

## KINGSTON BAGPUIZE WITH SOUTHMOOR PARISH COUNCIL

### DATA PROTECTION POLICY

We understand the importance of ensuring that personal data, including sensitive personal data is always treated lawfully and appropriately and that the rights of individuals are upheld.

We are required to collect, use and hold personal data about individuals. Data is required for the purposes of carrying out our statutory obligations, delivering services and meeting the needs of individuals that we deal with. This includes current, past and prospective employees, service users, members of the public, Members of the Council, our business partners and other local authorities or public bodies.

#### Policy Objectives

In order to comply with the requirements of the Data Protection Act 1998, and the General Data Protection Regulations 2018 we will ensure that:

1. Any personal data will be collected, used and held, lawfully and appropriately.
2. Regular data sharing with external partners and other relevant agencies will be subject to information sharing agreements. Partnerships will only be entered into where there is a clear statutory power enabling the council to participate.
3. External agencies contracted to undertake any data processing on behalf of the us will be required to demonstrate compliance with the Data Protection Act and satisfy the council that it has the necessary technical and organisational measures in place to protect personal data.
4. Training needs are identified and provided to ensure that those handling personal data are trained appropriately.
5. [There is an appointed officer who has specific responsibility and knowledge about data protection compliance covering all aspects within the scope of this policy and who is a point of contact for all queries.]
6. There are a number of employees throughout the organisation who have specific responsibilities for data protection.
7. Data Subjects rights can be fully exercised.
8. Subject Access Requests are dealt with promptly and courteously.
9. Any new projects being implemented that involve personal data will undergo a privacy impact assessment.

We are required by law to share or make available some of the personal data we collect and hold. This information may be shared for a number of reasons including to safeguard public funds and for the prevention and detection of fraud, and for the prevention and detection of crime. For more details on this please read our [Privacy Notice](#).

#### Meeting our Policy's Objectives

In order to meet the objectives that are listed above we need to ensure that the following are always considered and that appropriate controls and procedures are in place to ensure compliance with the Data Protection Act.

#### Collecting and Processing Personal Data

- When we collect personal data we will ensure that where required, we make individuals aware that their information is being collected, the purpose for collecting

the data specified, and whether it will be shared with any third parties. This will be done through the use of privacy notices. When reviewing documents and forms, we will always consider whether a privacy notice should be included.

### Data Security

- The Clerk and Members must report any suspected data breaches to the Data Protection Officer for investigation and where necessary the Data Protection Officer will notify the Information Commissioner's Office
- The Clerk and Members must use appropriate levels of security to store or share personal data.

An Information Asset Register will be maintained by the Data Protection Officer identifying:

- all personal data held
- where it is held
- how it is processed
- what teams have access to it
- who has overall responsibility for the data.

Personal data will not be shared with a third party organisation without a valid business reason and where required we will notify individuals that the sharing will take place in the form of a privacy notice. If any new purposes for the data sharing are to take place, we will seek consent from the individuals concerned.

When personal data is to be shared regularly with a third party, a Data Sharing Agreement must be implemented.

Any data sharing will also take into consideration:

- any statutory basis of the proposed information sharing
- whether the sharing is justified
- how to ensure the security of the information being shared.

### Data Access

- The Clerk and Members will have access to personal data only where it is required in order to fulfil their role.
- All data subjects have a right of access to their own personal data; employees will be made aware of and will provide advice to data subjects about how to request or access their personal data held by us.
- A Subject Access Request will be acknowledged to the data subject within 24 hours, with the final response and disclosure of information (subject to exemptions) within 40 calendar days.
- Third party personal data will not be released by us when responding to a Subject Access Request (unless consent is obtained, it is required to be released by law, or it is deemed reasonable to release).

Adopted by the council at their meeting of 9 April 2018

To be reviewed as and when new regulations require it.