KINGSTON PARISH COUNCIL

DATA PROTECTION POLICY

September 2018

1. Introduction

Kingston Parish Council is required to process relevant personal data regarding members of staff, Councillors, subscribers to its email services and other members of the public.

The processing of personal data is governed by legislation relating to personal data which applies in the United Kingdom including the General Data Protection Regulation (the GDPR) and other legislation relating to personal data and rights such as the Human Rights Act.

This policy sets out the Council's commitment to protecting personal data. For clarity, personal data means any data or information, in paper or digital format, relating to a living individual.

2. Data Protection Principles

Kingston Parish Council complies with the General Data Protection principles and ensures that personal data is:

- Processed fairly and lawfully and in a transparent manner;
- Obtained for one or more specified, explicit and lawful purposes;
- Adequate, relevant and only limited to what is required;
- Accurate and where necessary kept up to date;
- Not kept in a form which permits identification of data subjects for longer than is necessary;
- Processed in accordance with the rights of data subjects; and
- Processed in a manner that ensures appropriate security of the personal data.

Anyone who processes data on behalf of the Council, including staff, Councillors, volunteers, contractors or others who process or use any personal information must ensure that they follow these principles at all times.

3. General requirements

Significant requirements under the DPA and GDPR are:

- Personal data should only be accessed by those who need to for work purposes
- Personal data should not be divulged or discussed except when performing normal work duties
- Personal data must be kept safe and secure at all times, including at the office, public areas, home or in transit
- Personal data should be regularly reviewed and updated
- Queries about data protection, internal and external must be dealt with promptly.

4. Sensitive personal information

There are more stringent measures in place to protect sensitive personal data. Sensitive personal data means personal data consisting of information as to:

- the racial or ethnic origin of the data subject,
- political opinions, religious beliefs or other beliefs of a similar nature,

- membership of a trade union,
- physical or mental health or condition,
- sexual life
- the commission or alleged commission of any offence, or any proceedings for any offence committed or alleged to have been committed by the data subject, the disposal of such proceedings or the sentence of any court in such proceedings.

Data of this nature is subject to additional protection because the presumption is that information about these matters could be used in a discriminatory way and is likely to be of a private nature.

The majority of the Council's work should be carried out without the need to collect sensitive personal information. In the event that such information is required to perform a legitimate business function, the collection should be limited to only what is necessary and processed only for that function and be stored securely.

5. Information Sharing

Personal data may need to be shared with other organisations in order to deliver services or to perform duties of the Council. This can only be done where the Council has permission or there is a legal obligation to share such data.

Emails and other correspondence received by the Council and not specifically addressed to the Clerk (e.g. to Kingston Parish Council or the Council's generic email address) may be shared with Councillors. Other emails or correspondence received by the Clerk may be shared with Councillors provided that all personal data is redacted from such email or correspondence save if the sender has first given approval for sharing without redaction. For all other business functions, there should be an information-sharing agreement in place which sets out the reasons for the collection and processing of the data.

Personal data can be shared within the Council or with other third parties where there is an established purpose.

One of the key changes within the GDPR is data protection by default and design. Data Sharing Agreements should be completed when setting up 'on-going' or 'routine' information sharing arrangements with third parties. However, they are not needed when information is shared on a "one-off" basis in "exceptional circumstances" (i.e. in conditions of real urgency). In these cases, a record of the decision and the reasons for sharing information should be kept.

All Data Sharing Agreements must be signed off by the Chairman or Vice-Chairman and the Data Protection Officer who will keep a register of all Data Sharing Agreements.

6. Privacy Impact Assessments (PIAs)

PIAs will be completed in these situations to help identify and minimise risks to individuals and must be completed in the following situations that involve personal data:

- At the beginning of a new project or when implementing a new system
- Before entering a data sharing agreement
- When major changes are introduced into a system or process

7. Subject Access Requests (SARs)

The Council recognises that access to personal data held about an individual is a fundamental right provided in the GDPR and will ensure that all requests from individuals

to access their personal data are dealt with as quickly as possible and within the timescales allowed in the legislation.

Individuals will be expected to submit SARs in writing and provide any necessary proof of identification as part of the request. No charge can be made to provide this data.

Of prime importance is that information is not given out recklessly. Anybody requiring data should be requested to write to the Clerk detailing their request. The Council can offer to forward any correspondence, or information, should its records show that it has the necessary data.

8. Complaints

Anyone who feels that the Council has broken the law in any way can complain. Examples of this are when they think their information has not been obtained fairly, it has not been handled securely or they have asked for a copy of their information and they are not happy with the Council's response.

Individuals who consider that data is inaccurate or out of date may also request, in writing, that the information be corrected or erased. They will receive a written response indicating whether or not the Council agrees and if so, the action to be taken.

Individuals can also ask the Council to stop handling their personal information if they think this will cause them harm or distress. This is not always possible but in such circumstances the request will be reviewed on a case by case basis.

Data Protection Act complaints will be dealt with by the Chairman or Vice-Chairman and a Councillor.

9. Non Compliance

One of the major changes implemented through the GDPR is the level of fine which can be levied on an organisation in cases of non compliance or data breaches. The administrative fines are discretionary rather than mandatory; they must be imposed on a case-by-case basis and must be "effective, proportionate and dissuasive". In the most serious of cases the fine can be up to €20,000,000 or 4% of annual turnover, whichever is the greater. Serious breaches of this policy caused by deliberate, negligent or reckless behaviour could result in disciplinary action and may even lead to criminal prosecution.

Where those breaching the policy are not Council employees, this will be regarded as a breach of contract and may lead to termination of their contract.

10. Role of the Data Protection Officer

The Council has designated the Clerk to act as Data Protection Officer. Any query relating to the implementation within the Council, of the Data Protection Act and Subject Access Requests under section 7 of the Act should be referred to the Chairman.

The Data Protection Officer will be responsible for ensuring that the Council's entry on to the ICO register is kept up to date and all fees to the ICO are paid in time.