Bramerton Parish Council

GENERAL DATA PROTECTION REGULATIONS (GDPR) POLICY

INTRODUCTION

1. The GDPR are EU regulations which come into force in May 2018. The Government has confirmed that after the UK leaves the EU, GDPR will still be a legal requirement in England. This policy identifies how Bramerton Parish Council will meet the requirements set out in those regulations. The Council will be registered with the Information Commissioner's Office.
2. Personal data must be:
    i. processed lawfully, fairly and transparently;
    ii. collected for specified, explicit and legitimate purposes;
    iii. adequate, relevant and limited to what is necessary for processing;
    iv. accurate and kept up to date;
    v. kept only for as long as is necessary for processing;
    vi. processed in a manner that ensures its security.

IDENTIFYING ROLES & MINIMISING RISK

3. GDPR require that the Council and its staff understand the implications of GDPR and that roles and duties must be assigned. The Council is the data controller and the Clerk is the data processor. The Council will appoint a suitably qualified Data Protection Officer (DPO) who may serve as Clerk provided this does not lead to a conflict of interest. It is the DPO's duty to undertake an information audit and to manage the information collected by the Council, the issuing of privacy statements, dealing with requests and complaints raised and also the safe disposal of information.
4. GDPR require continued care by Councillors and staff when sharing information about individuals as hard copy or electronically. A breach of the regulations could result in a fine from the Information Commissioner's Office (ICO) for the breach itself and payment of compensation to any individual(s) who are adversely affected. The handling of information is a high/medium risk to the Council (both financially and reputationally) and must be included in the Council's Risk Management Policy. Potential risks will be minimised by undertaking an information audit, issuing privacy statements, maintaining privacy impact assessments (an audit of potential data protection risks with new projects), by minimising who holds protected data, and by Councillors and staff undertaking training in data protection.

DATA BREACHES

5. Data breaches should be reported to the DPO who will conduct an investigation with the support and co-operation of Councillors and the Clerk. Investigations must

be undertaken within one month of the report of a breach. The DPO will (within 3 days of notification) advise the ICO of any breach where it is likely to result in a risk to the rights and freedoms of individuals, for example, if it could result in discrimination, damage to reputation, financial loss, loss of confidentiality, or any other significant economic or social disadvantage. Where a breach is likely to result in a high risk to the rights and freedoms of an individual(s) the DPO will also notify those concerned directly.

6. No person may use IT equipment which is logged in by another person. No employee, volunteer or Councillor may use IT in any way that may cause problems for the Council. For example, the discussion of internal Council matters on social media sites could result in reputational damage for the Council and/or individuals.

PRIVACY NOTICES

7. The Council will adopt a privacy notice which will be issued to individuals to tell them what the Council does with their personal information. A privacy notice will contain the name and contact details of the data controller and Data Protection Officer, the purpose for which the information is to be used and the length of time for its use. It will be written in clear language and will advise the individual that they can, at any time, withdraw their agreement for the use of this information. Some changes to the wording may be needed depending the recipient, for example, when it is issued to children. Issuing of a privacy notice must be detailed on the Information Audit kept by the Council. All privacy notices must be verifiable.

INFORMATION AUDIT

8. The DPO will undertake an information audit which details the personal data held, where it came from, the purpose for holding that information and with whom the Council will share that information. This will include information held electronically or as a hard copy. Information held could change from year to year with different activities, and so the information audit will be reviewed at least annually or when the Council undertakes a new activity. The information audit review should be conducted ahead of the review of this policy and the reviews should be minuted.

INDIVIDUALS' RIGHTS

9. GDPR confirms existing rights for individuals:
    i. the right to be informed
    i. the right of access
    ii. the right to rectification
    iii. the right to erasure
    iv. the right to restrict processing
    v. right to data portability
    vi. the right to object
    vii. the right not to be subject to automated decision-making, including profiling.

10. GDPR also give individuals the right to:
    i. have their personal data erased (sometime known as the 'right to be forgotten') where retention of personal data is no longer necessary for the purpose for which it was originally collected;

ii. data portability free of charge. Data portability refers to the ability to move, copy or transfer data easily between different computers.

11. When a request is received to delete information the DPO must respond within a month. The DPO has the delegated authority from the Council to delete information.

12. If a request is considered to be manifestly unfounded then the request may be refused or a charge may be applied. The charge will be as detailed in the Council's Freedom of Information Publication Scheme. The DPO will inform the Council of such requests.

CHILDREN

13. There is special protection for the personal data of a child. For the purposes of these regulations the age when a child can give their own consent is 13. If the Council requires consent from a child under 13 years of age, the Council must obtain a parent or guardian's consent in order to process the personal data lawfully. Consent forms for children age 13 plus, will be written in clear language that they can understand.

SUMMARY

14. The main actions arising from this policy are:

i. The Council will be registered with the ICO.
ii. A copy of this policy will be available on the Council's website. The policy will be considered as a core policy for the Council.
iii. The Clerk's Contract and Job Description (if appointed as DPO) will be amended to include additional responsibilities relating to data protection.
iv. An information audit will be conducted and reviewed at least annually or when projects and services change.
v. Privacy notices will be issued as required.
vi. Data Protection will be included on the Council's Risk Management Policy.

15. This policy document is written with current information and advice. It will be reviewed annually or earlier if further guidance is received.

16. All employees, volunteers and Councillors are expected to comply with this policy at all times to protect privacy, confidentiality and the interests of the Council.