KESGRAVE TOWN COUNCIL

Confidentiality Policy

1. Introduction

a) The purpose of this policy is to introduce the concept of confidentiality for the processing of information by Council. This policy will raise awareness of the importance of confidentiality and set out a framework for the processing of sensitive information by those acting on behalf of Council.

b) Sensitive information can include:
- Personal Information;
- Sensitive Personal Information;
- Commercially Sensitive Information; or
- Sensitive Corporate Information.

c) We believe that everyone has a fundamental right to the information held about them being kept secure and confidential.

d) Council Officers have the authority to obtain and disclose personal data, but they will be committing a criminal offence if they use this position to obtain, disclose, or procure disclosure of personal data for their own purposes.

e) All Council employees are expected to:
- Treat all personal and sensitive information as confidential to the authority, whether the information has been received formally, informally or discovered by accident;
- Comply with the law regarding the protection and disclosure of information:
- Only disclose personal information where there is a justified purpose and in accordance with the General Data Protection Regulations; and
- Not gain or attempt to gain access to information they are not authorised to have.

f) Council's Terms and Conditions of Employment stipulate the confidentiality clause employees are bound to comply with.

2. Scope

a) This policy applies to everyone acting on behalf of Council including councillors and employees, whether permanent, temporary or contracted, either as an individual or through a third-party supplier.

b) Council is fully committed to the broad principles of social justice and is opposed to any form of discrimination or oppression, and will act at all times in accordance with Equality legislation.

3. Legal Framework

a) Council work requires the collection, use and disclosure of information for a variety of purposes, and this processing is subject to the following legislation:
- The Human Rights Act (1989) - Article 8 guarantees the right to respect for privacy and family life, home and correspondence.
- The General Data Protection Regulations (2018) – guarantees that all personal data and special categories of personal data collected satisfy legal obligations. Please refer to our Data Protection policies.
- The Public Interest Disclosure Act (1998) – allows exemptions for specific kinds of disclosures by employees, such as the raising of concerns of practice.
- The Freedom of Information Act (2000) – provides a general right of access to the information held by the council.

4. Council's Responsibilities

a) Everyone acting on behalf of Council must be aware of, and comply with the requirements of this policy and appropriate legislation when handling or processing information, and challenge and report inappropriate behaviour or breaches of this policy.

b) The Town Clerk is responsible for raising awareness of the policy and for providing advice and guidance in relation to it.

5. How to Keep Information Confidential

5.1. Overview

a) All information should be classified and handled in accordance with Council's policies and procedures.

b) Only authorised officers should process confidential information.

c) Confidential information must not be disclosed, discussed or viewed in public or unsecure areas.

d) The processing of information should be evidenced.

5.2. Processing Information

a) The processing of all information must be in accordance with relevant legislation and Council's policies and procedures. In regard to the collection and use of personal and special categories of personal data please refer to Council's Data Protection policies.

5.3. Disclosing Information

a) Council can receive spurious or fraudulent requests for information. Officers must therefore take all reasonable steps to verify the identity of the requester. Requests should normally be made in writing.

b) Personal information relating to deceased individuals will continue to be treated as confidential and will not be disclosed without clear justification. The privacy and wishes of relatives will be taken into account when considering the appropriateness of such disclosures. Wishes expressed by a Data Subject prior to their death will be respected.

c) Data Subjects have a right to be provided with their own personal information via a Subject Access Request (SAR) under the General Data Protection Regulations. Please refer to Council's Data Protection Policy (General) and Privacy Notice.

5.4. Accessing Information

a) Councillors and employees must only have access to the systems, equipment and information that they genuinely need to carry out their work, and will respect the confidentiality of that information at all times.

b) Councillors and employees must never view or amend information about themselves, their family or friends. If authority has been given to an employee to act on behalf of someone else then this should be done through the same channels as all other queries (i.e. through the Chair or Town Clerk).

c) In all cases where a councillor or employee has an interest in a claim, property or account, or where there may be a conflict of interest, a declaration of interest should be completed. It is the responsibility of the relevant Officer to inform the Chair of any conflict of interest or changes to the individual's declaration of interest.

5.5. Physical Security

a) Confidential information must be kept in a secure environment.

b) Information must be put away securely when not in use.

c) Confidential information must never be left unattended.

d) When transferring confidential information it must always be passed to an authorised Officer; it must never be left on a desk or other unsecure place.

e) All confidential information must be disposed of appropriately; confidential information or equipment (i.e. encrypted USB's) must not be place in normal waste or recycling bins.

5.6. Transportation of information

a) Confidential information must not be taken out of a secure environment without a justified reason which should be recorded in writing.

b) Before taking confidential information out of a secure environment, always consider if it can be summarised or anonymised.

c) If confidential information and equipment is taken out of a secure environment then it must be kept secure and returned as soon as possible e.g. office laptops.

d) Confidential information and equipment must never be left unattended on public transport, personal transport or in public areas.

e) Where confidential information or equipment is outside of a secure environment overnight, it must be stored in a secure location.

f) Confidential information downloaded to personal devices must be deleted as soon as it has served its purpose.

5.7. Use of Equipment

a) Council equipment must remain secure at all times and never left unattended.

b) Council issued equipment must only be used by Council employees.

c) Council issued equipment must be encrypted and password protected wherever possible.

d) Passwords must be kept secure at all times and meet password requirements.

5.8. Universal Serial Buses (USBs)

a) Only encrypted USB memory sticks may be used.

5.9. Telephone and Private Conversations

a) Councillors and employees should not disclose confidential information over the telephone unless they have satisfied themselves as to the identity of the requester and are in a secure environment to prevent information being overheard by others.

b) When answering the telephone consider where you are positioned and who is around you, where the call is private you should ensure you are in a place to take that call.

5.10. Emails

a) When sending confidential information via email always use a secure email account.

b) Always check the recipients email address before sending, where required send a test email.

c) When sending confidential information ensure this is transferred either by a password protected file or via a secure email address.

See also Council's Email, Internet etc Policy and Procedure which includes, "If you are copying in a recipient(s) who has not given explicit permission for their email to be circulated, use the blind copy facility (BCC) to protect their personal data.".

5.11. Social Media

a) No confidential information must ever be published onto any social media sites.

6. Breaches in Policy

a) Breaches of this policy may constitute be investigated under disciplinary procedures for employees and Code of Conduct sanctions in regard to councillors. The unauthorised disclosure of personal information is an offence under GDPR.

b) Any confidential information which is obtained accidentally must be reported immediately; otherwise, this will be seen as a breach in policy.

c) Where it is found confidential information has been obtained for personal gain this will result in a disciplinary procedure and possible court action for criminal misconduct in regard to employees, or Code of Conduct sanctions in regard to councillors.

Policy effective from: 02 June 2025

Date for next review: 02 June 2028