BLANDFORD FORUM TOWN COUNCIL

Privacy Policy

Adopted by full council: 23rd April 2018
Updated: 27th April 2018 (to remove references to the Data Protection Officer)

Twinned with Preetz, Germany

Town Clerk's Office
Church Lane, Blandford Forum
Dorset DT11 7AD

LOCAL COUNCIL AWARD SCHEME QUALITY GOLD

Twinned with Mortain, France

Tel: 01258 454500 • Fax: 01258 454432
Email: admin@blandfordforum-tc.gov.uk
www.blandfordforum-tc.gov.uk

Contents

1. Introduction

Blandford Forum Town Council is fully committed to compliance with the requirements of the General Data Protection Regulation (GDPR) from 25th May 2018, and subsequent Data Protection Act 2018, which supersedes the Data Protection Act 1998.
The Council will therefore follow procedures that aim to ensure that all employees, elected members, contractors, agents, consultants, partners or other servants of the council who have access to any personal data held by or on behalf of the council, are fully aware of and abide by their duties and responsibilities under the Act / Regulations and that the Council remains committed to protecting and respecting the privacy of all who provide their data.

For the purpose of the General Data Protection Regulation, the data controller is:

Blandford Forum Town Council, Town Clerk's Office, Church Lane, Blandford Forum, Dorset DT11 7AD.

2. Statement of Policy

In order to operate efficiently, the Town Council has to collect and use information about people with whom it works. This may include members of the public, current, past and prospective employees, clients and customers, and suppliers. In addition, it may be required by law to collect and use information in order to comply with the requirements of central government. This personal information must be handled and dealt with properly, however it is collected, recorded and used, and whether it be on paper, in computer records or recorded by any other means there are safeguards within the Act / Regulation to ensure this. The Town Council regards the lawful and correct treatment of personal information as very important to its successful operations and to maintaining confidence between the council and those with whom it carries out business. The Town Council will ensure that it treats personal information lawfully and correctly. Personal data may be processed on the basis that such processing is necessary for the performance of tasks carried out by public authority acting in the public interest, out of contractual necessity or on a lawful basis (e.g. a contract).

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.

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

Blandford Forum 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.

a) 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.

b) Data Controllers:

Blandford Forum Town Council, is the data controller for all data collected.

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.

c) What data do we process?

The council will process some, or all of, the following personal data where necessary to perform its tasks (see also the Town Council's Information Audit):

- Names, titles, and aliases, photographs;
- Contact details such as telephone numbers, addresses, and email addresses;
- Where they are relevant to the services provided by a council, or where you provide them to us, we may process information such as gender, age, marital status, nationality, education/work history, academic/professional qualifications, hobbies, family composition, and dependants;
- Where you pay for activities such as use of a council venue, financial identifiers such as bank account numbers, payment card numbers, payment/transaction identifiers, policy numbers, and claim numbers.
- The personal data we process may include sensitive or other special categories of personal data such as criminal convictions, racial or ethnic origin, mental and physical health, details of injuries, medication/treatment received, political beliefs, trade union affiliation, genetic data, biometric data, data concerning and sexual life or orientation.

d) How we use sensitive personal data

- We may process sensitive personal data, known as special category data, in order to comply with legal requirements and obligations to third parties.

- We need to have further justification for collecting, storing and using this type of personal data.
- We may process special categories of personal data in the following circumstances:
  - In limited circumstances, with explicit written consent.
  - Where we need to carry out our legal obligations.
  - Where it is needed in the public interest.
- Less commonly, we may process this type of personal data where it is needed in relation to legal claims or where it is needed to protect an individual's interests and they are not capable of giving consent, or where the information is already public.

e) Do we need consent to process sensitive personal data?

- In limited circumstances, we may approach individuals for written consent to allow us to process certain sensitive personal data. If we do so, we will provide full details of the personal data that we would like and the reason we need it, so that the individual can carefully consider whether they wish to consent.

f) The council will comply with data protection law, this says that the personal data we hold about you must be:

- Used lawfully, fairly and in a transparent way.
- Collected only for valid purposes that we have clearly explained and not used in any way that is incompatible with those purposes.
- Relevant to the purposes we have stated and limited only to those purposes.
- Accurate and kept up to date.
- Kept only as long as necessary for the purposes we have stated.
- Kept and destroyed securely including ensuring that appropriate technical and security measures are in place to protect personal data from loss, misuse, unauthorised access and disclosure.

g) We use your personal data for some or all of the following purposes:

- To deliver public services, including to understand individuals needs to provide the services that they request and to understand what we can do for the individual and inform them of other relevant services;
- To confirm identity to provide some services;
- To contact by post, email, telephone or using social media (e.g., Facebook, Twitter, WhatsApp);
- To help us to build up a picture of how we are performing;
- To prevent and detect fraud and corruption in the use of public funds and where necessary for the law enforcement functions;
- To enable us to meet all legal and statutory obligations and powers including any delegated functions;
- To carry out comprehensive safeguarding procedures (including due diligence and complaints handling) in accordance with best safeguarding practice from time to time with the aim of ensuring that all children and adults-at-risk are provided with safe environments and generally as necessary to protect individuals from harm or injury; (see Safeguarding Policy).
- To maintain our own accounts and records;
- To seek views, opinions or comments;
- To notify of changes to our facilities, services, events and staff, councillors and other role holders;
- To send communications which you have requested and that may be of interest to you. These may include information about campaigns, appeals, other new projects or initiatives;
- To process relevant financial transactions including grants and payments for goods and services supplied to the council
- To allow the statistical analysis of data so we can plan the provision of services.

Our processing may also include the use of CCTV systems for the prevention and prosecution of crime.

h) What is the legal basis for processing your personal data?

The council is a public authority and has certain powers and obligations. Most of the personal data is processed for compliance with a legal obligation which includes the discharge of the council's statutory functions and powers. Sometimes when exercising these powers or duties it is necessary to process personal data of residents or people using the council's services. We will always take into account the

interests and rights of the individual. This Privacy Policy, and the Privacy Notices, we display and distribute sets out the rights and the council's obligations to each individual. We may process personal data if it is necessary for the performance of a contract, or to take steps to enter into a contract. An example of this would be processing data in connection with the use of sports facilities, or the acceptance of an allotment garden tenancy. Sometimes the use of personal data requires consent, we will first obtain consent to use that data.

i) Sharing personal data

This section provides information about the third parties with whom the council may share personal data. These third parties have an obligation to put in place appropriate security measures and will be responsible to the individual directly for the manner in which they process and protect personal data. It is likely that we will need to share data with some or all of the following (but only where necessary):

- The data controllers listed above under the heading "Other data controllers the council works with";
- Our agents, suppliers and contractors. For example, we may ask a commercial provider to publish or distribute newsletters on our behalf, or to maintain our database software;
- On occasion, other local authorities or not for profit bodies with which we are carrying out joint ventures e.g. in relation to facilities or events for the community.

j) How long do we keep personal data?

We will keep some records permanently if we are legally required to do so. We may keep some other records for an extended period of time. For example, it is currently best practice to keep financial records for a minimum period of 8 years to support HMRC audits or provide tax information. We may have legal obligations to retain some data in connection with our statutory obligations as a public authority. The council is permitted to retain data in order to defend or pursue claims. In some cases, the law imposes a time limit for such claims (for example 3 years for personal injury claims or 6 years for contract claims). We will retain some personal data for this purpose as long as we believe it is necessary to be able to defend or pursue a claim. In general, we will endeavour to keep data only for as long as we need it. This means that we will delete it when it is no longer needed.

k) 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.

i) 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.

ii) 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.

iii) 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).

iv) 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.

v) 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.

vi) 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).

vii) 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.

l) 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.

m) Further processing

If we wish to use personal data for a new purpose, we will provide you with a new notice explaining this new use prior to commencing the processing and setting out the relevant purposes and processing conditions.

n) Changes to the Policy

We keep this Privacy Policy under regular review and we will place any updates on the Town Council's website at www.blandfordforum-tc.gov.uk.

4. Subject Access Request (SAR)

- The Town Council will inform data subjects of their right to access data and provide an easily accessible mechanism through which such a request can be submitted.
- 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.
- Ensure personal data is easily accessible at all times in order to ensure a timely response to SARs and that personal data on specific data subjects can be easily filtered.
- The Town Council will implement standards to respond to SARs, including a standard response.

Upon receipt of a SAR, staff are to refer to the SAR Policy and templates provided by NALC saved under BFTC GDPR 2018.

5. 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 Chairman of Council, whose advice will be sought in the following areas:

- Whether or not to carry out a DPIA (refer to the ICO website);
- 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.
- 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.

6. Cybersecurity

Data security is an ever-increasing requirement for most organisations, including councils. The number of risks and breaches which are the result of highly sophisticated attacks from hackers is still very limited and most breaches are the result of human error or relatively unsophisticated phishing attacks. The Town Council holds the Data Protection Policy of its current IT provider (available on request) and an explanation of how our data is managed securely. Please contact the Town Clerk's Office for further information should you have any concerns.

7. Security Incident Response

The Town Council takes any breach of data security seriously and in the event of such a breach the following response plan will be followed:

A data security breach is defined as the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data. This includes breaches that are the result of both accidental and deliberate causes. It also means that a breach is more than just about losing personal data.

Examples of which are:
- Access by an unauthorised third party.
- Deliberate or accidental action (or inaction) by a controller or processor.
- Sending personal data to an incorrect recipient.
- Computing devices containing personal data being lost or stolen
- Loss of availability of personal data.

In the event of a breach the Town Clerk is to be notified immediately, and in her absence the Operations Manager should be informed. Officers have been instructed to report any breaches immediately they suspect one may have occurred. An assessment will be made on the severity of any potential breach. Decisions are to be made by the Town Clerk after consultation with the Chairman of Council and Officers. These decisions will include but are not limited to: notifying the correct supervisory bodies and the individual involved in the breach.

If after investigating the incident it is confirmed that a personal data breach occurred, we will establish the likelihood and severity of the resulting risk to people's rights and freedoms. If it is likely that there will be a risk then we will notify the Information Commissioners Office (ICO). Any notifications to the ICO will be done not later than 72 hours after the breach was identified. The GDPR recognises that it will not always be possible to investigate a breach fully within 72 hours to understand exactly what has happened and what needs to be done to mitigate it. Article 34(4) allows us to provide the required information in phases, as long as this is done without undue delay. We will always prioritise the investigation, give it adequate resources, and expedite it urgently.

The Town Clerk will decide if the breach is notifiable after assessing both the severity of the potential or actual impact on individuals as a result of a breach and the likelihood of this occurring. In such cases, we will promptly inform those affected, particularly if there is a need to mitigate an immediate risk of damage to them, therefore allowing them time to take steps to protect themselves from the effects of a breach. We will provide them with a description of the likely consequences of the personal data breach; and what measures are being taken, or proposed

to be taken, to deal with the breach and including, where appropriate, the measures taken to mitigate any possible adverse effects.

If the decision is taken not to notify individuals, we will still notify the ICO unless the breach is unlikely to result in a risk to rights and freedoms. However, if a decision is made not to inform the ICO then that decision will be documented. As with any other breach of procedures or security incident officers will thoroughly investigate to ascertain whether the breach was a result of human error or a systemic issue. It will then be determined the best way to ensure how a recurrence can be prevented, whether this is through better processes, further training or other corrective steps.

8. Associated Documents

Other documents related to both the Privacy Policy are:

- Risk Management Policy (including Financial)
- Privacy Notice
- Audit Questionnaire
- Information Audit
- Freedom of Information Policy and Model Publication Scheme