DATA PROTECTION POLICY

Background and purpose

Lawful basis: In the course of its activities, Cranbrook Town Council (CTC) needs to collect information (data) about the people it serves and those with whom it deals in order to provide its services. Such information (data) may include names, addresses, email addresses, dates of birth, private and confidential information and sensitive information.

Legal framework: The General Data Protection Regulations GDPR 2018 set out the legal framework within which organisations who are controllers of personal data must operate, whether that data is held in manual or computerised formats. Organisations are legally obliged to protect any personal data they hold.

Town and Parish Councils are required to notify and register their status as data controllers with the Information Commissioner's Office, which maintains a public register of data controllers. Although District and County Councillors are required to register as individuals with the ICO, Town Councillors are not required to do so in their own right and are covered by the Town Council's notification.

New legislation

The GDPR applies to 'personal data' and the, GDPR's definition is more detailed and makes it clear that information such as an online identifier (e.g. an IP address) can be personal data. Its more expansive definition provides for a wide range of personal identifiers to constitute personal data, reflecting changes in technology and the way organisations collect information about people.

The GDPR applies to both automated personal data and to manual filing systems where personal data are accessible according to specific criteria. This is wider than the DPA's definition and could include chronologically ordered sets of manual records containing personal data.

Personal data that has been anonymised can fall within the scope of the GDPR depending on how difficult it is to attribute the record to a particular individual.

The GDPR places greater emphasis on the documentation that data controllers must keep demonstrating their accountability.

In most cases organisations will not be able to charge for complying with a Request and will have a month to comply, rather than the current 40 days.

Organisations will also have to explain their lawful basis for processing personal data in their privacy notice and when they answer a subject access request. They must also ensure they have the right procedures in place to detect, report and investigate a personal data breach.

The GDPR sets a high standard for consent. Consent means offering people genuine choice and control over how their data is used. When consent is used properly, it helps organisations build trust and enhances reputations.

Information covered and relevant definitions

The GDPA defines "personal data" as any information relating to an identified or identifiable natural person (‘data subject’); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person”.

Regardless of the way it is collected, recorded and used (i.e. whether held on computer or other digital media, on paper or as an image, including CCTV) this personal information must be dealt with correctly to ensure compliance with the GDPR. Some of the personal data processed can be more sensitive in nature and therefore requires a higher level of protection. The GDPR refers to the processing of these data as ‘special categories of personal data’. This means personal data about an individual’s:

- race;
- ethnic origin;
- political opinions;
- religious or philosophical beliefs;
- trade union membership;
- genetic data;
- biometric data (where this is used for identification purposes);
- health data;
- sex life; or
- sexual orientation.
- Personal data can include information relating to criminal convictions and offences. This also requires a higher level of protection.

The Freedom of Information Act 2000 (FOI) created a new category of data which extended the definition of “data” in the GDPR to include any information held by a public authority which would not otherwise be caught by the definition. Where, however, information requested under the FOI Act includes information about identifiable individuals, public authorities must consider whether its release would breach the GDPR. The new category of data (often referred to as ‘category [e] data’)

is designed to ensure that before releasing any personal information under the FOI Act, public authorities consider whether this would be fair. Processing category [e] data is exempt from most of the rights and duties created by the GDPR.

Scope

This policy applies to all paid Cranbrook Town Council employees, to its members (Councillors), to any person contracted to carry out services on behalf of CTC and to any intern or volunteer requested to carry out activities on behalf of CTC.

Principles of operation

CTC supports and will seek at all times, to comply with the 8 principles of the GDPR summarised below:

1. Personal data shall be processed fairly and lawfully.

2. Personal data shall be obtained/processed for specific lawful purposes.

3. Personal data held must be adequate, relevant and not excessive.

4. Personal data must be accurate and kept up to date.

5. Personal data shall not be kept for longer than necessary.

6. Personal data shall be processed in accordance with rights of data subjects (the people it relates to).

7. Personal data must be kept secure.

8. Personal data shall not be transferred outside the European Economic Area (EEA) unless there is adequate protection.

Roles and responsibilities

CTC will:

i) Ensure it is registered with the Information Commissioner's Office (ICO) as a Data Controller and that there is always one person with overall responsibility for data protection. Currently this person is the Town Clerk and Responsible Financial Officer.

ii) Provide general awareness information for all staff and specific training for staff handling personal information or involved in relevant activities, ensuring they have access to further guidance, support and supervision.

iii) At the point of awarding a contract, satisfy itself that the company/provider has a suitable Data Protection policy in place and request to see this.

iv) Explain, wherever appropriate, that personal information collected will be held in accordance with the GDPR.

v) Ensure adequate security measures are in place to protect personal data.

vi) Review, revise and update this document on a regular basis, in line with current legislation and good practice and in response to any issues which arise between reviews.

Employees will:

i) Observe all forms of guidance, codes of practice and procedures provided regarding the collection and use of personal information.

ii) Collect and process only appropriate information and then only in accordance with the purposes for which it is to be used by CTC to meet its service needs or legal requirements.

iii) Ensure information is destroyed (in accordance with the provisions of the GDPR) when no longer required, seeking guidance from the Town Clerk before doing so.

iv) On receipt of a request by or on behalf of an individual for information held about them, immediately notify their line manager/the Town Clerk.

v) Not send any personal information outside of the United Kingdom unless there is adequate protection and this has been authorised by the Town Clerk.

Links to other policies

This policy should be read in conjunction with the employee's contract of employment and with other relevant policies such as the Equality & Diversity Policy, Customer Service Policy and Complaints Procedure, Publication Scheme and Social Media Policy.

Useful external links

Information Commissioners Office website: https://ico.org.uk/
The governments guide to the General Data Protection Regulation:
https://www.gov.uk/government/publications/guide-to-the-general-data-protection-regulation

Cranbrook Town Council

Date of Approval: 13/05/2019
Date of Review: May 2023

General Privacy Notice

1) Who are we? Cranbrook Town Council acts as '*data controller'* for any personal data you provide to us. That means we will ensure the data you give us is processed in line with our organisation's policies and with your rights under data protection law including the General Data Protection Regulations, Data Protection Act 2018.

If you have any queries about this Privacy Notice or the personal data we hold about you, please contact our Town Clerk at clerk@cranbrooktowncouncil.gov.uk or 01404 514552 or by post to Cranbrook Town Council office, Younghayes Centre, 169 Younghayes Rd Cranbrook, EX5 7DR.

Our Privacy Notice will be regularly reviewed, and we will post updated versions on our website at https://www.cranbrooktowncouncil.gov.uk/governance/

2) What do we mean by 'data' and why is it important? *Personal data* is any information about a living individual which means they can be identified from that data (for example a name, photographs, videos, email or postal address). It can be identification directly from the data itself or indirectly, gained by combining partially anonymised information with other information which can identify an individual. (For example, although a staff list might only use ID numbers, if a separate list of ID numbers gives corresponding names identifying staff in the first list, the first list will also be treated as personal data).

Personal data includes names, titles, aliases, photographs, images, contact details such as phone numbers, addresses and email addresses. If relevant to the services provided by us and or where you provide information to us, we may process information such as your gender, age, marital status, nationality, education/work history, academic/professional qualifications, hobbies, family composition, and dependants. Where you pay for activities such as use of a council hall or facility, financial identifiers such as bank account numbers, payment card numbers, payment/transaction identifiers, policy numbers and claim numbers may also be processed. Our processing may also include the use of CCTV systems for the prevention and prosecution of crime.

Certain information, such as criminal convictions, racial or ethnic origin, mental and physical health, details of injuries, medication/treatment received, political beliefs, trade union affiliation, genetic data, biometric data and data concerning sexual life or orientation is known as *Sensitive personal data* and is a special category of data which can only be processed in certain circumstances.

The processing of personal data is governed by legislation which applies in the United Kingdom which includes the General Data Protection Regulation (the GDPR) and other legislation relating to personal data and rights, such as the Human Rights Act.

3) Why are we collecting your personal data? We collect this to help us respond to your request or enquiry when you communicate with us. We should always have a lawful basis for the processing your personal data. Usually this will be with your consent and for a specific purpose. For example, we may hold contact details

including name, telephone number(s), email address(es) and postal address(es) for the purposes of liaising with you about information or services you have requested and for invoicing and record keeping. Or it may be because there is a contract between us. We may also do so if the processing of your data is necessary for us to perform a task which is in the public interest and which has a clear basis in law, or if we have an obligation to process it to comply with the law, or if it is a vital interest (where processing is necessary to protect someone's life). [Legitimate interests for processing do not apply, as we are a public authority.] If we collect personal data for one reason, we will not use it for a different purpose without your consent (unless there is a legal basis for doing so).

Please note that if you choose not to provide your personal data or decide to withdraw your consent for us to use it, we may not be able to effectively respond to your request.

4) How do we hold and use (process) your data? Personal data is always stored securely. Our IT systems are robust and we will ensure appropriate technical and security measures are in place to protect your personal data from loss, misuse, unauthorised access or disclosure. Please see also sections **3)**, **5)** and **7)**.

5) Who do we share your personal data with? In some circumstances, so we can respond to your request or query, it may be necessary for us to share your name and other identifying information with other services or organisations, but we will not share your personal data outside our organisation unless we have a lawful reason to do so and we will aim to explain when we need to do this, ensuring we have your consent if that is necessary. [We do not currently transfer data outside the European Economic Area (EAA) but please be aware our website is accessible from overseas, so any data which is publicly visible (such as your picture in a news item) may be viewed overseas.]

6) What do we mean by 'other organisations' (data controllers)? These are other organisations we need to work with to provide services to you or to respond to your enquiry. For example, you contact us to ask us to investigate a faulty streetlamp and we need to contact the developer to do this, or you report a piece of damaged play equipment and we need to pass this to the organisation responsible for playground maintenance. In such cases, we may also need to retain your details, so we can provide an update if you have requested this. We will only, however, share the information which is needed by the other organisation and will explain when we are doing so. If we and the other data controller are processing your data jointly for the same purposes, we would be acting as joint data controllers which means we are all collectively responsible to you for your data. If the organisations are processing your data for their own independent purposes then each one will be independently responsible to you and if you have any questions, wish to exercise any of your rights or wish to raise a complaint, you should do so directly with the data controller of that organisation.

7) How long will we hold your personal data? We will keep your personal data only for as long as is necessary and in line with good practice. We will keep some records permanently if legally required to do so. We may keep other records for an extended period. For example, it is currently good practice to keep financial records for a period of 8 years to comply with HMRC (Her Majesty's Revenue & Customs)

requests. As a public authority we may have other legal obligations to retain some data and are allowed to do so to defend or pursue claims (various time limits apply). In general, we aim to keep data only for as long as we need it. This means it will be deleted when it is no longer needed.

8) Correspondence with councillors Any personal information shared with councillors will be used for the purpose intended by you only. Councillors do not store personal information for longer than necessary to carry out that purpose and will only share your information with the appropriate bodies as instructed by you. Should you wish to remove your consent at any point please inform both the councillor in question and also Cranbrook Town Council as per the contact details contained in this Privacy Notice.

9) Your rights Under the General Data Protection Regulations, Data Protection Act 2018 you have the right to: access to your own personal data, request amendments (if there are errors) or deletion (removal) of your personal data under certain circumstances, object to the processing of your personal data, request a copy of the information you provided to us in machine readable format or withdraw your consent to any processing which relies purely on your consent. If any of these apply, please contact our Town Clerk in the first instance using the contact details in section **1)**.

10) Your right to complain If you wish to complain about the way we have handled your personal data, please write to the Town Clerk in the first instance, clearly outlining your case. Your complaint will then be investigated in accordance with the Council's procedure. If you are still unhappy about the way your data has been handled, you can refer the matter to the Information Commissioner's Office at: Wycliffe House, Water Lane, Wilmslow, Cheshire, SK9 5AF, Email: casework@ico.org.uk or Tel: 0303 123 1113.

April 2019

Cranbrook Town Council

Date of Approval: 13/05/2019
Date of Review: May 2023