Binfield Parish Council

Data Retention Transfer and Disposal Policy

1. Policy statement

1.1. This policy is intended to help employees and Councillors make appropriate decisions about the Retention, Transfer and Disposal of data in line with the Information and Data Protection Policy [adopted February 2023].

1.2. All statutory requirements are to be in line with current Government legislation.

2. The scope of the policy

2.1. All employees and Councillors are expected to comply with this policy at all times.

2.2. This policy refers to the Retention, Transfer and Disposal of all the Council's collected information including paper, electronic, hand-written and any other data in the possession of the council covered by the rules of this policy.

3. Responsibility for implementation of the policy

3.1. The council has overall responsibility for the effective operation of this policy.

3.2. The Clerk is responsible for monitoring and reviewing the operation of this policy and making recommendations for changes to minimise risks to the Council.

3.3. All employees should ensure that they take the time to read and understand it. Any breach of this policy should be reported to the Clerk.

3.4. Questions regarding the content or application of this policy should be directed to the Clerk.

4. Data Audit

4.1 The Clerk shall be responsible for a Data Audit. This details what information is retained, the legal basis for holding it, how it is processed, for what reason and any consent sought. The audit also should include information about how long the information will be kept and how it will be disposed of.

5. Security of Data

5.1 The majority of physical data and paperwork of the Council is held at the Parish Office. This will be locked when neither a member of staff nor Councillor is present.

5.2 Some archived records may be held in a secure storage facility offsite. A copy of legal documentation is also retained offsite at the private residence of the Clerk.

5.3 All computers and laptops are password protected for use by employees. Only employees have access to the MS365 system where all the Council's documents are stored. For documents including sensitive data, the documents will be password protected with the passwords only being given to staff who will process the data.

5.4 Councillors who, in order to progress Council business, have received data are also bound to treat it in the manners described in this and other data protection policies adopted by the Council.

5.5 If a member of the public has requested access to information whilst visiting the parish office or by prior arrangement, access will be facilitated whilst in the presence of a member of staff.

6. Consent

6.1 Consent will be sought to hold information, both personal and/or sensitive, from those in contact with the Council unless a lawful reason to hold data without consent exists (eg contractual). Those whose data will be held will be advised about their consent and information given as detailed in this policy about its retention, transfer and disposal.

7. Retention of Data

7.1 The data audit lists the information held by the Council. This list will be added to when new projects or systems are started and will be reviewed, as a minimum, annually

7.2 The Council will adhere to the principle that data should only be kept as long as necessary and, if no longer necessary, the data will be disposed of in the manner set out in this policy.

7.3 Personal information will be held on the many groups and members of the public as listed in the Data Audit. This will be held where required by compliance with legal obligation or contractual necessity and to facilitate the work of the council.

7.4 Sensitive information will be held about employees relating to payroll, heath, employment issues. Sensitive information may be held on members of the public or children due to work undertaken by the Council. Sensitive information may be held on Councillors. This will be held where required by compliance with legal obligation or contractual necessity as laid out in the Data Audit.

8. Transfer of Data

8.1 Data may be transferred to facilitate the work of the council.

8.2 Where possible, information will be anonymised so that transfer of data will not include personal or sensitive information.

8.3 If consent is required (ie there is no lawful reason to hold or transfer the data), consent will be requested to transfer data. Where consent is not given, the data subject will be redirected to the proposed recipient.

8.4 All data transferred will be managed as set out in the Information and Data Protection Policy.

9. Disposal of Data

9.1 Data will be retained in line with Government legislation with regard to financial records (six years plus the current year) and as listed on the Data Audit and agreed with Council. After that time it will be disposed of. All Councillors and employees should take particular care with sensitive data and its disposal should be in line with all the Council's policies related to data protection.

9.2 Personal Data on paper will be shredded. Councillors are requested to shred all paper information in the timescale stated on the adopted Data Audit.

9.3 Personal Data held electronically will be deleted from the O365 and email systems. Councillors are requested to make their best endeavours to delete information transferred to them from the office staff.

9.4 Sensitive Data on paper will be disposed of via a data management service in a responsible and sustainable way.

9.5 Sensitive Data held electronically will be deleted from the O365 and email systems. Councillors are requested to make their best endeavours to delete information transferred to them from the office staff.

9.6 If there are historic records that are of wider interest, it may be appropriate that they are transferred to the County Records Office.

10. Monitoring and Review of this Policy

10.1 The Clerk shall be responsible for reviewing this policy annually to ensure that it meets legal requirements and reflects best practice.

10.2 The Clerk shall be responsible for reviewing the Data Audit to ensure that it reflects the current data held by the Council.

10.3 The Council shall consider adoption of the reviewed policy and Data Audit annually.

11. Breaches

11.1 All breaches of this policy will be reported to the Council and subject to the adopted Disciplinary Policy.