Data Protection Policy

Prepared by:	Leroy Philbrook Chief Executive Officer and Town Clerk
Date:	October 2018
Next Review date:	October 2019

Contents

1. Policy Statement

Colne Town Council takes Data Protection very seriously and understands that it has statutory and moral obligations to ensure that individuals personal data is collected and used only when necessary to carry out Colne Town Council Business. This policy outlines the responsibility that the Colne Town Council has as a Corporate Body and gives clear indication as to how this duty will be carried out in line with The Data Protection Act 2018 as UK's implementation of the General Data Protection Regulation.

2. Definitions

Corporate Body	means Colne Town Council.
GDPR	means the General Data Protection Regulation.
Responsible Person	means Chief Executive Officer as Lead for Corporate Body on Data Protection.
Register of Systems	means a register of all systems, procedures and contexts in which personal data is processed by the Corporate Body.

3. Data protection principles

3.1 The Corporate Body is committed to processing data in accordance with its responsibilities under The Data Protection Act 2018 which is UK's Act implementing GDPR.

3.2 Article 5 of the GDPR requires that personal data shall be:

3.2.1 Processed lawfully, fairly and in a transparent manner in relation to individuals;

3.2.2 Collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be considered to be incompatible with the initial purposes;

3.2.3 Adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed;

3.2.4 Accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay;

3.2.5 Kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed;

3.2.6 Personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, historical research purposes or statistical purposes subject to implementation of the appropriate technical and organisational measures required by the GDPR in order to safeguard the rights and freedoms of individuals; and

3.2.7 Processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and accidental loss, destruction or damage, using appropriate technical or organisational measures.

4. General provisions

4.3 This policy applies to all personal data processed by the Corporate Body.

4.4 The Responsible Person shall take responsibility for the Corporate Body's ongoing compliance with this policy.

4.5 This policy shall be reviewed at least annually.

4.6 The Corporate Body shall register with the Information Commissioner's Office as an organisation that processes personal data.

4.7 The Corporate Body will be designated at the Data Controller.

5. Lawful, fair and transparent processing

5.1 To ensure its processing of data is lawful, fair and transparent, the Corporate Body shall maintain a Register of Systems.

5.2 The Register of Systems shall be reviewed at least annually.

5.3 The Corporate Body will create a **Fair Processing Notice** and **Internal Fair Processing Notice** which will give full information about how and why personal data is being processed.

5.4 The Fair Processing Notice will be available to the public on The Corporate Body's Website.

5.5 All individuals who are having their personal data processed by the Corporate Body will be provided access to the Fair Processing Notices prior to the processing of their data.

5.6 All individuals have the right to be forgotten, with exceptions where limited personal data must be kept for statutory reasons.

5.7 Individuals have the right to access their personal data, and any such requests made to the Corporate Body shall be dealt with promptly, and within no more than 40 working days.

5.8 The Responsible Person will oversee the dealing of data access requests.

5.9 The Register of Systems will outline the procedure for dealing with such requests.

5.10 All Individual rights will be clearly indicated in the Fair Processing Notice.

5.11 The Register of Systems will demonstrate what procedures are in place to ensure those individuals having their data processed are informed about the Fair Processing Notice.

6. Lawful purposes

6.1 All data processed by the Corporate Body must be done on one of the following lawful bases: consent, contract, legal obligation, vital interests, public task or legitimate interests.

6.2 The Corporate Body shall note the appropriate lawful basis in the Register of Systems.

6.3 Where consent is relied upon as a lawful basis for processing data, evidence of opt-in consent shall be kept with the personal data.

6.4 Where communications are sent to individuals based on their consent, the option for the individual to revoke their consent should be clearly available, and systems should be in place to ensure such revocation is reflected accurately in the Corporate Body's systems.

7. Data minimisation

7.1 The Corporate Body shall ensure that personal data are adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed.

7.2 The Register of Systems will document the procedures that are in place to ensure that personal data are adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed.

8. Accuracy

8.1 The Corporate Body shall take reasonable steps to ensure personal data is accurate.

8.2 Where necessary for the lawful basis on which data is processed, steps shall be put in place to ensure that personal data is kept up to date.

8.3 The Register Systems will document processes to keep data up to date and measures for monitoring that these procedures are adhered to.

9. Risk Assessment

9.1 When carrying out Risk Assessments in line with The Corporate Body's Health and Safety Policy, there will be a provision to ensure that a **Data Protection Impact Assessment** is carried out to assess if there are any additional actions to be taken in relation to Personal Data.

10. Archiving / removal

10.1 To ensure that personal data is kept for no longer than necessary, the Corporate Body will put in place an archiving policy for each area in which personal data is processed and review this process annually.

10.2 The archiving policy shall consider what data should/must be retained, for how long, and why.

11. Security

11.1 The Corporate Body will ensure that Personal Data on paper is stored securely in locked storage.

11.2 The Corporate Body shall ensure that personal data in digital form is stored securely using modern software that is kept up-to-date.

11.3 Access to personal data shall be limited to personnel who need access, and appropriate security should be in place to avoid unauthorised sharing of information.

11.4 When personal data is deleted, this should be done safely such that the data is irrecoverable.

11.5 Appropriate back-up and disaster recovery solutions shall be in place.

11.6 The detailed security measures for each type of Data will be outlined in the Register of Systems.

12. Partners and contracted Data Processors

12.1 The Corporate Body will not share personal data with a third party without written consent from the data's owner to share with that specific third party.

12.2 The Corporate Body will ensure they have evidence of GDPR compliance from every organisation that Process Data on their behalf. (known as Data Processors).

12.3 A list of Data Processor Partners and evidence of their GDPR compliance will be kept in the Register of Systems.

13. Breach

13.1 In the event of a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data, the Corporate Body shall promptly assess the risk to people's rights and freedoms and if appropriate report this breach to the ICO within 72 hours of the breach discovery.

13.2 Any Breach or Potential Breach must be reported to the Responsible Person (CEO), and Chair of Colne Town Council within 12 hours of the breach discovery.

13.3 The Responsible Person will write a report documenting the breach and providing recommended actions. This report must be sent to the Chair of Colne Town Council within 24 hours of the breach discovery.

14. End of Policy