council will seek the consent of individuals and companies to hold their personal data, where possible to do so. Records of those consenting will be kept.

2. General Data Protection Regulations

Article 5 of the General Data Protection Regulation requires that personal data shall be:

- Processed lawfully, fairly and in a transparent manner in relation to individuals;
- 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 to be incompatible with the initial purposes;
- Adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed;
- 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, are erased or rectified without delay;

- 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 the GDPR in order to safeguard the rights and freedoms of individuals;
- 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.

3. Privacy Policy

Shaftesbury Town council is committed to protecting and respecting the privacy of everyone and of ensuring it is fully compliant under the General Data Protection Regulation.

This policy (together with any other documents referred to within it) sets out the basis on which any personal data we collect, or is provided to us, will be processed. The following policy sets out the Town Council's practices regarding the collection and processing of personal data and how we treat it.

3.1. Personal Data we may collect:

"Personal data" is any information about a living individual which allows them to be identified from that data (for example a name, photographs, videos, email address, or address). Identification can be directly using the data itself or by combining it with other information which helps to identify a living individual. The processing of personal data is governed by legislation relating to personal data which applies in the United Kingdom including the General Data Protection Regulation (GDPR) and other legislation relating to personal data and rights such as the Human Rights Act.

3.2. Data Controllers:

Shaftesbury Town Council, is the data controller for all data collected.

3.2.1. Other data controllers the council works with:

- Town, District and County Councillors
- Local groups and organisations
- Sports Clubs
- DCC Occupational Health
- North Dorset District Council
- Dorset County Council
- Funeral Directors
- Stonemasons
- Charities
- Contractors

We may need to share personal data that we hold with them so that they can carry out their responsibilities to the council. If we and the other data controllers listed above are processing data jointly for the same purposes, then the council and the other data controllers may be “joint data controllers” which mean we are all collectively responsible for the data. Where each of the parties listed above are processing data for their own independent purposes then each of us will be independently responsible.

4. Individual rights and their personal data

Individuals have the following rights with respect to personal data:

When exercising any of the rights listed below, in order to process a request, we may need to verify identity for security. In such cases we will need the individual to respond with proof of identity before they can exercise these rights.

4.1. The right to access personal data we hold

At any point an individual can contact us to request the personal data we hold as well as why we have that personal data, who has access to the personal data and where we obtained the personal data from. Once we have received a request we will respond within one month.

There are no fees or charges for the first request but additional requests for the same personal data or requests which are manifestly unfounded or excessive may be subject to an administrative fee.

4.2. The right to correct and update the personal data we hold

If the data we hold is out of date, incomplete or incorrect, individuals can inform us and the data will be updated.

4.3. The right to have personal data erased

If an individual feels that we should no longer be using their personal data or that we are unlawfully using it, they can request that we erase the personal data we hold.

When we receive a request, we will confirm whether the personal data has been deleted or the reason why it cannot be deleted (for example because we need it for to comply with a legal obligation).

4.4. The right to object to processing of personal data or to restrict it to certain purposes only

Individuals have the right to request that we stop processing their personal data or ask us to restrict processing. Upon receiving the request, we will contact the person concerned and let them know if we are able to comply or if we have a legal obligation to continue to process the data.

4.5. The right to data portability

Individuals have the right to request that we transfer some of their data to another controller. We will comply with a request, where it is feasible to do so, within one month of receiving it.

4.6. The right to withdraw consent to the processing of data to which consent was obtained

Individuals can withdraw their consent easily by telephone, email, or by post (see Contact Details below).

4.7. The right to lodge a complaint with the Information Commissioner's Office.

To lodge a complaint, individuals can contact the Information Commissioner's Office on 0303 123 1113 or via email https://ico.org.uk/global/contact-us/email/ or at the Information Commissioner's Office, Wycliffe House, Water Lane, Wilmslow, Cheshire SK9 5AF.

5. Transfer of Data Abroad

Any personal data transferred to countries or territories outside the European Economic Area ("EEA") will only be placed on systems complying with measures giving equivalent protection of personal rights either through international agreements or contracts approved by the European Union. Our website is also accessible from overseas so on occasion some personal data (for example in a newsletter) may be accessed from overseas.

6. Further processing

If we wish to use personal data for a new purpose, not covered by the Privacy Policy or Privacy Notice, then we will provide you a new notice explaining this new use prior to commencing the processing and setting out the relevant purposes and processing conditions. Where and whenever necessary, we will seek prior consent to the new processing.

7. Subject Access Requests

Under section 7 of the Data Protection Act, a person may make a subject access request in relation to information held about them. A person who makes a request and pays a maximum £10 fee is entitled to the following information:

- To be told whether any personal data is being processed;

- A description of the personal data which is held, why the data is being processed and whether this data will be given to any other organisations or people;
- A copy of the information comprising the data; and
- The source of the data.

Once the Council receives such a request, should the data be disclosable, the request must be dealt with within 40 calendar days of receiving the request.

If the personal data which is the subject of the request is normally held for less than 40 days, then the request may be legitimately refused.

8. A Subject Access Request Which Concerns Other People's Information

A person may request access to data about them which also carries information regarding a third party. In such circumstances, the Council will assess whether the request can be complied with, without infringing the third party's privacy.

If the Council receives a request from an employee to access some personal data and complying with the request would mean disclosing information relating to another individual who can be identified from that information, then the request will be legitimately declined unless the third party consents to the disclosure or it is reasonable for the Council to comply with the request without the third party's consent.

There is an obligation upon a data controller to comply with as much of a request as possible. If the consent of the third party cannot be obtained and compliance with the request is reasonable, then the Council will consider separating the disclosable information from the non-disclosable information.

9. What is 'Personal Data'?

The Data Protection Act covers any data which concerns a living and identifiable individual.

Personal data could be a name accompanied by other information about the individual such as address, age or telephone number.

The Act does not cover information which is anonymous or aggregated data provided that the anonymisation or aggregation is not reversible.

10. Exceptions

There are circumstances in which a data controller is not obliged to supply certain information to the requester. Some of the most important exemptions apply to:

- Crime prevention and detection;
- Confidential references given by you (but not ones given to you); and
- Information covered by legal professional privilege.

11. Disclosure Information

The Council will as necessary undertake checks on both staff and members with the Disclosure and Barring Service and will comply with its Code of Conduct relating to the secure storage, handling, use, retention and disposal of disclosures and disclosure information. It will include an appropriate operating procedure.

12. Data Protection Impact Assessments (DPIAs)

The Town Council will carry out Data Protection Impact Assessments, (DPIAs), when it is necessary (e.g. prior to installing CCTV/ANPR surveillance systems). The decision to carry one out will be decided in consultation with the DPO whose advice will be sought in the following areas:

- Whether or not to carry out a DPIA;
- What methodology to follow when carrying out a DPIA;
- Whether to carry out the DPIA in-house or whether to outsource what it safeguards (including technical and organisational measures) to apply to mitigate any risks to the rights and interests of the data subjects.
- Whether or not the data protection impact assessment has been correctly carried out and whether its conclusions (whether or not to go ahead with the processing and what safeguards to apply) are in compliance with the GDPR.
- If the Town Council disagrees with the advice provided by the DPO, the DPIA documentation should specifically justify in writing why the advice has not been taken into account.
- The GDPR requires that councils carry out a DPIA when processing is likely to result in a high risk to the rights and freedoms of data subjects. This might

include using CCTV to monitor public areas, however separate Town council documentation is in place to cover the use of CCTV.

12.1. DPIA Assessment Checklist

Under the GDPR, data protection impact assessments (DPIAs) are mandatory where the processing poses a high risk to the rights and freedoms of individuals. While they can also be carried out in other situations, councils need to be able to evaluate when a DPIA is required. A checklist is provided by NALC to help Councils assess the need for a DPIA and provides a springboard for some of the issues to consider in more detail.

If two or more of the following apply, it is likely that a DPIA is required. This does not apply to existing systems but would apply if a new system is proposed.

1. Profiling is in use. Example: you monitor website clicks or behaviour and record people's interests. ☐
2. Automated-decision making. Example: when processing leads to the potential exclusion of individuals. ☐
3. CCTV surveillance of public areas. Processing used to observe, monitor or control data subjects. ☐
4. Sensitive personal data as well as personal data relating to criminal convictions or offences. ☐
5. Large scale data processing. There is no definition of "large scale". However consider: the number of data subjects concerned, the volume of data and/or the range of different data items being processed. ☐
6. Linked databases - in other words, data aggregation. Example: two datasets merged together, which could "exceed the reasonable expectations of the user" e.g. you merge your mailing list with another council, club or association. ☐
7. Data concerning vulnerable data subjects, especially when power imbalances arise, e.g. staff-employer, where consent may be vague, data of children, mentally ill, asylum seekers, elderly, patients. ☐
8. "New technologies are in use". E.g. use of social media, etc. ☐
9. Data transfers outside of the EEA. ☐
10. "Unavoidable and unexpected processing". For example, processing performed on a public area that people passing by cannot avoid. Example: Wi-Fi tracking. ☐