DATA PROTECTION POLICY
October 2023

Contents

1 Aims

Corsham Town Council is committed to ensuring that all personal data collected is processed in accordance with all relevant data protection laws including the UK General Data Protection Regulation (GDPR) and the Data Protection Act 2018 (DPA 2018).
The lawful basis of processing will be with the consent of the data subject, necessary for compliance with a legal obligation, or necessary for the legitimate interests of the Town Council. Further information regarding the legal basis is in section 9.
The Town Council is registered as a data controller with the Information Commissioner with the identifying reference Z1248459.

The details of the Town Council's Data Protection Officer can be found in section 6.

2 Scope

This policy applies to anyone who uses council controlled data in any format including those who have access to and/or is a user of Town Council ICT systems, both in and out of the Town Council, including staff, Councillors, volunteers and contractors.

This policy applies to all personal data, regardless of whether it is in paper or electronic format.

In order to conduct its business, services and duties, Corsham Town Council processes a wide range of personal data and non-personal data relating to its own operations and some which it handles on behalf of partners. In broad terms, this data can be classified as:

- Confidential information about other organisations because of commercial sensitivity.
- Personal data concerning current, past and potential employees, Councillors and volunteers.
- Personal data concerning individuals who contact the Town Council for information, to access its services or facilities or to make a complaint.
- Data shared in the public arena about the services the Town Council offers, its mode of operations and other information it is required to make available to the public.
- Confidential information and data not yet in the public arena such as ideas or policies that are being progressed.

Corsham Town Council will adopt procedures, and manage responsibly, all data which it handles and will respect the confidentiality of both its own data, that belonging to partner organisations it works with and members of the public. In some cases it will have contractual obligations towards confidential data but, in addition, will have specific legal responsibilities for personal and sensitive information under data protection legislation.

The Council will be as transparent as possible about its operations and will work closely with public, community and voluntary organisations. Therefore, in the case of all information which is not personal or confidential, it will be prepared to make it available to partners and members of the town's communities. Details of information which is routinely available is contained in the Council's Publication Scheme which is based on the statutory model publication scheme for local councils.

Children

We will not process any data relating to a child (under 13) without the express parental/guardian consent of the child concerned, or where we are lawfully obliged to do so.

3 Distribution

This policy is available on the Town Council website and in hard copy from the Town Council office.

To comply with the fair processing requirements of the UK GDPR, the Town Council informs its staff, Councillors, volunteers, contractors, and other community users of the data it collects, processes and holds, the purposes for which the data is held, and any third parties to whom it may be passed. This information forms part of the Privacy Notice which is available on the main Town Council website.

A hard copy of the Privacy Notice is available from the Town Council office. Privacy Notices are reviewed at least annually, and any significant changes will be publicised.

4 Definitions

Personal data - Any combination of data items which could identify a living person and provide specific information about them, their families, or circumstances. The term covers both facts and opinions about an individual. The Town Council may process a wide range of personal data of staff (including councillors and volunteers) and residents as part of its operation.

This personal data may include (but is not limited to):

- names and addresses (including email addresses)
- date of birth
- photo
- bank details
- references
- employment history
- taxation and national insurance records
- appraisal records
- bookings (cemeteries, halls etc)
- complaints
- posts on social media networking sites
- Computer IP address

Special category personal data - Personal data which is more sensitive and so needs more protection, including information about a living individual's:

- Racial or ethnic origin
- Political opinions
- Religious or philosophical beliefs
- Trade union membership
- Genetics
- Biometrics (such as fingerprints, retina and iris patterns), where used for identification purposes
- Health – physical or mental
- Sex life or sexual orientation

Criminal records are treated in much the same way as other special category data.

Processing - Anything done to personal data such as obtaining, recording, or holding the information or data or carrying out any operation or set of operations on the information or data, including:

- collecting, organising, structuring, storing, adapting, altering, retrieving, using, erasing, or destroying.
- disclosing the information or data by transmission, dissemination or otherwise making it available.

Processing can be automated or manual.

Data subject - The identified or identifiable (living) individual whose personal data is held or processed. That may be an employee, prospective employee, associate or prospective associate of Corsham Town Council or someone transacting with it in some way, or an employee, Councillor, or volunteer with one of our customers, or persons transacting or contracting with one of our customers when we process data for them.

Data controller - a person who (either alone or jointly or in common with other persons) (e.g. Town Council, employer, other council) determines the purposes for which, and the manner in which, any personal data is to be processed.

Data processor - A person or other body, other than an employee of the data controller, who processes personal data on behalf of the data controller.

Personal data breach - A breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data.

5 Roles and Responsibilities

This policy applies to all staff (including volunteers and Councillors) who work at the Town Council, and to external organisations or individuals working on its behalf.

Councillors - Councillors have overall responsibility for ensuring that the Town Council complies with all relevant data protection obligations.

Chief Executive - The Chief Executive acts with the delegated authority of the full Council on a day-to-day basis and will liaise with the DPO. In the Chief Executive's absence, in case of emergency, this role will be delegated to the Head of Finance and Administration.

All staff - All staff are responsible for:

- Familiarising themselves with and complying with this policy and acceptable use policies for staff; The learning culture within the organisation seeks the avoidance of a blame culture and is key to allowing individuals the confidence to report genuine mistakes. However, staff should be aware, that a deliberate or reckless disregard of this policy could result in disciplinary action being taken.
- Taking care to ensure the safe keeping of personal data, minimising the risk of its loss or misuse at all times. All staff should adopt the approach that they should treat the personal data of others with the same care with which they would treat their own.
- Using personal data only on secure password protected computers and other devices, ensuring that they are properly "logged-off" at the end of any session in which they are using personal data.
- Storing, transporting and transferring data using encryption and secure password protected devices.
- Not transferring personal data offsite or to personal devices

- Deleting data in line with this policy and the retention schedule
- Informing the Town Council of any changes to their personal data, such as a change of address
- Reporting to the Chief Executive, or in their absence the DPO in the following circumstances:
    - Any questions about the operation of this policy, data protection law, retaining or sharing personal data or keeping personal data secure.
    - If they have any concerns that this policy is not being followed.
    - If they are unsure whether they have a lawful basis upon which to use personal data in a particular way.
    - If they need to rely on or capture consent, deal with data protection rights invoked by an individual, or transfer personal data outside the European Economic Area.
    - The discovery of a data breach or near miss (immediate action is required) – please refer to the Data Breach Policy and section 12 of this policy.
    - Whenever they are engaging in a new activity that may affect the privacy rights of individuals.
    - If they are to share personal data with a data processor, for example a contractor or someone offering a service, in which case a contract is likely to likely to be required please see - *Sharing Personal Data* (section 10)

6 Data Protection Officer (DPO)

The Data Protection Officer (DPO) is responsible for advising on the implementation of this policy, monitoring compliance with data protection law, providing support and developing related policies and guidelines where applicable, in amongst other data protection related functions. They will provide an annual report on compliance directly to the Council and, where relevant, provide the Town Council with advice and recommendations on data protection issues.

The Town Council has appointed i-West as its DPO, and they can be contacted by email at

Email: i-west@bathnes.gov.uk.

Telephone: 01225 395959

One West
Bath and North East Somerset Council
Guildhall
High Street
Bath
BA1 5AW

Under usual circumstances the Chief Executive or Head of Finance and Administration will be the point of contact with the DPO.

7 Subject Access Requests and Other Rights of Individuals

In all aspects of its work, the Town Council will ensure that the rights of the data subject are protected by all practicable measures associated with the conduct of the Town Council's work. Subject to exceptions, the rights of the data subject as defined in law are:

a) The Right to be informed.

The Town Council advises individuals how it will use their data through the use of transparent Privacy Notices and other documentation such as consent forms where appropriate.

b) The Right of access

An individual when making a subject access request (SAR) is entitled to the following:

i. confirmation that their data is being processed.
ii. access to their personal data.
iii. other supplementary information – this largely corresponds to the information that should be provided in a Privacy Notice.

The Town Council must respond to such a request within 30 days unless the request is complex, in which case it may be extended by a further 60 days. Please refer to the Subject Access Request Policy for further details as to how to manage a subject access request.

c) The Right to rectification

Individuals have the right to ask to rectify information that they think is inaccurate or incomplete. The Town Council has a duty to investigate any such claims and rectify the information where appropriate within 30 days, unless an extension of up to a further 60 days can be justified.

d) The Right to erasure

The right for an individual to request that their data is erased is not absolute. It applies where:

- the information was given voluntarily, consent is now withdrawn and no other legal basis for retaining the information applies.
- the information is no longer required by the Town Council.
- a legal obligation to erase the data applies.
- the data was collected from a child for an online service.
- the Town Council has processed the data on the basis that it is in their legitimate business interests to do so, and having conducted a legitimate interests test, it concludes that the rights of the individual to have the data erased outweigh those of the Town Council to continue to process it.

e) The Right to restrict processing

An individual may ask the Town Council to temporarily limit the use of their data when it is considering:

- a challenge made to the accuracy of their data, or
- an objection to the use of their data.

In addition, the Town Council may be asked to limit the use of data rather than delete it, if the individual does not want the Town Council to delete the data but does not wish to it continue to use it, in the event that the data was processed without a lawful basis or to create, exercise or defend legal claims:

f) The Right to data portability

An individual can make a request in relation to data which is held electronically for it to be transferred to another organisation or to themselves where they have provided it either directly or through monitoring activities eg apps. The Town Council only has to provide the information where electronically feasible.

g) The Right to object

Individuals have a right to object in relation to the processing of data for

- a task carried out in the public interest
- a task carried out in its legitimate interests
- scientific or historical research, or statistical purposes, or
- direct marketing.

h) The right to withdraw consent to processing

i) *Rights related to automated decision making* (This does not apply as the Town Council does not employ automated decision-making processes).

8 Data Protection Principles

The GDPR is based on 7 key data protection principles that the Town Council complies with.

The principles say that personal data must be:

- **Processed lawfully, fairly and in a transparent manner** – the Town Council will explain to individuals why the Town Council needs their data and why it is processing it – for example on consent forms (where consent is used as the basis for processing), and in its Privacy Notice(s). The Town Council reviews its documentation and the basis for processing data on a regular basis.

- **Collected for specified, explicit and legitimate purposes** – the Town Council explains these reasons to the individuals concerned when it first collects their data. If the Town Council wishes to use personal data for reasons other than those given when the data was first obtained, it will inform the individuals concerned before doing so, and will seek consent where necessary and appropriate unless the new purpose is compatible with that in respect of which consent was given, or there is another lawful basis for sharing the information/ The Town Council will document the basis for processing. For special categories of personal data, it will also meet one of the special category conditions for processing which are set out in the GDPR and Data Protection Act 2018.

- **Adequate, relevant, and limited to what is necessary to fulfil the purposes for which it is processed -** the Town Council must only process the minimum amount of personal data that is necessary in order to undertake its work.

- **Accurate and, where necessary, kept up to date** – the Town Council will check the details of those on its databases at appropriate intervals and maintain the databases. It will consider and respond to requests for inaccurate data to be rectified in accordance with the Data Protection Act 2018.

- **Kept for no longer than is necessary for the purposes for which it is processed** – when the Town Council no longer needs the personal data it holds, it will ensure that it is deleted or anonymised in accordance with the retention schedule.

- **Processed in a way that ensures it is appropriately secure** – the Town Council implements appropriate technical measures to ensure the security of data and systems for staff and all users. Please refer to the Information Security Policy for further information which incorporates principles around bringing your own device and how data is securely transferred in and out of the Town Council's system.

- **Accountability –** The Town Council complies with its obligations under data protection laws including the GDPR and can demonstrate this via the measures set out in this policy, including:

    - Completing Data Protection Impact Assessments (DPIAs) where the Town Council's processing of personal data presents a high risk to rights and freedoms of individuals, and when introducing new technologies. This largely involves special category personal data and CCTV. However, the Town Council will liaise with the DPO who will advise on this process. Any activity involving the processing of personal data must be registered on the Register of Processing Activity and reviewed, at the very least, annually.
    - Integrating data protection into internal documents including this policy, any related policies and Privacy Notices.
    - Regularly training members of staff on data protection law, this policy, any related policies and any other data protection matters; the Town Council also maintains a record of attendance.
    - Regularly conducting reviews and audits to test its privacy measures and ensure compliance with relevant legislation and Town Council policies.
    - Maintaining records of its processing activities for all personal data that it holds.

9 Processing Personal Data

In order to ensure that the Town Council's processing of personal data is lawful; it will always identify one of the following six grounds for processing **before** starting the processing:

- The data needs to be processed so that the Town Council can fulfil a **contract** with the individual, or the individual has asked the Town Council to take specific steps before entering into a contract;

- The data needs to be processed so that the Town Council can comply with a **legal obligation;**

- The data needs to be processed to ensure the **vital interests** of the individual e.g. to protect someone's life;

- The data needs to be processed so that the Town Council, as a public authority, can **perform a task in the public interest, and carry out its official functions**;

- The data needs to be processed for the **legitimate interests** of the Town Council or a third party where necessary, balancing the rights of freedoms of the individual). However, where the Town Council can use the public task basis for processing, it will do so rather than rely on legitimate interests as the basis for processing.

- The individual has freely given clear consent. In the case of **special categories of personal data**, this must be **explicit consent.** For processing special categories of personal data an additional lawful basis is needed – these are detailed in the Special Categories of Personal Data Policy

10 Sharing Personal Data

Please refer to the Town Council's Privacy Notices.

- The Town Council will only share personal data under limited circumstances, when there is a lawful basis to do so and where identified in the Privacy Notice(s). The following principles apply:
    - The Town Council will share data if there is an issue that puts the safety of staff at risk;
    - The Town Council will share data where there is a need to liaise with other agencies. It will seek consent as necessary and appropriate before doing so. However, where safeguarding concerns apply, it will apply the **Seven Key Data Protection Principles** (see section 8) which provide that in limited circumstances data may be shared with external agencies without the knowledge or consent of the individual;
    - The Town Council's suppliers and contractors need data to provide services – for example, IT companies. When sharing data, the Town Council will:
        - Only appoint suppliers or contractors which can provide sufficient guarantees that they comply with data protection law;
        - Establish a data processing contract with the supplier or contractor, either in the contract or as a standalone agreement, to ensure the fair and lawful processing of any personal data it shares where there is regular sharing;
        - Only share data that the supplier or contractor needs to carry out their service, and information necessary to keep them safe while working with the Town Council.
- The Town Council may also share personal data with law enforcement and government bodies where there is a lawful requirement / basis for us to do so, including:
    - For the prevention or detection of crime and/or fraud;
    - For the apprehension or prosecution of offenders;
    - For the assessment or collection of tax owed to HMRC;
    - In connection with legal proceedings;
    - For research and statistical purposes, as long as personal data is sufficiently anonymised, or consent has been provided.
- The Town Council may also share personal data with emergency services and local authorities to help them to respond to an emergency situation that affects Councillors or staff.

11 Data Protection by Design and Default

The Town Council has a legal obligation to integrate appropriate technical and organisational measures into all of its processing activities, and to consider this aspect before embarking on any new type of processing activity.

It is a statutory requirement that any activity involving a high risk to the data protection rights of the individual when processing personal data be assessed by the Data Protection Impact

Assessment. Prior to the assumption of any such activity One-West must be consulted and an initial screening be conducted assessing risk.

Please refer to the Information Security Policy for further detail as to how the Town Council implements this principle in practice.

12 Personal data breaches or near misses

A personal data breach is defined as *"a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed in connection with the provision of a public electronic communications service."* It may be deliberate or accidental.

Wherever it is believed that a security incident has occurred or a 'near miss' has occurred, the staff member must inform the Chief Executive and DPO **immediately** in order that an assessment can be made as to whether the ICO should be informed within 72 hours as is legally required, and / or those data subjects affected by the breach. The learning culture within the organisation seeks the avoidance of a blame culture and is key to allowing individuals the confidence to report genuine mistakes.

Further details on security incidents and data breaches can be found in the Data Breach Policy.

13 Destruction of records

We apply our retention policy and will permanently destroy both paper and electronic records securely in accordance with these timeframes.

We will securely destroy hard copies and will ensure that any third party who is employed to perform this function will have the necessary accreditations and safeguards.

If we delete electronic records and our intention is to put them beyond use, although it may be technically possible to retrieve them, we follow the Information Commissioner's Code of Practice on deleting data and this information will not be made available on receipt of a subject access request.

14 Training

To meet our obligations under Data Protection legislation, we ensure that all staff, volunteers, and Councillors receive an appropriate level of data protection training as part of their induction. Those who have a need for additional training will be provided with it, for example relating to use of systems or as appropriate.

Data protection also forms part of continuing professional development, and updates will be provided where changes to legislation, guidance or the Town Council's processes make it necessary.

15 Monitoring Arrangements

Whilst the DPO is responsible for advising on the implementation of this policy and monitoring the Town Council's overall compliance with data protection law, the Town Council is responsible for the day-to-day implementation of the policy and for making the data protection officer aware of relevant issues which may affect the Town Council's ability to comply with this policy and the legislation.

This policy will be reviewed annually, unless an incident or change to regulations dictates a sooner review.

16 Complaints

The Town Council seeks to implement best practice, strives for the highest standards, and ensures that data subjects are aware of their rights and have easy access to that information on request. The Town Council operates an "open door" policy to discuss any concerns about the implementation of this policy or related issues. The Town Council's complaints policy may be found on its website.

You have a right to make a complaint to the Information Commissioner's Office (ICO), but under most circumstances the ICO would encourage the complainant to raise the issues in the first instance with the Town Council or via the Town Council's DPO (details in section 6).

The ICO is contactable at;

Wycliffe House,
Water Lane,
Wilmslow,
Cheshire,
SK9 5AF.
casework@ico.org.uk
Telephone: 0303 123 1113.

17 Legislation and Guidance

This policy takes into account the following:

- The General Data Protection Regulation (GDPR) 2016
- The Data Protection Act (DPA) 2018.
- The Protection of Freedoms Act 2012
- Guidance published by the Information Commissioner's Office

18 Links with Other Policies

This Data Protection Policy is linked to the following:

- Information Security Policy
- Retention of Records Policy
- Data Breach Policy
- Management of Transferable Data Policy
- Special Categories of Personal Data Policy
- Privacy Notices
- Consent / Permissions Form

Who is responsible for protecting a person's personal data?

The Town Council, as a corporate body, has ultimate responsibility for ensuring compliance with the Data Protection legislation. The Town Council has delegated this responsibility day to day to the Chief Executive.

- Email: dmartin@corsham.gov.uk
- Phone: 01249 702130
- Correspondence: David Martin, Chief Executive, Corsham Town Council, High Street, Corsham, Wiltshire SN13 0EZ

The Town Council has also appointed an external Data Protection Officer to ensure compliance with Data Protection legislation who may be contacted at: i-west@bathnes.gov.uk

Date: October 2023

File: GDPR policies and forms – CTC GDPR policies