KESGRAVE TOWN COUNCIL

Data Protection Policy (General)

Purpose

Kesgrave Town Council ("Council") is committed to being transparent about how it collects and uses personal data to meeting our data protection obligations. This policy sets out Council's obligations and commitment to data protection, and all parties rights in relation to personal data in line with the General Data Protection Regulation (GDPR) and the Data Protection Act 2018 (DPA).

This policy applies to the personal data of current and former job applicants, employees, workers, contractors and other suppliers, former employees, Councillors, customers, residents and other members of the public in regard to personal data processed for Council business.

Council has appointed the Town Clerk ("Clerk") as the person with responsibility for data protection compliance within Council. Questions about this policy, or requests for further information, should be directed to the Clerk.

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 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

In accordance with the following data protection principles, 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; and
- adopts appropriate measures to make sure that personal data is secure, and protected against unauthorised or unlawful processing, and accidental loss, destruction or damage.

In our privacy notices, Council will advise of the personal data it processes, the reasons for processing personal data, how it is used, how long it is retained, and the legal basis for processing.

Council will not use personal data for an unrelated purpose without advising those concerned together with the legal basis relied upon for processing it. Council will not process personal data if it does not have a legal basis for doing so.

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

Processing

Personal data

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

If Council processes personal data (excluding special categories of personal data) in line with one of the above bases, it does not require consent. Otherwise, Council is required to gain consent to process personal data. If Council asks for consent to process personal data, then we will explain the reason for the request. Individuals do not need to consent or can withdraw consent later.

Council will not use personal data for an unrelated purpose without telling the individual about it and the legal basis that we intend to rely on for processing it.

For employees personal data gathered during their employment is held in their personnel file in hard copy and electronic format on Council's HR and IT systems and servers. The periods for which Council holds HR-related personal data are contained in our privacy notices to individuals.

Sometimes Council will share personal data with contractors and agents to carry out our obligations under a contract with the individual or for our legitimate interests. We require those individuals or companies to keep personal data confidential and secure and to protect it in accordance with Data Protection law and our policies. They are only permitted to process that data for the lawful purpose for which it has been shared and in accordance with our instructions.

Council will update personal data promptly if advised that information has changed or is inaccurate. Individuals may be required to provide documentary evidence in some circumstances.

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

Special categories of data

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 vital interests or those of another person where an individual is physically or legally incapable of giving consent;
- where the data has been made 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 employee 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 Council processes special categories of personal data in line with one of the above bases, it does not require consent. In other cases, Council is required to gain consent to process special categories of personal data. If Council asks for consent to process a special category of personal data, then we will explain the reason for the request. Individuals do not need to consent or can withdraw consent later.

Individual rights

Data subjects have a number of rights in relation to their personal data.

Subject access requests

Individuals have the right to make a subject access request. If they make a subject access request, Council will advise:

- whether or not their 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 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 personal data is stored (or how that period is decided);
- rights to rectification or erasure of data, or to restrict or object to processing;
- the right to complain to the Information Commissioner if it is thought Council has failed to comply with anyone's data protection rights; and
- whether or not Council carries out automated decision-making and the logic involved in any such decision-making.

Council will also provide individuals with a copy of personal data undergoing processing. This will normally be in electronic form if a request was made electronically, unless agreement is reached otherwise.

If additional copies are required, Council may charge a fee, which will be based on the administrative cost to Council of providing the additional copies.

To make a subject access request, it should be sent to the Clerk or Chair of Council. In some cases, Council may need to ask for proof of identification before the request can be processed. Council will advise if we need to verify identity and the documents we require.

Council will normally respond to a request within a period of 30 days from the date it is received. Where Council processes large amounts of an individual's data, this may not be possible within one month. Council will write within 30 days of receiving the original request to advise if this is the case.

If a subject access request is manifestly unfounded or excessive, Council is not obliged to comply with it. Alternatively, 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 Council has already responded. If a request is received that is unfounded or excessive, Council will notify that this is the case and whether or not we will respond to it.

Other rights

Individuals have a number of other rights in relation to personal data. They can require 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 their interests override Council's legitimate grounds for processing data (where 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 their interests override Council's legitimate grounds for processing data; and
- complain to the Information Commissioner. This can be done by contacting the Information Commissioner's Office directly. Full contact details including a helpline number can be found on the Information Commissioner's Office website (www.ico.org.uk).

To ask Council to take any of these steps, a request should be sent to the Clerk or Chair of Council.

Data security

Council takes the security of personal data seriously. 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 in the proper performance of their duties.

Where 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 Council carries out may result in risks to privacy. Where this would result in a high risk to rights and freedoms, 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 and the measures that can be put in place to mitigate those risks.

In regard to the monitoring of public areas via CCTV, Council maintains a separate specific Policy which is available on the Council's website or in hard copy on request from the Council's office.

Data breaches

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

Awareness of a data breach should be notified to the Clerk or Chair of Council immediately and any evidence in relation to the breach retained.

If Council discovers that there has been a breach of personal data that poses a risk to anyone's rights and freedoms, we will report it to the Information Commissioner within 72 hours of discovery. Council will record all data breaches regardless of their effect.

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

International data transfers

Council will not transfer personal data to countries outside the EEA.

Individual responsibilities

Those supplying personal data to Council are responsible for keeping their personal data up to date and should advise Council of any changes, for example address or bank details.

Everyone who works for, or on behalf of, Council has some responsibility for ensuring data is collected, stored and handled appropriately, in line with Council's policies.

Employees and Councillors may have access to the personal data of other individuals and of members of the public in the course of their work with Council. Where this is the case, Council relies on them to help meet our data protection obligations. Those who have access to personal data are required:

- to access only data they have authority to access and only for authorised purposes;
- not to disclose data except to individuals (whether inside or outside 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 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;
- 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 Council; and
- to ask for help from Council's data protection lead if unsure about data protection or in the case of a potential breach or any areas of data protection or security that can be improved upon.

Any staff member failing to observe these requirements may be subject to 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. Councillors in breach of the requirements may be subject to investigation under Council's Code of Conduct.

Training

Council provides training to all employees and Councillors about their data protection responsibilities.

Additional training is provided to those whose roles require regular access to personal data, or they are responsible for implementing this policy or responding to subject access requests under this policy, to help understanding of their duties and how to comply with them.

Policy effective from: 26 June 2023

Date for next review: 26 June 2025 (unless the document below is updated sooner)

[Based on the National Association of Local Councils' template policy last updated December 2019.]