Hurworth Parish Council
Data Protection Regulations
Procedure 32, dated 7th June 2018

1. Introduction

a) The General Data Protection Regulations (GDPR) came into effect on 25th May 2018. The New Regulations regulate the use of personal data relating to living data subjects. The purpose of Regulations are to regulate the way that personal information about living individuals, (no matter how that information is held) is obtained, stored, used and disclosed. The legislation grants rights to individuals, to see data stored about them and to require modification if the data are incorrect, and, in certain cases, to compensation. These provisions amount to a right of privacy for the individual.

b) The GDPR requires that all processing of personal data must be kept and used in accordance with the provisions of the Act. Hurworth Parish Council (the 'Council') is registered with the Information Commissioner as required by these regulations.

c) The purpose of this Policy Statement is to formalise the position of the Council and to state its commitment to maintaining the strictest level of confidentiality of personal data within its record system in accordance with the provisions of the Regulations.

2. Scope

a) The obligations contained in this policy apply equally to councillors and the employee of the Council.

b) The Council is the Data Controller and has the responsibility to administer the day to day compliance with the Regulations The Clerk will be responsible for processing data on behalf of the Council. Overall responsibility to ensure the Data Protection Policy is understood and enforced remains with the Council.

c) Disclosure of personal data within the Council to Councillors or officers will be on the basis of a need to know.

d) The Regulations apply to records held in a relevant filing system, which includes structured and, in the case of public bodies, unstructured files where personal data relating to an individual is readily accessible.

3. Definitions

a) **Personal Data** is any data that relates to a living individual who can be identified from that data. This includes any expression of opinion about the individual and any indication of the intentions of the Council in respect of the individual.

b) **Processing**, in relation to information or data, means obtaining, recording or holding information or data or carrying out any operation or set of operations on the information or data, including retrieval disclosure of that information or data.

c) **Data Subject** is an individual who is the subject of Personal data.

d) **Sensitive Personal Data** is defined in the Regulations defines by eight categories of information about the Data Subject relating to;

I. racial or ethnic origins
II. political opinions
III. religious or similar beliefs
IV. membership of a trade union
V. physical or mental health
VI. sexual life and orientation
VII. Genetic Data
VIII. Biometric Data (eg Facial Recognition, Finger Print Data)

e) **Data Protection Officer** is a person who, either alone or jointly with others, determines the purposes for which, and the manner in which, personal data is, or will be, processed. The Data Protection Officer for the Council is the Council Member appointed by the Council

f) **Person** relates to a legal person and thus includes a corporate body such as the Council.

g) **Information Commissioners Office (ICO)** is the organisation responsible for administering and enforcing the General Data Protection Regulations 2018 nationally.

h) General Data Protection Regulations has a number of underlying principles and the **six principles of data protection** are as follows;

I. Personal data must be processed lawfully, fairly and transparently
II. Personal data shall be used for a specific processing purpose that the data subject has been made aware of and no other, without further consent.
III. Personal should be adequate, relevant and limited i.e. only the minimum amount of data should be kept for specific processing.
IV. Personal data must be accurate and where necessary kept up to date.
V. Personal data should not be stored for longer than is necessary, and that storage is safe and secure
VI. Personal data should be processed in a manner that ensures appropriate security and protection.

4. Data Protection Policy

a) The Council will hold the minimum personal data necessary to enable it to perform its functions. The data will be deleted in accordance with the Records Management Policy of the Council. Every effort will be made to ensure that data is accurate and up to date, and that inaccuracies are corrected quickly.

b) The Council will design IT and manual systems to comply with the six principles of the General Data Protection Regulations. The Council ensures that personal data is treated as confidential, ensuring that access to personal data can be restricted to identifiable system users.

c) The Council is committed in its aim that its employee will be properly trained, fully informed of their obligations under the Regulations, and made aware of their personal liabilities. The Council

expects its employee and Councillors to comply fully with this Policy and the Data Protection Principles.

d) It is the duty of the Clerk acting on behalf of the Council in accordance with the written contract between the Council and the Data Processor (Clerk) to comply with the data protection principles and to ensure individuals are informed if their personal data is to be processed by way of a fair processing notice, unless an exemption applies.

e) The Council must fulfil a request for access to personal data within one calendar month. The Council will not to make a financial charge for this service.

f) The Council will provide to any individual who makes a written request for their personal data with;

   I. A reply stating whether or not we hold personal data about them.
   II. A copy of that information, in clear language, unless specific legal exemptions apply.

5. Third Party Disclosure / Requests for Data Sharing

As regards any request for Third Party Disclosure, the Council will determine such request in accordance with the principles set out in the "Data sharing Code of Practice" published and periodically updated by the Information Commissioner's Office (https://ico.org.uk/for-organisations/guide-to-data-protection,) applying as relevant the "Data sharing check lists" appearing at section 15 of the Code. A record will be kept of all third party disclosure requests which are received by the Council, which will include the decision made on the request and the reasons why such a decision was made.

6. Breaches of Data

The Council will nominate a person(s) to be responsible for recording and dealing with all data breaches which may arise, outline a response plan and setting out procedures to be followed. The responsible person shall notify the ICO of any data breach that meets the reporting criteria, within the prescribed timescale set out in the regulations.