HONITON TOWN COUNCIL DATA PROTECTION POLICY

Purpose

The council is committed to being transparent about how it collects and uses the personal data of individuals, and to meeting our data protection obligations. This policy sets out the council's commitment to data protection, and individual's information rights and obligations in relation to personal data in line with the UK Data Protection Law which includes but may not be limited to the UK General Data Protection Regulation (UK GDPR) the Data Protection Act 2018 (DPA) and the Privacy and Electronic Communications Regulation (PECR)

This policy applies to the personal data of any individuals that the council may need to process in order to meet its objectives including its current and former job applicants, employees, workers, contractors, and former employees, referred to as HR-related personal data. For the avoidance of doubt this policy also applies to the personal data relating to members of the public or other personal data processed for council business.

The council has appointed the Clerk as the person with responsibility for data protection compliance within the council. Questions about this policy, or requests for further information, should be directed to them.

Definitions

"Personal data" is any information that relates to a living person who can be identified from that data (a 'data subject') on its own, or when taken together with other information. It includes both automated personal data and manual filing systems where personal data are accessible according to specific criteria. It does not include anonymised or statistical data.

"Processing" is any use that is made of data, including collecting, recording, organising, consulting, storing, amending, disclosing or destroying it.

"Special categories of personal data" means information about an individual's racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, health, sex life or sexual orientation and genetic or biometric data as well as criminal convictions and offences.

"Criminal records data" means information about an individual's criminal convictions and offences, and information relating to criminal allegations and proceedings.

Data protection principles

The council processes personal data in accordance with chapter II of the UK GDPR the following data protection principles the council:

- processes personal data lawfully, fairly and in a transparent manner
- collects personal data only for specified, explicit and legitimate purposes

- processes personal data only where it is adequate, relevant and limited to what is necessary for the purposes of processing
- keeps accurate personal data and takes all reasonable steps to ensure that inaccurate personal data is rectified or deleted without delay
- keeps personal data only for the period necessary for processing
- adopts appropriate measures to make sure that personal data is secure, and protected against unauthorised or unlawful processing, and accidental loss, destruction or damage
- Can demonstrate that it is accountable for its processing activities by keeping suitable records of its actions

The council will inform individuals in accordance with its obligations to Art 13 of the UK GDPR of the personal data it processes, the reasons for processing the personal data, how we use such data, how long we retain the data, and the legal basis for processing in our privacy notices.

The council will not use personal data for an unrelated purpose without informing the individuals about it and the legal basis that we intend to rely on for processing it. The council will not process personal data if it does not have a legal basis for processing.

The council keeps a record of our processing activities in respect of the personal data in accordance with the requirements of the UK General Data Protection Regulation (UK GDPR).

Processing

Personal data

The council will process the personal data (that is not classed as special categories of personal data) for one or more of the following reasons:

- it is necessary for the performance of a contract, e.g., your contract of employment (or services); and/or
- it is necessary to comply with any legal obligation; and/or
- it is necessary for the council's legitimate interests (or for the legitimate interests of a third party), unless there is a good reason to protect your personal data which overrides those legitimate interests; and/or
- it is necessary to protect the vital interests of a data subject or another person; and/or
- it is necessary for the performance if a task carried out in the public interest or in the exercise of official authority vested in the controller.

If the council processes the personal data (excluding special categories of personal data) in line with one of the above bases, it will not rely upon the consent of the individual.

Otherwise, the council may be required to rely upon consent to process the personal data. If the council decides to rely upon consent to process personal data, then it will explain the reason for this according to the UK GDPR Art 7(1-4).

The council will not use the personal data for an unrelated purpose unless it has a legal or contractual obligation to do so. In some circumstances the council may rely upon an exemption contained within the Data Protection Act 2018 to process the data. In such circumstances it may not need to inform the individual of such processing activities.

Personal data gathered for the purposes of employment is held in the personnel files in hard copy and electronic format on HR and IT systems and servers. The periods for which the council holds the HR-related personal data are contained in our privacy notices to individuals and recorded in the councils Records of Processing Activity (RoPAs).

Sometimes the council will share the personal data with contractors and agents to carry out its obligations under a contract with the individual or in its legitimate interests. We require individuals authorised to access the council's data who may be sole traders or partnerships or companies to keep such personal data confidential and secure and to protect it in accordance with UK Data Protection law and the council's policies. They are only permitted to process the data for the lawful purpose for which it has been shared and in accordance with the council's instructions and where they act as a data processor.

The council will update HR-related personal data promptly where advised or where information has changed or is inaccurate.

The council keeps a record of our processing activities in respect of HR-related personal data in accordance with the requirements of the UK General Data Protection Regulation (UK GDPR).

Special categories of data

The council will only process special categories of personal data (see above) on the following basis in accordance with legislation:

- where it is necessary for carrying out rights and obligations under employment law or a collective agreement;
- where it is necessary to protect your vital interests or those of another person where you are physically or legally incapable of giving consent;
- where you have made the data public;
- where it is necessary for the establishment, exercise or defence of legal claims;
- where it is necessary for the purposes of occupational medicine or for the assessment of your working capacity;

- where it is carried out by a not-for-profit body with a political, philosophical, religious or trade union aim provided the processing relates to only members or former members provided there is no disclosure to a third party without consent;
- where it is necessary for reasons for substantial public interest on the basis of law which is proportionate to the aim pursued and which contains appropriate safeguards;
- where is it necessary for reasons of public interest in the area of public health; and
- where is it necessary for archiving purposes in the public interest or scientific and historical research purposes.

If the council processes special categories of personal data in line with one of the above bases, it does not require the consent of the individual. In other cases, the council is required to gain consent to process your special categories of personal data. If the council asks for consent to process a special category of personal data, then it will explain the reason for the request. Such processing will be undertaken in the council's Legitimate Interests or using an exemption contained within the Data Protection Act 2018. In some cases, we may rely upon an Appropriate Policy Document.

Individual rights

All data subjects for whom the council may process personal data have a number of rights in relation to your personal data.

Subject access requests

Individuals have the right to make a subject access request. If such a request is received, the council will endeavour to inform the requester:

- whether or not their personal data is processed and if so why, the categories of personal data concerned and the source of the data if it is not collected from the individual.
- to whom the personal data is or may be disclosed, including to recipients located outside the European Economic Area (EEA) and the safeguards that apply to such transfers.
- for how long the personal data is stored (or how that period is decided)
- the rights to rectification or erasure of data, or to restrict or object to processing.
- the right to complain to the Information Commissioner's Office (ICO) if the individual thinks the council has failed to comply with their data protection rights; and
- whether or not the council carries out automated decision-making and the logic involved in any such decision-making.

The council will also provide individuals with access to personal data undergoing processing. This will normally be in electronic form unless otherwise agreed.

If additional requests are made to access the personal data, the council may charge a fee, which will be based on the administrative cost to the council of providing the additional copies.

To make a subject access request, the individual should send the request to the Clerk or Chairman of the Council. In some cases, the council may need to ask for proof of identification before the request can be processed. The council will inform the individual if it needs to verify the identity of the individual and the documents that may be required.

The council will normally respond to a request within a period of one month from the date it is received. Where the council processes large amounts of personal data, this may not be possible and may be extend to three months. The council will inform the individual within one month of receiving the original request to tell you if this is the case.

If a subject access request is manifestly unfounded or excessive, the council is not obliged to comply with it. Alternatively, the council can agree to respond but will charge a fee, which will be based on the administrative cost of responding to the request. A subject access request is likely to be manifestly unfounded or excessive where it repeats a request to which the council has already responded. If an individual submits a request that is unfounded or excessive, the council will notify them that this is the case and whether or not it will respond to it.

Other rights

Individuals have a number of other rights in relation to your personal data. They can require the council to:

- rectify inaccurate data;
- stop processing or erase data that is no longer necessary for the purposes of processing;
- stop processing or erase data if your interests override the council's legitimate grounds for processing data (where the council relies on our legitimate interests as a reason for processing data);
- stop processing or erase data if processing is unlawful; and
- stop processing data for a period if data is inaccurate or if there is a dispute about whether or not your interests override the council's legitimate grounds for processing data.

complain to the Information Commissioner's Office (ICO). The council will ensure that individuals are aware they may complain and provide contact details of the ICO in the public domain and upon request.

-

Data security

The council takes the security of personal data seriously. The council has internal policies and controls in place to protect personal data against loss, accidental destruction, misuse or disclosure, and to ensure that data is not accessed, except by employees or those authorised to access the data in the proper performance of their duties.

Where the council engages third parties to process personal data on our behalf, such parties do so on the basis of written instructions, are under a duty of confidentiality and are obliged to implement appropriate technical and organisational measures to ensure the security of data.

[Impact assessments

Some of the processing that the council carries out may result in risks to privacy (such as monitoring of public areas via CCTV). Where processing would result in a high risk to individual's rights and freedoms, the council will carry out a data protection impact assessment (DPIA) to determine the necessity and proportionality of processing. This will include considering the purposes for which the activity is carried out, the risks to individuals and the measures that can be put in place to mitigate those risks.

Data breaches

The council have robust measures in place to minimise and prevent data breaches from taking place. Should a breach of personal data occur the council must take notes and keep evidence of that breach.

If the council becomes aware of a data breach, details of the incident will be sent to the Clerk or Chairman of the Council without delay to ensure appropriate action may be taken. This may include reporting such a breach to the ICO. Regardless of the severity of the circumstances and potential impact on individuals' rights, the incident will be recorded.

If the council discovers that there has been a breach of data protection law concerning personal data that poses a serious risk to the rights and freedoms of individuals, it will report it to the Information Commissioner within 72 hours of discovery.

If the breach is likely to result in a high risk to the rights and freedoms of individuals, the council will inform the individuals concerned that there has been a breach and provide them with information about its likely consequences and the mitigation measures the council has taken.

International data transfers

The council may not transfer HR-related personal data to countries outside the EEA. However, where data is stored outside of these countries certain precautions are taken. Such safeguards may include but are not limited to the UK Addendum in conjunction with the EU Standard Contractual Clauses (SCCs) or the UK International Data Transfer Agreement (IDTA). All such transfers will be subject to Transfer Risk Assessments (TRAs).

Individual responsibilities

Individuals are responsible for helping the council keep the personal data up to date. The individual should let the council know if data provided to the council changes, for example if they move to a new house or change their bank details. The council will from time to time take appropriate measures to check the personal data is accurate and up to date.

All individuals who may work for, or on behalf of, the council have some responsibility for ensuring data is collected, stored and handled appropriately and in line with the council's policies.

Such individuals may have access to the personal data of other individuals and of members of the public in the course of their work with the council. Where this is the case, the council expects such individuals to help it meet the data protection obligations included in this policy. Individuals who have access to personal data are required:

- to access only data that they are authority to access and only for authorised purposes.
- not to disclose data except to individuals (whether inside or outside the council) who have appropriate authorisation;
- to keep data secure (for example by complying with rules on access to premises, computer access, including password protection, locking computer screens when away from desk, and secure file storage and destruction including locking drawers and cabinets, not leaving documents on desk whilst unattended);
- not to remove personal data, or devices containing or that can be used to access personal data, from the council's premises without prior authorisation and without adopting appropriate security measures (such as encryption or password protection) to secure the data and the device; and
- not to store personal data on local drives or on personal devices that are used for work purposes.
- to never transfer personal data outside the European Economic Area except in compliance with the law and with express authorisation from the Clerk or Chair of the Council
- to ask for help from the council's data protection lead if they are unsure about data protection or if they notice a potential breach or any areas of data protection or security that can be improved upon.

Failing to observe these requirements may amount to a disciplinary offence, which will be dealt with under the council's disciplinary procedure. Significant or deliberate breaches of this policy, such as accessing personal data without authorisation or a legitimate reason to do so or concealing or destroying personal data as part of a subject access request, may constitute gross misconduct and could lead to dismissal without notice.

Training

The council provides training to all individuals about their data protection responsibilities.

If the individual's roles require them to have regular access to personal data, or they are responsible for implementing this policy or responding to subject access requests under this policy, they will receive additional training to help them understand their duties and how to comply with them.

This is a non-contractual policy and procedure which will be reviewed from time to time.

Date of policy: May 2022
Approving committee:
Date of committee meeting:
Policy version reference:
Supersedes: [Name of old policy and reference]
Policy effective from:
Date for next review:

The council must ensure that any commitment made in their policy is relevant and up to date.

1. Data Protection Officer

The policy assumes that the council has a Data Protection lead rather than appointed a Data Protection Officer (DPO). The role of DPO is set out in legislation and infers specific obligations. Parish councils in England and community councils in Wales and Scotland are exempt from having to appoint a DPO (https://ico.org.uk/for-organisations/in-your-sector/local-government/local-gov-gdpr-faqs/) but are still subject to data protection legislation and must ensure sufficient resources to meet the obligations under the GDPR.