PORTSKEWETT COMMUNITY COUNCIL

GENERAL DATA PROTECTION REGULATIONS (GDPR) POLICY

1. INTRODUCTION

1.1 The General Data Protection Regulation ("GDPR") came into effect in the UK on 25th May 2018. It replaced the Data Protection Act 1998 and gives individuals more rights and protection regarding how their personal data is used. Community Councils must comply with its requirements, just like any other organisation.

1.2 The GDPR requires councils to appoint a Data Protection Officer ("DPO")

1.3 For the GDPR and new data protection legislation, the definition of public authorities is the same as that used in the Freedom of Information Act 2000 (which includes local councils).

2. UNDERLYING PRINCIPLES OF GDPR

2.1 The GDPR has a number of underlying principles. These include that personal data:

a. Must be processed lawfully, fairly and transparently.

b. Is only used for a **specific processing purpose** that the data subject has been made aware of and no other, without further consent.

c. Should be **adequate, relevant and limited** i.e. only the minimum amount of data should be kept for specific processing.

d. Must be **accurate** and where necessary **kept up to date**.

e. Should **not be stored for longer than is necessary**, and that storage is safe and secure.

f. Should be processed in a manner that ensures **appropriate security and protection**.

3. DATA / INFORMATION

3.1 "Data" is any information that can be identified to an individual. The rights of the "Data Subject" are crucial. If any information is held in respect of an EU resident then GDPR applies.

3.2 Under GDPR personal data now includes information relating to a living person, who can be identified directly or indirectly by such information (e.g. name, ID number, location data, an online identifier or one or more factors specific to the physical, physiological, genetic, mental, economic or social identity of that person).

3.3 The council is required to document what personal data it holds, where it comes from and who it is shared with (See Appendix 2).

4. DATA SUBJECT RIGHTS

4.1 GDPR includes the following rights for individuals:

a. The right to be informed.

b. The right to access.

c. The right to rectification.

d. The right to erasure.

e. The right to restrict processing.

f. The right to data portability.

g. The right to object.

h. The right not to be subject to automated decision making, including profiling.

5. LAWFUL BASIS FOR PROCESSING

5.1 The GDPR sets out six lawful bases for processing date. Unless an exemption applies, at least one of these will apply in all cases. It is possible for more than one to apply at the same time. The privacy notice must set out which lawful basis is being used (See Appendix 3).

5.2 The six lawful bases for processing personal data under GDPR are:

a. **Consent -** a controller must be able to demonstrate that consent was given.

b. **Legitimate Interests –** local councils are public authorities and under GDPR public authorities cannot rely on legitimate interests as a legal basis for processing personal data.

c. **Contractual Necessity**

d. **Compliance with Legal Obligation**

e. **Vital Interests –** e.g. in a life or death situation it is permissible to use a person's emergency contact information without their consent.

f. **Public Interest**

6. CONSENT

6.1 Consent must be transparent. Consents given in written declarations which also cover other matters must be clearly distinguishable and must be intelligible, easily accessible and in clear and plain language.

6.2 A record of how and when the consent was obtained must be made. This must be reviewed periodically. A consent form may be used by the council (See Appendix 4).

7. DATA BREACHES

7.1 A personal data breach is one that leads to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data.

7.2 Under GDPR there is an obligation to notify certain breaches to the Information Commissioners Office (ICO) within 72 hours, and in some cases data subjects have to be notified too.

7.3 All data breaches must be recorded along with details of actions taken.

7.4 Data breaches will be detected, reported and investigated in accordance with the council's Personal Data Breach policy (See Appendix 5).

8. DATA STORAGE

8.1 Personal data held by the council may be stored in different ways:

a. Paper copy.

b. Electronic files on computer.

c. Electronic files on memory stick.

d. Electronic files stored on the cloud.

8.2 The council is required to keep a record of how each set of data held is stored (See Appendix 2).

9. DATA SECURITY

9.1 Data security is an ever-increasing risk and the council takes various steps to limit the risk and impact of a personal data breach:

a. Personal data held by the council in paper format is kept in a locked cabinet.

b. Electronic files containing personal data held on the council computer are password protected and passwords are not duplicated. Access to passwords is restricted to the clerk, and the Chairman holds a sealed, documented copy of the passwords used which is stored away from the council office.

c. Monthly back-ups of electronic files are taken and stored on a memory stick which the Chairman stores away from the council office.

d. Daily/Weekly back-ups of electronic files are stored on the Microsoft Cloud.

e. The password has been changed on the router through which the council accesses the internet, from the password it was issued with.

f. Norton Anti-virus has been installed on the council computer.

g. Use of the council computer is password controlled, and access is restricted to the clerk.

This policy has been reviewed by an independent 3rd party, Mr B. Lillie, and was adopted by the Council at it's meeting held on 18th September 2018.