HELSTON TOWN COUNCIL

DATA PROTECTION POLICY

Reviewed: 3rd May 2018

1.0 Introduction

1.1 An essential activity within the Council is the requirement to gather and process information about its employees and people in the community in order to operate effectively. This will be done in accordance with the General Data Protection Regulations (GDPR), and other related government legislation.

1.2 The Council, acting as custodians of personal data, recognises its moral duty to ensure that all such data is handled properly and confidentially at all times, irrespective of whether it is held on paper or by electronic means. This covers the following:-

- the obtaining of personal data;
- the storage and security of personal data;
- the use of personal data; and
- the disposal/destruction of personal data.

2.0 Aims and Scope of this Policy

2.1 This policy is intended to:-

- Ensure everyone is aware of their responsibility regarding the GDPR.
- Provide a list of definitions to assist in the understanding of the Regulations.
- Sets out the basic guidelines for employees.
- Provide information on the types of information held by the Council.

3.0 Definitions

To aid the understanding of this document and the provisions of the GDPR the following definitions are provided for assistance:-

3.1 **Data** is any writing, image, recording.

3.2 **Data Controller** means the Council as the organisation that determines how data is processed.

3.3 **Data Processor** is a person, or a firm, processing data for the Council.

3.4 **Data Subject** is the individual about whom personal data is held.

3.5 **Personal Data** means data about a living individual who can be identified from that information (or from that and other information in the possession of the data controller).

3.6 **Sensitive Personal Data** means personal data consisting of information as to:

- racial or ethnic origin of the data subject
- his/her political opinion
- his or her religious beliefs or other beliefs of a similar nature
- whether he or she is a member of a trade union
- his or her physical or mental health or condition
- his or her sexual life
- the commission or alleged commission by him or her of an offence

- any proceedings for any offence committed by him or her, the disposal of such proceedings or the sentence of any court in such proceedings.

3.7 **Processing** is very widely drawn and means obtaining, recording or holding the information or data or carrying out any operation or set of operations on the information or data including:

- organisation, adaptation or alteration
- retrieval, consultation or use
- disclosure
- destruction of the information or data.

3.8 **Relevant Filing System** means any data that is recorded as part of a manual filing system or with the intention that it should form part of a relevant filing system (e.g. "any set of information relating to individuals to the extent that, although the information is not processed by means of equipment operating automatically in response to instructions given for that purpose, the set is structured, either by reference to individuals or by reference to criteria relating to individuals, in such a way that specific information relating to a particular individual is readily accessible").

4.0 Principles

4.1 Below are the governing Principles relating to the collection, use, processing and disclosure of data, and the rights of data subjects to have access to personal data relating to themselves:

- Personal data shall be **processed fairly and lawfully**.
- Personal data shall be obtained only for **specified and lawful purposes**.
- Personal data shall be **adequate, relevant and not excessive**.
- Personal data shall be **accurate** and, where necessary, kept **up to date**.
- Personal data **shall not be kept for longer than necessary**.
- Personal data shall be processed **in accordance with the rights of the data subject** under this Act (this includes the rights of subjects to access the data and to correct it).
- Appropriate **technical and organisational measures** shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data (this relates to data security).
- Personal data **shall not be transferred to any other country** without adequate protection in situ.

These principles are required as the minimum standards of practice for any organisation with respect to personal data.

5.0 Policy

5.1 The Council supports the objectives of the GDPR. This policy is intended to maintain the confidentiality of personal data held or processed either on computer or in manual files and to increase the access given to individuals to information relating to them.

5.2 To ensure compliance with the GDPR, the Council will:

i) Acknowledge the rights of individuals to whom personal data relates, and ensure that these rights may be exercised in accordance with the Act;

ii) Ensure that both the collection and use of personal data is done fairly and lawfully;

iii) Ensure that personal data will only be obtained and processed for the purposes specified;

iv) Collect and process personal data on a need to know basis, ensuring that such data is fit for the purpose, is not excessive, and is disposed of at a time appropriate to its purpose;

v) Ensure that adequate steps are taken to ensure the accuracy and currency of data;

vi) Ensure that for all personal data, appropriate security measures are taken, both technically and organisationally, to protect against damage, loss or abuse;

vii) Ensure that the movement of personal data is done in a lawful way, both inside and outside the Council and that suitable safeguards exist at all times.

viii) All actions regarding data subject access requests will be logged. This audit trail will include details regarding the nature of the request, the steps taken to validate it, the information provided as well as any withheld, e.g. for legal reasons.

ix) Treat all employee data with respect and will not obtain or disclose unauthorised, inappropriate or excessive information about individuals.

x) Respond to any information requests under the GDPR within one calendar month.

xi) Provide details of exemptions if they apply to a specific request.

xii) Destroy or amend inaccurate information when it is brought to light.

xiii) Responses to subject access requests will not incur a charge.

5.3 **Amount of data to be held**

The Council will hold the minimum personal data necessary to enable it to perform its functions. The data will be erased once the need to hold it has passed. Every effort will be made to ensure that data is accurate and up-to-date, and that inaccuracies are corrected quickly.

5.4 **Employee Information**

5.4.1 Helston Town Council will need to keep information for purposes connected with an employee's employment, including recruitment and termination information. This information will be kept throughout the period of employment and for as long as is necessary following the termination of employment.

5.4.2 These records may include:

- Information gathered about an employee and any references obtained during recruitment
- Details of terms of employment
- Payroll, Income Tax, National Insurance and Superannuation information
- Performance information
- Details of grade and job duties
- Health records

- Absence records, including holiday records and self certification forms
- Details of any disciplinary investigations and proceedings
- Training records
- Contact names and addresses
- Correspondence with the Council and other information provided to the Council.

5.4.3 Any information held within the Council is kept in the strictest confidence. In addition, the Council operates a Confidential Reporting Policy which supports our aim that no employee should feel reluctant, for fear of management's response, to give information about any wrongdoing within the organisation.

5.5 **Subject Access**

The Council will provide to any individual who requests it, in a specified manner, a reply stating whether or not the Council holds personal data about that individual. A written copy, in clear language, of the current data held, will be given. A fee will not be levied for this service.

However, there are certain exemptions from the right of subject access, which relate largely to a test of prejudice. For example, personal data that is held for the purpose of the prevention or detection of crime is exempt, to the extent that providing access would be likely to prejudice that purpose. In addition, data may be withheld if it is not possible to release information without disclosure of personal data about other people.

5.6 **Disclosures**

Disclosures of information must be in accordance with the provisions of the Regulations and the Council's registration/notification. Where the Council has a duty to disclose certain data to public authorities (such as the Inland Revenue, Customs and Excise, Benefits Agency), this will be done in accordance with statutory and other requirements.

Legal and internal rules limit disclosure within the Authority either to Council officers or elected Members. When a request for information is made, the minimum of personal data will be made available on a need to know basis.

5.7 **System Design**

The Council intends that personal data must be treated as confidential. Computer systems will be designed to comply with the Principles of the GDPR so that access to personal data should be restricted to identifiable system users.

5.8 **Training**

It is the aim of the Council that all staff will be fully informed of their obligations under the GDPR and be aware of their personal liabilities, and where appropriate further training will be given.

5.9 **Disciplinary Action**

The Council expects all of its staff and Members to comply fully with this Policy and the Principles of the GDPR. Disciplinary action may be taken against any employee who breaches any of the instructions or procedures contained in this Policy.

6.0 Responsibilities

6.1 **All employees** have a duty to observe the Principles of the Regulations and the procedures referred to in this document.

6.2 **Individuals who do not handle data** as part of their normal work have a responsibility to ensure that any personal data they see or hear goes no further. This includes personal data and information extracted from such data, thus, for example, unauthorised disclosure of data might occur by passing information over the telephone, communicating information contained on a computer print-out or even inadvertently by reading a computer screen.

6.3 **The Town Clerk**

6.3.1 Ensures that any third party processing personal information on Helston Town Council's behalf is contractually obliged to put in place similar measures.

6.3.2 Has a responsibility to ensure that data subjects have appropriate access, upon written request, to details regarding personal information relating to them.

6.3.3 The Town Clerk is responsible for gathering and disseminating information and issues relating to information security, the GDPR and other related legislation and ensuring that all staff comply with the legislation.

7.0 Members

7.1 Members are bound by this Policy and must adhere to the guidelines.