A great place to live, work & play

SCARBOROUGH BOROUGH COUNCIL

DATA PROTECTION POLICY

DOCUMENT CONTROL

Author	Petra Jackson
Owner	Data Protection Officer
Protective Marking	NA
Review Date	28/10/20

Revision History

Date	Revised By	Version	Description of Revision
2014	David Kitson	0.1	Creation of Policy
22/5/ 2018	David Kitson	1.0	Revision of Policy to reflect GDPR
28/10/19	Petra Jackson		

Document Approvals

Approval	Name	Date
Cabinet	Chairperson	8 April 2014
Council	Chairperson	12 May 2014

1. Introduction

1.1 In carrying out its day to day business and duties, the Council processes significant amounts of information concerning individuals.

1.2 The General Data Protection Regulation (GDPR) and the Data Protection Act 2018 (DPA) place various duties and responsibilities on the Council when processing personal information. The GDPR and the DPA also create legal rights for individuals in respect of personal information held and processed by the Council.

1.3 This Policy sets out the Council's overarching approach to ensuring compliance with the GDPR and the DPA, and other corresponding legislation.

1.4 A breach of this policy may result in disciplinary proceedings leading to dismissal. It may also amount to a criminal offence and/or lead to civil action for compensation.

2. What is Personal Data?

2.1 Under the GDPR and the DPA 'personal data' is defined as any information relating to an identified or identifiable natural person ('data subject').

2.2 An identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

2.3 It covers all personal information regardless of how it is held, whether electronically (such as in an e-mail) or manually (such as in a hand written file note).

2.4 In the context of the GDPR and the DPA, the word 'processing' means any operation or set of operations which is performed on personal data or on sets of 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. Commitment

3.1 The Council is committed to

- protecting the privacy of individuals and their personal data;
- respecting the rights of individuals;

- complying with the GDPR, the DPA and any other relevant legislation;

- ensuring that Officers, Members and any other relevant persons receive appropriate training and support to ensure a consistent approach across the organisation.

3.2 The Council regard the lawful, fair and transparent treatment of personal information as being critical to successful operations and to maintaining confidence between the Council, its customers and third parties.

4. Data Protection Principles

4.1 The Council will ensure that appropriate management, controls and procedures are in place to enable compliance with the data protection principles when processing personal information. The principles are:

1. **Lawfulness, fairness and transparency** - Personal data shall be processed lawfully, fairly and in a transparent manner in relation to the data subject;

2. **Purpose limitation** - Personal data shall be collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes;

3. **Data minimisation** - Personal data shall be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed;

4. **Accuracy** - Personal data shall be accurate and, where necessary, kept up to date;

5. **Storage limitation** - Personal data shall be 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;

6. **Integrity and confidentiality** - Personal data shall be 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;

5. Roles and Responsibilities

5.1 This Policy applies to the activities of all Officers, Members, contractors, agents, volunteers and any other party when processing information on the Council's behalf. Compliance with this policy, the GDPR, the DPA and any other relevant legislation is mandatory.

5.2 The Council will ensure that a Data Protection Officer (DPO) is appointed who shall in the performance of his or her tasks have due regard to the risk associated with processing operations, taking into account the nature, scope, context and purposes of processing, and who has the following tasks:

5.2.1 informing and advising the Council and Officers who carry out processing of their obligations pursuant to the GDPR and the DPA;

5.2.2 monitoring compliance with the GDPR, the DPA, and with the policies of the Council in relation to the protection of personal data, including the assignment of responsibilities, awareness and training of Officers involved in processing operations, and the related audits;

5.2.3 providing advice where requested in regards to data privacy impact assessments (DPIA) and monitoring their performance;

5.2.4 co-operating with the Information Commissioner's Office (ICO);

5.2.5 co-ordinating the investigation of any reported breaches of the GDPR and the DPA, and determining any actions to be taken (including but not limited to notification of breach to the ICO, and those who are affected by the breach).

5.2.6 acting as the contact point for the ICO on issues relating to processing, including the prior consultation in relation to a DPIA which has indicated that the processing to which it relates would result in a high risk in the absence of measures taken by the controller to mitigate the risk, and to consult, where appropriate, with regard to any other matter; and

5.2.7 reviewing and updating this policy and any relevant procedures when necessary.

5.3 The Council will ensure that a Senior Information Risk Owner (SIRO) is appointed who:

5.3.1 has overall responsibility for establishing an effective information governance framework; and

5.3.2 has overall responsibility for ensuring compliance with the Council's information governance policies and standards.

5.4 The Directors are responsible for:

5.4.1 developing a data protection culture within the Council;

5.4.2 ensuring that this policy and any relevant procedures are implemented within their respective service areas;

5.4.3 ensuring that the Council complies with its legal duties and responsibilities under the GDPR and the DPA;

5.4.4 ensuring that the DPO is involved, properly and in a timely manner, in all issues which relate to the protection of personal data;

5.4.5 supporting the DPO in performing their tasks by providing resources necessary to carry out those tasks and access to personal data and processing operations, and to maintain his or her expert knowledge;

5.4.6 ensuring that the DPO does not receive any instructions regarding the exercise of their tasks, and that he or she shall not be dismissed or penalised by the Council for performing their tasks;

5.4.7 developing the data protection culture across the Council; and

5.4.8 demonstrating the Council's commitment set out in section 3.1 of this policy.

5.5 Service Unit Managers are responsible for:

5.5.1 developing, implementing and operating service specific procedures to comply with this policy and the required standards;

5.5.2 ensuring that Officers (including contractors, consultants, agents and volunteers) who process personal information on behalf of the Council do so in accordance with this policy, the GDPR, the DPA and any other relevant procedures;

5.5.3 ensuring that appropriate resources are in place to enable compliance; and

5.5.4 ensuring that this policy and any relevant procedures are communicated appropriately.

5.6 All individuals undertaking the processing of personal information on behalf of the Council are personally responsible for complying with this policy, the GDPR, the DPA and any other relevant procedures.

6. Training

6.1 The Council will ensure that appropriate data protection;

6.1.1 training is available to all Officers and Members (at induction and on an ongoing basis); and

6.1.2 support and guidance is available.

7. Breach Procedure

7.1 The Council will maintain a clear procedure which must be followed for reporting any breach of the GDPR and the DPA.

7.2 The procedure should also contain a clear breach management section which should cover the following important elements:

7.2.1 Containment and recovery;

7.2.2 Assessment of ongoing risk;

7.2.3 Notification of breach (to the ICO and/or the individual/organisations); and

7.2.4 Evaluation and response.

7.3 The Council's DPO is responsible for overseeing the breach procedure, and should establish a team of appropriate Officers to assist with the breach management process.

8. Monitoring of Compliance

8.1 Compliance with this policy, any procedures made pursuant to it, and the GDPR and the DPA will be subject to monitoring through the Council's audit function and reported to the Audit Committee where appropriate.

8.2 A failure to comply with this policy, any relevant procedure or the underlying statutory framework will be taken seriously and may result in disciplinary proceedings (which may lead to dismissal). This is in addition to any criminal or civil proceedings (brought by the Council or third parties) which may also be considered in the circumstances.