Seaton Town Council Constitution

Chapter 9

Data Protection Policy

Marshlands Centre, Harbour Road, Seaton EX12 2LT

01297 21388

townclerk@seaton.gov.uk

Data Protection Policy

1.0 Introduction

1.1 This policy applies to the collection and processing of all personal data by the Council, the sharing of information between the Council and other parties and how we will act when using third parties who may process personal data on our behalf. It covers both papers and electronic records and covers both manual and automated filing systems. The policy applies to all employees (including temporary staff), Councillors and all people or organisations acting on our behalf.

2.0 Data Protection Principles

2.1 Seaton Town Council will, by putting in place appropriate policies and procedures, be responsible for ensuring that an individual's personal data is;

- Processed lawfully, fairly and in a transparent manner;
- Collected for specified, explicit and legitimate purposes and not further processed in a manner incompatible with those purposes;
- Adequate, relevant and limited to what is necessary in relation to the purposes for which it is processed;
- Accurate and kept up to date (where necessary) and every reasonable step taken to ensure that inaccurate personal data (having regard to purposes for which it is processed) is erased or rectified without delay;
- Kept in a form which permits identification for no longer than is necessary for the purpose for which it is being processed; and
- Processed with appropriate security which will include protection against unauthorised or unlawful processing and against accidental loss, destruction / damage using appropriate technical or organisational measures.

2.2 In addition we will, through this policy and other measures, ensure that we are accountable in that we can demonstrate compliance with the responsibilities detailed above.

3.0 Definitions

3.1 ***Personal data*** is information about a living individual which is capable of identifying that individual e.g. name, email address or photo

3.2 ***Sensitive Personal Data*** is also described in the GDPR as 'special categories of data' and is the following types of personal data about a data subject: racial or ethnic origin; political opinions; religious beliefs; trade union membership; physical or mental health condition; sexual life or orientation; genetic data; biometric data

3.3 ***Data subject*** – is the person about whom personal data is processed

3.4 ***Data Controller*** is the person or organisation who determines the how and what of data processing

3.5 ***Data Processor*** is the person or firm that processes the data on behalf of the controller

3.6 ***Data Protection Officer (DPO)*** is the person who will monitor internal compliance with the Regulations

3.7 ***Consent*** is a positive, active, unambiguous confirmation of a data subjects agreement to have their data processed for a particular purpose. Consent must be easy to withdraw and must be freely given, provided on an opt-in basis rather than opt-out.

3.8 ***Processing*** is anything done with/to personal data (obtaining, recording, adapting or holding/storing) personal data.

3.9 ***Privacy Notice*** is a notice from a data controller to a data subject describing how personal data will be used and what rights the data subject has.

4.0 The rights of individuals

4.1 Seaton Town Council recognises that an individual has rights in relation to the way it obtains and processes their personal data. Accordingly, and as part of our responsibilities detailed above, the Council will ensure that an individual is able to exercise them where permitted.

4.2 Individuals have the right to be provided with information about how the Council will process their personal data. The information to be provided varies depending on whether the personal data is obtained from the individual or from a third party. The Council will generally satisfy this requirement through the use of privacy notices. The Council will ensure that the information provided is concise, transparent, intelligible and easily accessible and written in clear and plain language.

4.3 In addition the Council will ensure that individuals are able to exercise the following rights (where permitted);

- Right of access
- Right to rectification
- Right to erasure
- Right to restriction of processing
- Right to data portability
- Right to object
- Rights in relation to automated decision-making (including profiling)

4.4 Detail in relation to each of the above rights and the processes / procedures for exercising them will be clearly detailed on our website

www.seaton.gov.uk and we will treat any request to exercise the rights in accordance with the legal requirements and the specific detail below

5.0 Purpose and Processing

5.1 The Council will only collect information that is necessary for what it does by ensuring that there is a specific, explicit and legitimate purpose to be doing so. We will endeavour to ensure that information about individuals is accurately recorded when we collect it and up to date when we use it and that only the minimum necessary personal information is used to assist in the performance of its functions.

5.2 We will ensure that there is at least one lawful basis for processing an individual's personal data. Given what we do, on the whole this will be because the processing is necessary to comply with a legal obligation or because we are performing a task in the public interest / in the exercise of official authority.

5.3 We will make sure that the purpose for processing and the lawful basis are properly recorded and provided to individuals, generally through our website and in other formats on request.

5.4 We may carry out further processing provided it is not incompatible with the original purpose for which we collected the personal data. This would include processing for purposes in the public interest or statistical purposes.

6.0 Special categories of information

6.1 Certain personal data is particularly sensitive (this covers information relating to race, religious belief, political opinion, health information, sexual orientation, trade union membership and (where processed to uniquely identify an individual) genetic and biometric data). We are not permitted to process this type of information unless one of the special conditions are met. By way of examples, the special conditions include situations where an individual gives their consent to the processing or an individual cannot give consent but processing is necessary to protect their vital interests.

6.2 We will ensure that we do not process special categories of information without one of the special conditions being met.

7.0 Data Security

7.1 In order to ensure the security of personal data, we will ensure we have appropriate physical, technical and organisational security measures in place. We will process personal data in accordance with our Information Security Policy, which our employees are required to comply with.

7.2 These measures will keep an individual's information secure and will

protect it against unauthorised use, damage, loss and theft.

8.0 Data sharing

8.1 We are permitted in appropriate circumstances to share data within the organisation and also with external bodies. This is most likely to occur when we are required to comply with legal requirements including prevention or detection of crime, preventing fraud and carrying out our other regulatory functions. For instance, it would be acceptable to share data between services if we had good reasons to believe that fraudulent activity was taking place or if we had reason to believe that a crime had been (or was going to be) committed.

8.2 We will only share personal data internally or externally where we are permitted to do so and individuals will be made aware the circumstances in which this will occur through privacy notices. Any new system access requests from staff or services within the Council will be considered by the Data Protection Officer.

8.3 We will use any relevant codes of practice on data sharing issued by the Information Commissioner to help with implementing these aims.

8.4 Where we obtain personal data from a third party rather than directly from an individual, we will, wherever possible, make sure they know that we have done this.

9.0 Third Party processing

9.1 We do on occasion ask external agencies or companies to carry out processing of personal data on our behalf. While such bodies are now also subject to detailed requirements regarding those processing activities, we are also under an obligation to ensure that those third parties are able to provide sufficient guarantees that their processing complies with legal requirements and protects the rights of an individual.

9.2 We will therefore ensure that there is a contract in place with any third party processors which complies with the legal requirements governing how a third party carries out the processing on our behalf.

9.3 We will endeavour to use only those third party processors who have signed up to and adhere to any relevant code of practice relevant to the processing activities they will be carrying out.

9.4 All contracts with third parties for the processing of personal data will be reviewed by the Data Protection Officer to ensure it meets the relevant requirements.

10.0 Privacy by design and data protection impact assessments

10.1 We will ensure that an individual's rights in relation to privacy and data

protection are a key consideration in the formulation and early stages of production of any project, process or policy as well as seeking to integrate them into existing project management and risk management policies. Privacy and data protection will remain relevant throughout the lifecycle of any project, process or policy.

10.2 Having regard to certain factors, including the nature, scope, context and purposes of processing and related costs, we will implement appropriate technical and organisational measures to ensure we have integrated privacy and data protection into our processing activities.

10.3 When formulating a project, process or policy we will consider the impact this will have on our data protection obligations and how we will meet individuals' expectations of privacy. To formally document this we will complete a data protection impact assessment

11.0 Transparency

11.1 We are under obligations to provide individuals with certain information regarding how we will use their personal data and their rights. The information to be provided varies depending on whether we have obtained the information directly from an individual or from a third party. The information provided should be concise, transparent and intelligible. We will comply with our obligations primarily through the use of Privacy Notices (which are on our website) or by directly contacting the individual concerned, in either case using clear and plain language.

11.2 In addition, we are also under an obligation to keep records of our processing activities and information relating to it so that we are able to demonstrate to the Information Commissioner that we are complying with our obligations overall. We will ensure that we maintain the records as required.

12.0 Document retention

12.1 We will hold information about individuals for as long as is necessary and, subject to any statutory retention periods, we will ensure that the information is disposed of in a secure and proper manner when it is no longer needed.

12.2 It is important that we understand what documents to keep and for how long and that we don't keep unnecessary documentation nor keep documentation for longer than is necessary. This is not only from the data protection point of view but also good administration (in the sense of resources for keeping documentation, whether electronic or manual files).

12.3 Any decision taken in respect of the retention / disposal of documents will be taken in accordance with the Council's Document Retention Scheme.

12.4 We will ensure that when disposing of papers which may contain personal or confidential data, we will destroy or dispose of them by shredding them on-site (with a cross cutting device). Employees shall not dispose of personal or confidential papers in normal refuse or recycling bins.

12.5 Disposal of computer equipment / electronic media are outside the scope of this policy and will be covered in a separate policy.

13.0 Data subject's rights

13.1 We recognise the importance of individuals being able to exercise the fundamental rights available to them in respect of their personal data. These rights are identified in section 4.3 above. We will ensure that all requests from individuals to exercise their rights are dealt with as quickly as possible and in any event within one month of receipt unless we consider it necessary, due to the complexity or number of requests, to extend the time period by two months. Any extension of time will be notified to the individual within one month of the receipt of the request.

13.2 The exercise of an individuals rights will be provided free of charge unless, in our view, requests are manifestly unfounded or excessive (including where this is due to repeat requests) in which case we may choose to either charge a fee for providing the information / taking the action requested or to refuse to act on the request. Additional copies of information already provided may be subject to a reasonable charge at our discretion.

13.3 Where there is an exemption which would permit us not to progress any request or which may limit the application of any right, we will normally apply the exemption unless it is appropriate or reasonable not to do so and, in any event, will always do so in circumstances where it is deemed necessary to the effective operation of our tasks, for the prevention and detection of crime, to protect an individual or is required by law.

13.4 Where we are not confident of the identity of an individual making a request we may ask for information (or additional information) in order to confirm the identity before progressing their request to exercise their rights.

13.5 The Council will inform individuals of its decisions in respect of any requests and any further rights there may be in terms of lodging a complaint with the Information Commissioner and / or seeking remedy through the Courts.

14.0 Breach reporting

14.1 A personal data breach occurs when (whether deliberate or accidental) there is a breach of security leading to the accidental or unlawful

destruction, loss, alteration, unauthorised disclosure of, or access to, personal data. In broad terms this means a security incident that has affected the confidentiality, integrity or availability of personal data.

14.2 We will implement a process to ensure all staff handling personal data know when and how to report any actual or suspected data breach(es) and we will also provide a process for breach reporting by an individual and any third party processors that we may use.

14.3 The Data Protection Officer will deal with the reports of any breaches and where appropriate we will take steps to deal with the breach including measures to mitigate any adverse impacts.

14.4 Where a breach results in a risk to an individual's rights and freedoms we will ensure the breach is appropriately reported to the Information Commissioner and / or the individual(s) concerned in accordance with the legal requirements and prescribed timeframes.

14.5 Individuals also have the right to progress a complaint under the Council's complaints procedure.

15.0 Training

15.1 Data protection training is crucial so that all staff understand their responsibilities relating to data protection and the use of personal data. Failure to comply with the data protection principles and our legal obligations could lead to serious problems and result in the rights and freedoms of an individual being adversely affected. This could lead to significant fines or criminal prosecution.

15.2 It is therefore our policy that all individuals handling personal data will be trained to an appropriate level in the use and control of personal data. Training will be given to all staff on a periodic basis (at least annually) to refresh existing staff and educate new staff. In addition to this training the Data Protection Officer will undertake further data protection training where appropriate to ensure that they are up to date with legislative requirements and best practice.

15.3 Councillors will be furnished with a copy of this Policy and all future Councillors will receive a copy as part of their induction pack. Awareness sessions for Councillors will take place at least annually.

16.0 Who is responsible for delivery?

16.1 The Data Protection Officer will be accountable for ensuring compliance with our legal requirements. Further details about the role of the Data Protection Officer are appended to this document as Annex 1.

16.2 The Data Protection Officer will ensure that this policy is followed by the Council and that there is an appropriate training programme for staff and

Councillors.

16.3 All staff are also responsible for ensuring compliance - the commitment of all Councillors and staff is essential to make this policy work. Employees should check with the Data Protection Officer if they are unsure about their responsibilities or the handling of an individual's personal data, particular if it relates to disclosing such information.

16.4 All members of staff are expected to comply with our other policies relating to the management and security of information, including personal data, and to follow any good practice guidance that we issue.

17.0 Disciplinary action and criminal offences

17.1 Where an employee breaches this Policy and where caused by deliberate, negligent or reckless behaviour then the normal consequence will be an appropriate disciplinary sanction (which could include dismissal) and may even give rise to criminal offences.

17.2 The person concerned may also become liable for any financial consequences resulting from a breach of the Policy.

18.0 Related Legislation, Policies and Strategies

- General Data Protection Regulations 2016 / Data Protection [Act 2018]
- Freedom of Information Act 2000
- Human Rights Act 1998
- Environmental Information Regulations 2004
- Local Government (Access to Information) Act 1985
- Equality Act 2010
- Data sharing code of practice (Information Commissioner's Office)
- The Council's Complaints Procedure
- Information Security Policy

Annex One

The role of Data Protection Officers (taken from the NALC guidance)

1. What does a Data Protection Officer do?

(a) The GDPR sets out in detail the minimum responsibilities of the Data Protection Officer ("DPO") role. GDPR specifies that DPOs "should assist the controller or the processor to monitor internal compliance with this Regulation".

(b) A DPO's duties include:

(i) informing and advising the council and its staff of their obligations in the GDPR and other data protection laws;

(ii) monitoring compliance of the council, both its practices and policies, with the GDPR and other data protection laws;

(iii) raising awareness of data protection law; providing relevant training to staff and councillors;

(iv) carrying out data protection-related audits;

(v) providing advice to the council, where requested, in relation to the carrying out of data protection impact assessments ('DPIAs') and the council's wider obligations with regard to DPIAs; and

(vi) acting as a contact point for the Information Commissioner's Office.

(c) As part of these duties to monitor compliance, DPOs may, in particular:

(i) collect information to identify processing activities;

(ii) analyse and check the compliance of processing activities; and

(iii) inform, advise and issue recommendations to the controller or the processor

(d) Monitoring of compliance does not mean that it is the DPO is personally responsible where there is an instance of non-compliance. The GDPR makes it clear that it is the controller, not the DPO, who is required to 'implement appropriate technical and organisational measures to ensure and to be able to demonstrate that processing is performed in accordance with this Regulation.'

(e) The appointed DPO must at all times have regard to 'the risk associated with the processing operations, taking into account the nature, scope, context and purposes of processing.' This is an overarching obligation which means that the role of the DPO will vary in proportion to the risks to the rights of individuals affected by the council's processing of personal data.

(f) The DPO should 'cooperate with the supervisory authority'(in the UK, this is the Information Commissioners Office ("ICO") and 'act as a contact point for the supervisory authority on issues relating to processing, and to consult, where appropriate, with regard to any other matter'.

(g) It is the controller or the processor, not the DPO, who is required to 'maintain a record of processing operations under its responsibility' or

'maintain a record of all categories of processing activities carried out on behalf of a controller'.

2. DPOs and DPIAs

(a) A data controller (and not the DPO) is required to carry out a data protection impact assessment ('DPIA') under the GDPR in certain circumstances.

(b) The controller must 'seek advice' from the DPO when carrying out a DPIA. DPOs have the duty to 'provide advice where requested as regards the DPIA and monitor its performance'.

(c) It is recommended that controllers should seek the advice of the DPO on the following issues:

(i) Whether or not to carry out a DPIA;

(ii) What methodology to follow when carrying out a DPIA;

(iii) 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; and

(iv) 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.

(d) If the controller 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.

3. Data controllers and processors should ensure that:

(a) The DPO is invited to participate regularly in meetings of senior and middle management. For councils, this would include meetings of full council and relevant committee meetings.

(b) The DPO's name and contact details are provided to ICO;

(c) The DPO should be available to advise/ support councillors and relevant staff on data protection issues;

(d) The DPO is present when decisions with data protection implications are taken;

(e) All relevant information must be passed on to the DPO in a timely manner in order to allow him or her to provide adequate advice;

(f) The opinion of the DPO must always be given due weight. In case of disagreement it is good practice to document the reasons for not following the DPO's advice;

(g) The DPO should be promptly consulted once a data breach or another incident has occurred. This is good practice since the DPO will often have been involved in implementing data protection polices such as breach reporting and it will be important for the DPO to assess whether the policies work operationally.

4. Role Checklist

- ☐ Raising data protection awareness within the council, and advising on GDPR compliance;
- ☐ Ensuring the implementation of the appropriate documentation to demonstrate GDPR compliance;

- ☐ Monitoring the implementation and compliance with policies, procedures and GDPR in general;
- ☐ Involvement in council's handling of data breaches, including assisting and advising the council with its notification to the ICO and data subjects where necessary (but it is the council which has the obligation to notify in certain circumstances not the DPO);
- ☐ Liaising with the ICO, the relevant councillors and staff and with the data subjects;
- ☐ Monitoring Data Protection Impact Assessments;
- ☐ Cooperating with and acting as the contact point for the ICO on issues relating to processing

Adopted – May 2018