Chesham TOWN COUNCIL

DATA PROTECTION POLICY

Updated on the 13 March 2023
Next review by the 13 March 2024

1. INTRODUCTION

1.1. Chesham Town Council (the Council) are known as the Data Controller because it determines the purposes and means of the processing of personal data. The Council may also be a Data Processor, or may get other Data Processors to do this for the Council.

1.2. The Data Controller is the person responsible for ensuring that all personal data (any information relating to identified or identifiable natural, living persons), is processed lawfully in accordance with the UK General Data Protection Regulation (UK GDPR) and the Data Protection Act 2018 (DPA) (implementing the Law Enforcement Directive).

1.3. In order for the Council to provide services it must collect and use personal data about individuals. The Council collects personal data from a variety of individuals including current, past and prospective councillors, employees, consultants, agents, partners, suppliers, customers and others with whom the Council communicates. The Council regard the lawful and correct handling of personal data as essential to operating successfully. The Council considers it important that it maintains the confidence of its customers by keeping personal data secure.

1.4. The Council will ensure that personal information is dealt with properly and lawfully in compliance with the legislative requirements of the UK GDPR and the DPA, regardless of whether it is collected, recorded, and used in paper or electronic format.

2. SCOPE

2.1 Council employees will use this policy in conjunction with the Council's Data Protection procedures. This details the responsibilities, requirements and reporting procedures under the legislation.

2.2 In accordance with the requirements of the UK GDPR & the DPA, the Council are registered with the Information Commissioner's Office (ICO) for activities which involve processing personal data. The Council registration can be found on the ICO's register of Data Controllers. Any amendments are advised to the ICO as soon as they become apparent and registration is renewed annually.

2.3 The Council will adhere to the Data Protection Principles as required by the UK GDPR & DPA which require specifically that personal information/data is handled as set out in the seven data protection principles:

1. Personal information shall be processed lawfully, fairly and in a transparent manner (Lawfulness, Fairness and Transparency Principle)
2. Personal information must be collected for specified, explicit and legitimate purposes (Purpose Limitation Principle)
3. Personal information shall be adequate, relevant and limited to what is necessary (Data Minimisation Principle)
4. Personal information must be accurate and, where necessary, kept up to date (Accuracy Principle)

5. Personal information must be 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 (Storage Limitation Principle)
6. Personal information must be processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures (Integrity & Confidentiality Principle)
7. We are responsible for compliance with the principles and we must be able to demonstrate compliance with the principles. (Accountability Principle)

2.4 Failure to comply with UK GDPR's data protection principles could result in a breach of the Regulation and result in a financial penalty of up to €20,000,000 (approximately £17,000,000). Failure to comply with the Data Protection Policy and Procedure could result in disciplinary action for staff.

3. THE INFORMATION WE HOLD

3.1 The Council have conducted an information audit to identify the personal data that it collects and processes and how it flows into, through and out of the council. The audit is used to create an information asset register. As an organisation with less than 250 employees the Council keep records of any processing activities that:

- are not occasional
- could result in a risk to the rights and freedoms of individuals
- involve the processing of special categories of data or criminal conviction and offence data

3.2 As good practice, the Council also record the purposes for processing and retention schedules.

4. LAWFUL BASES FOR PROCESSING DATA

4.1 Before the Council process personal data, it must identify our lawful basis for doing so. When the lawful basis for processing data is **Consent,** the Council are committed to offering people genuine choice and control over how the Council uses their data. The Council's consent requests will:

- be kept separate from other terms and conditions
- require a positive opt-in
- not make consent a pre-condition of service
- provide the name of the council and any specific third-party organisations who will rely on this consent

The Council will:

- keep records of what an individual has consented to, including what the Council told them, and when and how they consented
- Tell individuals that they can withdraw consent at any time and how to do this

4.2 The Council are committed to keeping consent under review and refresh it if anything changes. The Council will record any changes.

5. COMMUNICATING WITH PEOPLE – THE RIGHT TO BE INFORMED

5.1 The Council understands that individuals need to know that their data is collected, why it is processed and who it is shared with. The Council will publish this information in a privacy notice on its web sites and within any forms or letters given to individuals. The information will be:

- concise, transparent, intelligible and easily accessible
- written in clear and plain language, particularly if addressed to a child
- free of charge

6. RIGHT OF ACCESS

6.1 People have the right to:

- obtain confirmation that their data is being processed
- access their personal data

6.2 The Council follow the Information Commissioner's Office's 'Subject Access Code of Practice' to identify and respond to subject access requests. However, the Council timeframe is in line with the General Data Protection Regulation:

6.3 Information must be provided without delay and at least within one calendar month of receipt of a subject access request. The Council can extend this period by a further two months for complex or numerous requests (in which case the person must be informed and given an explanation).

6.4 A calendar month ends on the corresponding date of the next month (e.g. 2 January to 2 February), unless that date does not exist in which case it is the last day of the next month (e.g. 31 January to 28 February).

6.5 This means that the legal deadline will vary from 28 days to 31 days depending on the month.

7. KEEPING DATA ACCURATE AND UP TO DATE

7.1 The Council respect that people have the right to have personal data rectified if it is inaccurate or incomplete and will respond to a request without delay (at least within one month of receipt). In some circumstances it may be necessary to extend this period by a further two months for complex or numerous requests (in which case the individual must be informed and given an explanation). If the Council have disclosed the personal data to a data processor (third party) it will inform them of the rectification where possible.

7.2 As part of the Councils annual review of its information asset register, it will review the information it processes or stores to identify when to do things like correct inaccurate records. Records management policies, with rules for creating and keeping records (including emails) will help with this.

7.3 If the Council identify any data accuracy issues, it is committed to communicating lessons learned to staff through ongoing awareness raising and internal training.

8. DISPOSING OF PERSONAL DATA

8.1 The Council will securely dispose of personal data for the following reasons:

- it is no longer required for the purpose for which it was originally collected/processed
- when the person withdraws consent
- when the person objects to the processing and there is no overriding legitimate interest for continuing with the processing
- if the data was unlawfully processed
- it has to be erased to comply with a legal obligation

8.2 There are occasions when the Council can refuse to delete personal information; please refer to the ICO web site for guidance.

8.3 A retention schedule is included within the Council information asset register to remind us when to dispose of different categories of data. The schedule will be reviewed annually to ensure that it continues to meet Council and statutory requirements.

9. RESTRICTIONS ON DATA PROCESSING

9.1 People have a right to block or restrict the processing of personal data. In these situations, the Council can store the personal data, but not carry out any further processing of it. The Council can retain just enough information about the person to ensure that the restriction is respected in the future. Processing restrictions to personal data are required in the following circumstances:

- Where a person contests the accuracy of the personal data, the Council will restrict the processing until it has verified the accuracy of the personal data.
- Where a person has objected to the processing (where it was necessary for the performance of a public interest task or purpose of legitimate interests), and the Council are considering whether our businesses legitimate grounds override those of the individual.
- When processing is unlawful and the person opposes erasure and requests restriction instead.
- If the Council no longer need the personal data but the person requires the data to be retained to allow them to establish, exercise or defend a legal claim.

9.2 If the Council have disclosed the personal data in question to third parties, it will inform them about the restriction on the processing of the personal data, unless it is impossible or involves disproportionate effort to do so.

9.3 The Council will inform individuals when we decide to lift a restriction on processing.

10. OBJECTING TO PROCESSING

10.1 The Council understand that people have the right to object to the following:

- Processing their personal data based on legitimate interests or the performance of a task in the public interest/exercise of official authority (including profiling)
- Processing for purposes of scientific/historical research and statistics.

10.2 The Council will stop the processing in response to an objection unless:

- The Council can demonstrate compelling legitimate grounds for the processing, which override the interests, rights and freedoms of the individual.
- The processing is for the establishment, exercise or defence of legal claims.

10.3 People can also object to any processing undertaken for direct marketing (including profiling). The Council will stop processing for direct marketing as soon as it receives an objection. The Council will inform individuals of their right to object "at the point of first communication" and clearly lay this out in privacy notices.

11. DATA PORTABILITY

11.1 If the Council processes data by automated means, people are allowed to receive that personal data, or have it moved, copied or transferred to a business in a safe and secure way. However, this only applies to:

- Automatically processed data which is also
- Personal data that an individual has provided to the Council
- Where processing is based on consent, or for the performance of a contract

11.2 Where the above conditions apply, the information will be provided without delay and at least within one month of receipt. The Council can extend this period by a further two months for complex or numerous requests (in which case the individual will be informed and given an explanation).

11.3 The Council will provide the personal data in a structured, commonly used and machine-readable format, e.g. XML files.

11.4 The information will be provided free of charge and if requested by the individual, the Council can transmit the data directly to another business where this is technically feasible.

12. AUTOMATED DECISION MAKING

12.1 At this time, the Council does not carry out processing that could be constituted as automated decision making. Should this change, the Council will review this policy to ensure that the required safeguards are put in place to prevent any potentially damaging decisions being taken without human intervention.

13. Working with Data Processors

13.1 The Council will put a written contract in place with any processors that it works with.

13.2 The Council understands that it is liable for our processors' compliance with the GDPR and must only appoint processors who can provide 'sufficient guarantees' that the requirements of the GDPR will be met and the rights of data subjects protected.

14. INFORMATION RISKS

14.1 The Chief Executive Officer has overall responsibility for managing information risks, coordinating procedures put in place to mitigate them and for logging and risk assessing information assets.

14.2 If an information risk is identified, the Council will put in place an appropriate action plan to mitigate any risks that are not tolerated or terminated.

15. DATA PROTECTION BY DESIGN AND DEFAULT

15.1 The Council have a general obligation to implement appropriate technical and organisational measures to show that it has considered and integrated data protection into our processing activities. The Council will adopt internal policies and implement measures which help the Council to comply with the data protection principles.

16. DATA PROTECTION IMPACT ASSESSMENTS (DPIAs)

16.1 The Council will undertake DPIAs before processing any data of such a nature that this assessment is required.

17 SECURITY POLICY

17.1 The Council's Information Security Policy is contained within its IT policy. This is based on the risks to the personal data that it holds and security measures that are appropriate to its needs.

18. INTERNATIONAL TRANSFERS

18.1 The Council are committed to ensuring an adequate level of protection for any personal data processed by others on our behalf that is transferred outside the European Economic Area.

19. DATA BREACHES

19.1 A data breach is a breach of security leading to the destruction, loss, alternation, unauthorised disclosure of, or access to, personal data.

19.2 The Council have an internal breach reporting procedure to identify, report, manage and resolve any personal data breaches. The Council will adhere to the Information Commissions' Office (ICO) guidelines to identify which data breaches should be reported to the ICO, and to the individuals affected.

19.3 The Council will maintain records of personal data breaches, whether or not they are notifiable to the ICO. A notifiable breach will be reported to the ICO within 72 hours of the Council becoming aware of it.

20. ROLES AND RESPONSIBILITIES

20.1 Overall responsibility for Data Protection compliance lies with the Chief Executive Officer. Each Head of Department is responsible for Data Protection compliance within their department and shall work with Service Managers to ensure compliance. Compliance will be monitored by a Data Protection consultant. The consultant will:

- Inform and advise the Council and its officers about their obligations to comply with the GDPR and other data protection laws.
- Monitor compliance with the GDPR and other data protection laws, including managing internal data protection activities, training staff and conducting internal audits.
- Be the first point of contact for supervisory authorities and for individuals whose data is processed (employees, service users, etc).

21. PROCEDURES

21.1. Individual procedures will be put in place for each area of the Council to ensure that data is being correctly processed.

22. COMPLIANCE

22.1 Failure to comply with this policy will result in disciplinary action being taken in line with the council's Disciplinary Procedure.