BROADSTAIRS & ST. PETER'S TOWN COUNCIL	**GDPR Data Protection Policy** **Version 1**
	BROADSTAIRS & ST. PETER'S TOWN COUNCIL **Adopted: 26th March 2018**

1. Introduction

1.1 Broadstairs & St. Peter's Town Council (BSPTC) is committed to protecting the rights and freedoms of data subjects and safely and securely processing their data in accordance with all legal obligations.

1.2 BSPTC holds personal data about our employees, clients, suppliers and other individuals for a variety of business purposes.

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

2. Scope

2.1 This policy applies to all Councillors and staff of Broadstairs & St. Peter's Town Council.

2.2 This policy supplements our other policies relating to internet and email use. We may supplement or amend this policy by additional policies and guidelines from time to time. Any new or modified policy will be circulated to staff before being adopted.

3. Who is responsible for this policy?

3.1 The Town Clerk with the support of the data protection officer (DPO) will have overall responsibility for the day-to-day implementation of this policy.

3.2 A DPO will be selected annual and their full details set out in the Town Council minutes.

4. General Data Protection Regulation Principles

Broadstairs & St. Peter's Town Council will comply with the principles of data protection (enumerated in the EU General Data Protection Regulation. The Principles are:

1. Lawful, fair and transparent
Data collection will be fair, for a legal purpose and we will be open and transparent as to how the data will be used.

2. Limited for its purpose
Data can only be collected for a specific purpose.

3. Data minimisation
Any data collected will be necessary and not excessive for its purpose.

4. Accurate
The data we hold will be accurate and kept up to date.

5. Retention
We cannot store data longer than necessary.

6. Integrity and confidentiality
The data we hold will be kept safe and secure.

5. Responsibilities

5.1 BSPTC will undertake the following responsibilities under the GDPR

- Analysing and documenting the type of personal data we hold
- Checking procedures to ensure they cover all the rights of the individual
- Identify the lawful basis for processing data
- Ensuring consent procedures are lawful
- Implementing and reviewing procedures to detect, report and investigate personal data breaches
- Store data in safe and secure ways
- Assess the risk that could be posed to individual rights and freedoms should data be compromised

6. Responsibilities of the Data Protection Officer

6.1 BSPTC will employ a DPO to undertake the following tasks. The DPO will be agreed annually in a meeting of the Finance and General Purposes Committee.

6.2 The DPO will have the following responsibilities:

- Keeping the board updated about data protection responsibilities, risks and issues
- Reviewing all data protection procedures and policies on a regular basis
- Arranging data protection training and advice for all staff members and those included in this policy
- Answering questions on data protection from staff, board members and other stakeholders
- Responding to individuals such as clients and employees who wish to know which data is being held on them by us
- Checking and approving with third parties that handle the company's data any contracts or agreement regarding data processing

7. Responsibilities of the IT Manager

7.1 The Town Clerk will become the internal 'IT Manager'. It will be the responsibility of the Town Clerk to undertake following:

- Ensure all systems, services, software and equipment meet acceptable security standards
- Check and scan security hardware and software regularly to ensure it is functioning properly
- Research third-party services, such as cloud services the company is considering using to store or process data
- Responsibilities of the Marketing Manager
- Approve data protection statements attached to emails and other marketing copy
- Address data protection queries from clients, target audiences or media outlets
- Coordinate with the DPO to ensure all marketing initiatives adhere to data protection laws and the company's Data Protection Policy

As BSPTC currently outsources its IT provision and helpdesk to an external provider, the external provider will comply with Section 18 of this policy.

8. Accountability and transparency

8.1 BSPTC will ensure accountability and transparency in all our use of personal data. BSPTC will keep a written record of how all the data processing activities comply with each of the GDPR Principles. This will be kept up to date and will be approved by the DPO annually.

8.2 To comply with data protection laws and the accountability and transparency Principle of GDPR, BSPTC will meet the following data protection obligations:

- Fully implement all appropriate technical and organisational measures
- Maintain up to date and relevant documentation on all processing activities
- Conducting Data Protection Impact Assessments
- Implement measures to ensure privacy by design and default, including:
- Data minimisation
- Pseudonymisation
- Transparency
- Allowing individuals to monitor processing
- Creating and improving security and enhanced privacy procedures on an ongoing basis

9. Procedures

9.1 Fair and lawful processing

9.1.1 BSPTC will process personal data fairly and lawfully in accordance with individuals' rights under the first Principle. This means that we will not process personal data unless the individual whose details we are processing has consented to this happening.

9.1.2 If we cannot apply a lawful basis (explained below), our processing does not conform to the first principle and will be unlawful. Data subjects have the right to have any data unlawfully processed erased

9.2 Controlling vs. processing data

9.2.1 Broadstairs & St. Peter's Town Council is classified as a [data controller (and/or) data processor]. We will maintain our appropriate registration with the Information Commissioners Office in order to continue lawfully [controlling (and/or) processing] data.

9.2.2 BSPTC as a data processor, will comply with all contractual obligations and act only on the documented instructions of the data controller. As a data processor, we will:

- Not use a sub-processor without written authorisation of the data controller
- Co-operate fully with the ICO or other supervisory authority
- Ensure the security of the processing
- Keep accurate records of processing activities
- Notify the controller of any personal data breaches

9.3 Lawful basis for processing data

9.3.1 BSPTC will establish a lawful basis for processing data, ensuring that any data we are responsible for managing has a written lawful basis approved by the DPO. At least one of the following conditions will apply whenever we process personal data:

a) Consent – BSPTC will hold recent, clear, explicit, and defined consent for the individual's data to be processed for a specific purpose.

b) Contract- The processing is necessary to fulfil or prepare a contract for the individual.

c) Legal obligation- We have a legal obligation to process the data (excluding a contract).

d) Vital interests-Processing the data is necessary to protect a person's life or in a medical situation.

e) Public function- Processing necessary to carry out a public function, a task of public interest or the function has a clear basis in law.

f) Legitimate interest- The processing is necessary for our legitimate interests. This condition does not apply if there is a good reason to protect the individual's personal data which overrides the legitimate interest.

9.4 Deciding which condition to rely on

9.4.1 When making an assessment of the lawful basis, BSPTC will first establish that the processing is necessary.

9.4.2 The following factors will be considered:

- Can it reasonably be done in a different way?
- What is the purpose for processing the data?
- Is there a choice as to whether or not to process the data?
- Who does the processing benefit?
- After selecting the lawful basis, is this the same as the lawful basis the data subject would expect?
- What is the impact of the processing on the individual?
- Are you in a position of power over them?
- Are they a vulnerable person?
- Would they be likely to object to the processing?
- Are you able to stop the processing at any time on request, and have you factored in how to do this?

9.4.3 BSPTC will also ensure that individuals whose data is being processed by us are informed of the lawful basis for processing their data, as well as the intended purpose. This should occur via a privacy notice. This applies whether we have collected the data directly from the individual, or from another source.

9.4.4 If you are responsible for making an assessment of the lawful basis and implementing the privacy notice for the processing activity, this will be approved by the DPO.

10. Special categories of personal data

10.1 Previously known as sensitive personal data, this means data about an individual which is more sensitive, so requires more protection. This type of data could create more significant risks to a person's fundamental rights and freedoms, for example by putting them at risk of unlawful discrimination. The special categories include information about an individual's:

- race
- ethnic origin
- politics
- religion
- trade union membership
- genetics
- biometrics (where used for ID purposes)
- health
- sexual orientation

10.2 In most cases where BSPTC process special categories of personal data we will require the data subject's explicit consent to do this unless exceptional circumstances apply or we are required to do this by law (e.g. to comply with legal obligations to ensure health and safety at work). Any such consent will need to clearly identify what the relevant data is, why it is being processed and to whom it will be disclosed.

10.3 The condition for processing special categories of personal data will comply with the law. BSPTC will not undertake any processing of special categories of data if there is no legal basis to do so.

11. Accuracy and relevance

11.1 BSPTC will ensure that any personal data we process is accurate, adequate, relevant and not excessive, given the purpose for which it was obtained. We will not process personal data obtained for one purpose for any unconnected purpose unless the individual concerned has agreed to this or would otherwise reasonably expect this.

11.2 Individuals may ask that we correct inaccurate personal data relating to them. If you believe that information is inaccurate you should record the fact that the accuracy of the information is disputed and inform the DPO.

12. Data, retention, security and storage

12.1 BSPTC will only store data when necessary. BSPTC will undertake the following storage policy:

- All financial data not relevant to current working practices will be shredded and or destroyed after 10 years.
- Documents which contain personal data will be shredded and or destroyed after 5 years, unless the content is paramount to the future running of the business. Personal data is defined as anything that includes names, addresses, email addresses or another personal identification.

12.2 If the content of the data is seen to be relevant to the business and or working practices and needs to be retained, BSPTC will comply with the following data storage practices:

- In cases when data is stored on printed paper, it will be kept in a secure place where unauthorised personnel cannot access it
- Printed data will be shredded when it is no longer needed
- Data stored on a computer will be protected by strong passwords that are changed regularly.
- Data stored on CDs or memory sticks will be encrypted or password protected and locked away securely when not being used
- The DPO will approve any cloud used to store data
- Servers containing personal data will be kept in a secure location, away from general office space
- Data will be regularly backed up in line with the company's backup procedures
- Data will never be saved directly to mobile devices such as laptops, tablets or smartphones
- All servers containing sensitive data will be approved and protected by security software
- All possible technical measures will be put in place to keep data secure

12.3 Broadstairs and St. Peter's Town Council holds an extensive archive of paper documentation. Therefore, it is important that the Town Council has an annual 'house-keeping' event to ensure that only relevant paper copies are kept. This event should be undertaken during the months of January to March each year.

12..4 BSPTC will keep personal data secure against loss or misuse. Where other organisations process personal data as a service on our behalf, the DPO will establish what, if any, additional specific data security arrangements need to be implemented in contracts with those third party organisations.

13. Rights of individuals

Individuals have rights to their data which we will respect and comply with to the best of our ability. BSPTC will ensure individuals can exercise their rights in the following ways:

13.1. Right to be informed

- Providing privacy notices which are concise, transparent, intelligible and easily accessible, free of charge, that are written in clear and plain language, particularly if aimed at children.
- Keeping a record of how we use personal data to demonstrate compliance with the need for accountability and transparency.

13.2. Right of access

- Enabling individuals to access their personal data and supplementary information
- Allowing individuals to be aware of and verify the lawfulness of the processing activities

13.3. Right to rectification

- We will rectify or amend the personal data of the individual if requested because it is inaccurate or incomplete.
- This will be done without delay, and no later than one month. This can be extended to two months with permission from the DPO.

13.4. Right to erasure

- We will delete or remove an individual's data if requested and there is no compelling reason for its continued processing.

13.5. Right to restrict processing

- We will comply with any request to restrict, block, or otherwise suppress the processing of personal data.
- We are permitted to store personal data if it has been restricted, but not process it further. We will retain enough data to ensure the right to restriction is respected in the future.

13.6 Right to data portability

- We will provide individuals with their data so that they can reuse it for their own purposes or across different services.
- We will provide it in a commonly used, machine-readable format, and send it directly to another controller if requested.
- Right to object
- We will respect the right of an individual to object to data processing based on legitimate interest or the performance of a public interest task.
- We will respect the right of an individual to object to direct marketing, including profiling.
- We will respect the right of an individual to object to processing their data for scientific and historical research and statistics.
- Rights in relation to automated decision making and profiling
- We will respect the rights of individuals in relation to automated decision making and profiling.
- Individuals retain their right to object to such automated processing, have the rationale explained to them, and request human intervention.

14. Privacy notices

14.1 Privacy notices will be concise, transparent, intelligible and easily accessible and will comply with the requirement of the Information Commissioners Officer ICO.

15. Subject Access Requests and Data potability requests

15.1 BSPTC will provide an individual with a copy of the information they request, free of charge. This will occur within one month of receipt. We endeavour to provide data subjects access to their information in commonly used electronic formats, and where possible, provide direct access to the information through a remote accessed secure system.

15.2 If complying with the request is complex or numerous, the deadline can be extended by two months, but the individual will be informed within one month. You will obtain approval from the DPO before extending the deadline.

15.3 BSPTC can refuse to respond to certain requests, and can, in circumstances of the request being manifestly unfounded or excessive, charge a fee. If the request is for a large quantity of data, we can request the individual specify the information they are requesting. This can only be done with express permission from the DPO.

15.4 Once a subject access request has been made, BSPTC will not change or amend any of the data that has been requested. Doing so is a criminal offence.

16. Right to erasure

16.1 BSPTC will erase any data relating to an individual if the individual requests the Town Council to do so.

17. The right to object

17.1 Individuals have the right to object to their data being used on grounds relating to their particular situation. BSPTC will cease processing unless:

- We have legitimate grounds for processing which override the interests, rights and freedoms of the individual.
- The processing relates to the establishment, exercise or defence of legal claims.

17.2 BSPTC will always inform the individual of their right to object at the first point of communication, i.e. in the privacy notice.

18. Using Third parties

18.1 As a [data controller (and/or) data processor], we will have written contracts in place with any third party [data controllers (and/or) data processors] that we use. The contract will contain specific clauses which set out our and their liabilities, obligations and responsibilities.

18.2 [For controllers] As a data controller, we will only appoint processors who can provide sufficient guarantees under GDPR and that the rights of data subjects will be respected and protected.

18.3 [For processors] As a data processor, we will only act on the documented instructions of a controller. We acknowledge our responsibilities as a data processor under GDPR and we will protect and respect the rights of data subjects.

19. Audits, training, reporting

19.1 Data audits- Regular data audits to manage and mitigate risks will inform the data register. This contains information on what data is held, where it is stored, how it is used, who is responsible and any further regulations or retention timescales that may be relevant. You will conduct a regular data audit as defined by the DPO and normal procedures.

19.2 Staff Training- All BSPTC staff will receive adequate training on provisions of data protection law specific for their role.

19.3 Reporting breaches- Any breach of this policy or of data protection laws will be reported as soon as practically possible. This means as soon as you have become aware of a breach. BSPTC has a legal obligation to report any data breaches to the DPO within 72 hours.

20. Monitoring and Review

20.1 The Town Clerk will keep the monitoring of this policy under review and will report any changes required to the Finance & General Purposes Committee.