BREDGAR PARISH COUNCIL (BPC)

Data Protection Management Procedure

This Procedure was reviewed by the Full Council at its meeting held on 12th February 2020.

1) **Scope**
   Staff and Councillors of BPC are required to read this procedure.

2) **Objective**
   To prescribe the Data Protection Management procedures that staff and councillors should operate as they implement BPC Policies.

3) **Parish Council New Contact Procedures**
   Staff and councillors of BPC must make new contacts aware if their personal data will be held and obtain agreement. The General Privacy Notice may be used to advise new contacts.

4) **New Projects Procedure**
   When starting a new project or community engagement BPC will define what personal data needs to be held, its scope of use and retention time-scale. This information will be disclosed to all who become involved to ensure they are fully informed about how their personal data will be used and for their permission or instructions to be obtained.

5) **Service Access Requests Procedure**
   When BPC receives a Service Access Request it will initiate the following response:

   a) The Clerk will immediately inform the Chair of BPC
   b) The Clerk will perform checks to validate the identity of the requester and their right to see the data requested. For example, checking the electoral roll and / or requiring a photo ID.
   c) If the identity cannot be validated the Clerk will inform the Chair of BPC, the requester and then await further instruction.
   d) If the identity of the requester is validated the Clerk will obtain copies of all the relevant personal data.
   e) If necessary to respond fully to the SAR, the Clerk may request that Councillors provide copies of emails or files held on their personal computers.
   f) The Clerk will redact any personal data of other people.
   g) The Clerk will provide copies to the requester within one month of receipt of the request or sooner (if possible).
   h) The requester will be advised that they have the right to complain to the ICO.

i) If the information requested “manifestly unfounded or excessive” a reasonable fee will be charged.

6) **Freedom of Information Requests Procedures**

a) BPC have published a Freedom of Information Act Schedule showing Class 1 to 7 information to be published and the fees applied for Hard Copy.
b) The Freedom of Information Request must include sufficient information for BPC to identify the information requested.
c) The Clerk will provide the information within 20 days of receiving the request.

7) **Personal Data Breach Procedures**

A personal data breach can be broadly defined as a security incident that has affected the confidentiality, integrity or availability of personal data. In short, there will be a personal data breach whenever any personal data is lost, destroyed, corrupted or disclosed; if someone accesses the data or passes it on without proper authorisation; or if the data is made unavailable, for example, when it has been encrypted by ransomware, or accidentally lost or destroyed.

In the event that BPC detects or becomes aware of a personal data breach the following actions will be taken:

a) The BPC Data Protection Compliance Officer (DPCO) and Chair must be made aware of the personal data breach immediately it is found.
b) The DPCO will initiate an investigation as soon as possible to identify the reason for the data breach, the scope, and the individuals whose personal data has been breached and to assess the risk to them.
c) Once identified the individuals will be informed without undue delay.
d) If the breach is likely to result in a high risk of adversely affecting individuals’ rights and freedoms BPC will notify the relevant supervisory authority within 72 hours. Section IV of the GDPR Article 29 Working Party guidelines on personal data breach notification will be used as guidance for assessing the risk.

   BPC will report the following information:

   - a description of the nature of the personal data breach including, where possible:
   - the categories and approximate number of individuals concerned; and
   - the categories and approximate number of personal data records concerned;
   - the name and contact details of the data protection officer or other contact point where more information can be obtained;
   - a description of the likely consequences of the personal data breach; and
   - a description of the measures taken, or proposed to be taken, to deal with the personal data breach, including, where appropriate, the measures taken to mitigate any possible adverse effects.

e) All data breaches will be recorded by BPC.

8) **Data Protection Monitoring Procedure**

Keep BPC staff and councillors regularly updated about data security issues.

Perform annual check of the BPC computer

a) Download and execute the latest Microsoft Safety Scanner tool.
b) Review system logs for data breach indicators.
c) Check regularly that patches are being installed successfully and in a timely manner.
d) Check that anti-virus software is operating and up to date.
e) Check that the Firewall software is operating.

9) **Data Protection Assessment – New Projects**
A data protection assessment will be performed at the start of any new BPC project or initiative that involves gathering of personal data. The assessment will identify the personal data that will be gathered, how it will be used and to prepare an appropriate privacy notice for distribution to all participants.