GRAIG COMMUNITY COUNCIL
Data Protection (GDPR) Policy

1. Introduction

1.1 General Data Protection Regulation ("GDPR") will take effect in the UK from 25 May 2018. It replaces the existing law on data protection (the Data Protection Act 2000) and gives individuals more rights and protection regarding how their personal data is used by councils. Local councils and parish meetings must comply with its requirements, just like any other organisation.

1.2 The purpose of this policy is to formalise the position of the Council and state its commitment to maintaining confidentiality of personal information within its record systems. Detailed guidelines are attached as an appendix.

2. Scope

2.1 The obligations contained in this Policy Statement apply equally to both Council Members and Employees.

3. Definitions

3.1 ***Personal Data:*** 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.

3.2 ***Processing:*** processing information or data means obtaining, recording or holding the information or data or carrying out set operations on it, including disclosure.

3.3 ***Data Subject:*** an individual who is the subject of personal data.

4. Policy

4.1 Graig Community Council is committed to maintaining the strictest level of confidentiality for any personal data it is responsible for processing. The Council will only process or disclose Personal data for purposes necessary for official Council business and that notified to the Data Protection Commissioner. The Council will adhere to the principles outlined in the General Data Protection Regulation 2018 for processing that data.

4.2 We will design computer and manual systems to comply with the principles of the GDPR and will train staff involved in processing personal data accordingly. The six principles are:

Personal data must be:

- Processed fairly, lawfully and in a transparent manner in relation to the data subject.
- Collected for specific, explicit and legitimate purposes and not be further processed in a manner that is incompatible with those purposes.
- Adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed.
- Accurate and, where necessary, kept up to date.
- Kept in a format that permits identification of data subjects for no longer than

is necessary for the purposes for which the personal data are processed.

- 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 (Article 5).

4.3 The Council carries out its affairs in an open manner. Apart from exceptional circumstances as outlined in the Act, we will make information about a data subject available to them, upon request, in an intelligible form.

4.4 Where a data subject asks the Council for access to data, the request will be free of charge and dealt with within one month.

4.5 The Council will try to hold only the minimum data necessary to perform its business, and will erase or destroy the data in such a manner that confidentiality is maintained. We will try to ensure that data is accurate and up to date, and correct inaccuracies without unnecessary delay.

GDPR POLICY GUIDELINES

1. Introduction

1.1. These guidance notes expand on some of the information in the Council's GDPR Policy, and the two documents should be used together.
1.2. The previous Acts covered data that was "processed by means of equipment operating automatically in response to instructions given for that purpose", i.e. personal data held on computer systems. This was widened to include "relevant filing systems" or manual data. Relevant filing systems are "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".
1.3. The current GDPR reinforces the principles of confidentiality for personal data.
1.4. Note - this only covers information that relates to living individuals.

2. Responsibilities

2.1. The Data Protection Officer will notify the Office of the Data Protection Commissioner of the systems in use and their stated purpose.
2.2. New "systems", new uses or changes to "systems" will be notified to the Office of the Data Protection Commissioner before the changes are implemented.
2.3. The Council is responsible for ensuring that notifications are up to date and renewals are effectively processed.
2.4. Every Member and employee of the Council is responsible for keeping to the GRPR guidelines when processing personal data.

3. System Contents

3.1. Only the minimum data necessary to carry out a function will be held. The information held must be relevant to the purpose. For example some systems allow users to make notes, and these facilities must not be used to record remarks that have no bearing on the

purpose of the system, especially if such comments are derogatory or they cannot be substantiated.

3.2. Information can be irrelevant if it is held for too long. Information must be both accurate and current. Inaccurate or out of date records must be amended without undue delay.

4. General Access to Personal Data

4.1. When information is gathered either in writing or verbally it is essential that the data subject is told what the information will be used for and to whom else the information may be disclosed. That information cannot then be used for any other purpose or disclosed to any other individual.

4.2. Information must only be provided to the person to whom it relates unless prior consent is obtained. If information identifies someone else who has not consented to their details being disclosed, any details identifying the third party must be removed before releasing any information.

4.3. There is an obvious risk that others may attempt to obtain confidential information relating to someone else. Awareness is particularly important where requests are made over the telephone or if the correspondence address is different from that held on any Council system. Checks must be made to verify the identity of the individual by telephoning the individual back, asking them to confirm something personal such as their account number or by checking an actual signature against others held by the Council.

5. Data Subject Access Request

5.1. The GDPR allows individuals to make a Data Subject Access Request. In such a case an individual is entitled to receive, in an intelligible form, all information held relating to them.

5.2. It is essential that both computer and manual systems are designed in such a way that access requests can be dealt with quickly and effectively.

6. Security

6.1. Appropriate measures will be taken to ensure that personal data is secured. In computer operations this includes control over password access and making sure that only authorised persons use the facilities.

6.2. Manual records containing personal data will be accessible only to individuals that have legitimate use for the data. Waste will be disposed of with care with documents shredded when appropriate.

7. Disciplinary Action

7.1. The Council may consider disciplinary action against any Member or Employee who deliberately disregards any provisions of the GDPR.

7.2. Everyone should also be aware that the Regulation provides for separate personal liability for any offences in the Regulation. Where an offence is committed, individuals may be prosecuted and punished accordingly.