KESGRAVE TOWN COUNCIL DATA PROTECTION POLICY GDPR 2018

The Town Council as an employer, believes that protecting personal information is very important. This statement outlines how the Council use and protect that information and the principles which reflect our commitment to safeguarding that information. For its employees, the principles of the Data Protection Act (DPA) are binding.

The Council fully adheres to the Data Protection law from 25th May 2018, when the 2016 EU Directive known as the General Data Protection Regulation (GDPR) takes effect. The GDPR will effectively replace the 1998 Act which implemented the EU Data Protection Directive. The Government has confirmed that the UK's decision to leave the EU will not affect the commencement of the GDPR in 2018.

The Council's Principles

Our principles in respect of processing personal information are:

- To comply with its obligation under the Data Protection Act 1998 replaced in May 2018 by the GDPR and other relevant legislation.
- To keep personal information in strict confidence.
- To obtain personal information lawfully and fairly.
- Not to disclose personal information without the permission of the individual to which it relates except in limited circumstances as permitted or required by law.
- However, the Council may share personal information with agents or service providers in connection with providing, administering and servicing the products purchased from it, subject to the clear consent of the Data Subject.
- The Council will maintain appropriate procedures to ensure that personal information in its possession is accurate and, where necessary, kept up to date.
- Where it chooses to have certain services, such as data processing, provided by third party providers, the Council does so in accordance with applicable law and takes all reasonable precautions regarding the practices employed by the service provider to protect personal information.
- The Council will maintain appropriate technical and organisational safeguards to protect personal information against loss, theft, unauthorised access, disclosure, copying, and use of modification.
- The Council will not sell or give out personal information.
- The Council's culture respects the personal data that it holds.
- The Council has a culture of compliance with information security in place with this policy and guidelines for its staff and councillors.

How we process personal information

The Council may make use of information given to it, or which it receives from any enquiries it makes as follows:

- for processing and administering any contract it has and for general business purposes including resident services, research and statistical analysis
- passing to any intermediary or other agent acting on behalf of the person to whom the information relates
- passing/disclosing to any third party providing services to the Council, including, where relevant, tracing agencies
- passing the information on to its regulators

Anyone has the right to ask for a copy of the information held by the Council in its records.

They also have the right to request correction of inaccuracies in our information.

The General Data Protection Act Regulation (GDPR) from 25th May 2018 (Replacing the Data Protection 1998 Act)

This will mean the requirement to notify staff/others of any breach within 72 hours of becoming aware of the breach. Financial penalties will be applied for non-compliance. The Town Council has an Action Plan. (See separate document). The Town Council has audited the data that it holds and the purposes for processing this. (January 2018). This is a continuous process. The Town Council has not as yet appointed its Data Protection Officer (DPO), as advice from NALC (National Association of Local Councils) and SALC (Suffolk Association of Local Councils) is awaited. This role will require informing and advising the Council and its staff about the obligations to comply, monitoring compliance – including managing internal data protection activities, advise on data protection impact assessments, train staff and conduct internal audits. Also, to be the first point of contact for the regulator and for individuals whose data is processed. (The DPO (Data Protection Officer) will manage this).

HR work involves handling employees' personal information, some of it sensitive, such as details about health or family life. Organisations are already familiar with their data protection responsibilities towards this information under the Data Protection Act 1998, but from May 2018, those duties will be tightened up under the General Data Protection Regulation. The new rules are intended to meet the needs of a digital age, and require a change in organisational attitude towards data privacy. HR has a crucial role to play in achieving the new goal of data protection by design and default.

Processing of data will need to be lawful and necessary. All organisations keep records and personal data.

A new employee will signify their agreement to process certain personal information by virtue of signing a contract of employment. This is consent in the context of employment. (Article 29) (GDPR Article 6, 9).

For those applying for jobs, a signature on the application form signifies the applicant's agreement to their personal data being confidentially, lawfully and processed in a necessary manner. All applications should be shredded after 6 months of a post being filled, for those who are unsuccessful.

Privacy settings and passwords should be included for recording data, with audit trails.

Threats to Data Security

- External hackers
- Sharing data with third parties
- Employee breaches/theft
- Wireless computing
- Inadequate firewalls.

Personal Data – This refers to a living individual who can be identified from the data, including any opinions about the individual.

Data Controller – This is a person, (including an organisation or company) who determine the manner in which any personal data is processed.

Data Processor – This is any person who processes personal data on behalf of a data controller. Employees of data controllers are excluded from this definition.

Data Subject – This is a living individual about whom a data controller holds personal data.

Data Processing – In relation to data, this includes obtaining, recording or holding data or carrying out any operation or setting up operations on the data including organising, amending, retrieving, using, disclosing, erasing or destroying data.

Principles

- The data must be fair and lawful processing
- It is obtained only for specified lawful purposes
- The data must be adequate, relevant and not excessive in relation to the purposes for which it is processed
- The data must be accurate and where necessary, kept up to date
- The data must not be kept for longer than is necessary
- The data must be processed in accordance with the rights of the data subject
- Appropriate technical and organisational security measures must be taken to prevent unauthorised or unlawful processing, accidental loss of or destruction or damage to personal data
- Personal data must not be transferred outside of the EEA unless the destination country ensures an adequate level of protection for the rights of the data subject in relation to the processing of personal data.

Consent of Processing Data

- This is necessary for the performance of a contract with the data subject.
- This is necessary for compliance with a legal obligation by the controller
- This is necessary in order to protect the vital interests of the individual or of another person
- This is necessary for the performance of a public interest task or in exercising an official authority vested.
- This is necessary for the purposes of the legitimate interests.

Valid Consent

- This should be positive, affirmative action
- It should be specific and unambiguous
- It should be freely given, (e.g. performance of a contract cannot be conditional on this)
- It signifies the individual's agreement to their personal data being processed
- Separate and distinguishable (e.g. a separate form)
- The valid consent should be clearly presented
- It is revocable
- Before the consent is given, the Town Council should set out clearly that the individual has the ***right to withdraw*** at any time
- The Town Council should ensure that the consent is affirmatively and freely given, and be clear and distinguishable, (e.g. provide a ***separate form***
- The Town Council should obtain consent for different processing operations. It ***should not "bundle" the data together*** for multiple uses.

Consent in Employment (Article 29) – Employees are in theory able to refuse their consent but the consequence may be the loss of a job opportunity.

Legitimate Interests to process Data

- It is necessary for the performance of a contract with the data subject
- It is necessary for compliance with the legal obligation of the controller

Lawful Processing
Contents of Information Notice (needs to go to all employees)

- This Notice should state the name and contact details of the controller.
- It should give details of the categories of the data being processed
- It should give details of whom data will be disclosed to
- It should state the purposes of the data processing
- It should give details about the legal basis of the processing
- It should give an explanation of the legitimate interests that justify the processing
- It should state that consent can be withdrawn

Sensitive Personal Data
(Para. 1 (1) (a) of Schedule 1, Part 1 of the Data Protection Bill) – The processing should be necessary for the purposes of performing or exercising obligations or rights of the controller or the data subject under employment law, social security, or the law relating to social protection.

Individual Rights

- Subject Access Requests are possible ("SARs")
- There should be data portability
- The individual can object to the processing.

Accountability – The importance of the Town Council demonstrating compliance with the data protection principles include:

- Implementing the appropriate technical and organisational measures to ensure compliance, (e.g. staff training, regular internal audits etc).
- compliance, (e.g. staff training, regular internal audits etc).
- Maintaining relevant documentation on processing activities
- Data Protection Impact Statements/internal audits.

Data Protection Breach Reporting

- Any breaches must be reported to the Town Council within 72 hours of the breach
- The Town Council will only report the alleged breach to the individual/s concerned if there is a potential "high risk" breach, (i.e. if actual damage could be caused, reputational or otherwise)

LAST REVIEWED AND RESOLVED; 15th January 2018;
Interim Review; 14th May 2018;
NEXT REVIEW DUE; March/April 2019.