Crowle & Ealand Town Council

General Data Protection Regulations (GDPR) Policy

1.0 Purpose of the policy and background to the General Data Protection Regulation

1.1 This policy is taken from policy and procedures as set by the UK government. For full, comprehensive information about GDPR, please refer to: https://www.gov.uk/government/publications/guide-to-the-general-data-protection-regulation

1.2 This Council must ensure personal data be:

- processed lawfully, fairly and transparently
- collected for specified, explicit and legitimate purposes
- be adequate, relevant and limited to what is necessary for processing
- be accurate and kept up to date
- be kept only for as long as is necessary for processing and be processed in a manner that ensures its security.

2.0 Identifying the roles and minimising risk

2.1 GDPR requires that everyone within the council must understand the implications of GDPR and that roles and duties must be assigned. The Council is the data controller and the Clerk /RFO are the Data Protection Officers (DPOs). It is the DPOs duty to undertake an information audit and to manage the information collected by the council, the issuing of privacy notices, dealing with requests and complaints raised and also the safe disposal of information.

2.3 Continued care is required by everyone within the council; councillors and staff plus any contactors or volunteers that access and/or share any information about individuals, whether hard copy or electronically. A breach of the regulations could result in the council facing a fine from the Information Commissioner's Office (ICO) for the breach itself and also to compensate the individual(s) who could be adversely affected. Therefore, the handling of information is seen as medium risk to the council which must be included in the Risk Management.

2.4 Policy of the council. Such risk can be minimised by undertaking an information audit, issuing privacy notices, maintaining privacy impact assessments (an audit of potential data protection risks with new projects), minimising who holds data protected information and the council undertaking training in data protection awareness.

2.5 Non-authorised users are not permitted access to IT using employees' log-in passwords or to use equipment while logged on. It is unacceptable for employees, volunteers and members to 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 to individuals.

3.0 Data breaches

3.1 The DPOs will the investigation any breaches identified or reported. The DPO will conduct this with the support of the Town Council. Investigations must be undertaken within one month of the report of a breach. The ICO will be advised of a breach (within 3 days) where it is likely to result in a risk to the rights and freedoms of individuals – if, for example, 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 individuals, the DPO will also have to notify those concerned directly.

4.0 Privacy Notices

4.1 Crowle & Ealand Town Council displays a Privacy Notice on the Council website. It can be found at www.crowleandealandcouncil.org and identifies; contact details of the data controller and Data Protection Officers, the purpose for which the information is to be used and the length of time for its use.

5.0 Information Audit

5.1 The DPOs will undertake information audits which detail 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.

5.2 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.

6.0 Individuals' Rights

6.1 GDPR gives individuals rights with some enhancements to those rights already in place:

- the right to be informed
- the right of access
- the right to rectification
- the right to erasure

- the right to restrict processing
- right to data portability
- the right to object
- the right not to be subject to automated decision-making including profiling.

6.2 The two enhancements of GDPR are that individuals now have a right to have their personal data erased (sometime known as the 'right to be forgotten') where their personal data is no longer necessary in relation to the purpose for which it was originally collected and data portability must be done free of charge. Data portability refers to the ability to move, copy or transfer data easily between different computers.

6.3 If a request is received to delete information, then the DPOs must respond to this request within a month. The DPOs have the delegated authority from the Council to delete information.

6.4 If a request is considered to be manifestly unfounded then the request could be refused or a charge may apply. The charge will be as detailed in the Council's Freedom of Information Publication Scheme. The Parish Council will be informed of such requests.

7.0 Children

7.1 There is special protection for the personal data of a child. The age when a child can give their own consent is 13. If the council requires consent from young people under 13, this must be obtained from a parent or guardian's in order to process the personal data lawfully. Consent forms for children age 13 plus, must be written in language that they will understand.

8.0 Summary

8.1 The Council's main actions from this policy are:

- The Council is registered with the ICO.
- A copy of this policy is available on the Council's website.
- Staff Contract and Job Descriptions have been amended to include additional responsibilities relating to data protection.
- An information audit will be conducted and reviewed at least annually or when projects and services change.
- Privacy notices must be issued.
- Data Protection is included on the Council's Risk Management Policy.
- All staff, councillors, contractors, volunteers will be instructed to read the necessary policies or briefed accordingly by the DPOs.
- The Town Council will manage the process.

8.2 This policy document is written with current information and advice. It will be reviewed at least annually or when further advice is issued by the ICO.

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

8.4 Attachments to this Policy

Crowle & Ealand Town Council Privacy Notice
Crowle & Ealand Town Council GDPR (Service) Consent to hold Contact Information
Crowle & Ealand Town Council Subject Access Request Form
Information Available From Crowle & Ealand Town Council under the Model Publication Scheme
Crowle & Ealand Town Council Date Security Breach Reporting Form
Crowle & Ealand Town Council Privacy Impact Assessment (PIA)

Adopted: April 2020
Review: April 2021