Data Protection Policy

Corporate Information Governance Group.

Data Protection Policy

CONTENTS

CLAUSE

SCHEDULE

Corporate Information Governance Group.

Data Protection Policy

1. POLICY STATEMENT

1.1 Everyone has rights with regard to the way in which their personal data in handled. During the course of our activities we will collect, store and process personal data about our customers, suppliers and other third parties, and we recognise that the correct and lawful treatment of this data will maintain confidence in the organisation and will provide for successful business operations.

1.2 Data users are obliged to comply with this policy when processing personal data on our behalf. A serious breach of this policy may result in disciplinary action.

2. ABOUT THIS POLICY

2.1 This Policy will apply to all council employees working for Canterbury City Council, Dover District Council, Thanet District Council and employees of East Kent Services and the East Kent Audit Partnership. Hereafter they will be referred to collectively as 'the councils'. It also applies to the Councillors in each of the three districts.

2.2 The types of personal data that the councils may be required to handle include information about current, past and prospective customers and others that we communicate with. The personal data, which may be held on paper or on a computer or other media, is subject to certain legal safeguards specified in the Data Protection Act 1998 (the Act) and other regulations.

2.3 This policy and any other documents referred to in it sets out the basis on which we will process any personal data we collect from data subjects, or that is provided to us by data subjects or other sources.

2.4 This policy does not form part of any employee's contract of employment and may be amended at any time.

2.5 This policy has been approved by the Corporate Information Governance Group [CIGG], acting on behalf of the councils. It sets out rules on data protection and the legal conditions that must be satisfied when we obtain, handle, process, transfer and store personal data.

2.6 The Data Protection Compliance Manager is responsible for ensuring compliance with the Act and with this policy. That post is held by the Senior Information Risk Owner, or their Deputy in each of the three councils.

Any questions about the operation of this policy or any concerns that the policy has not been followed should be referred in the first instance to the Data Protection Compliance Manager.

2.7 The designated officer will be responsible for completing the annual notification to the ICO and advising them of any updates to the register within 28 days.

3. DEFINITION OF DATA PROTECTION TERMS

3.1 **Data** is information which is stored electronically, on a computer, or in certain paper-based filing systems.

3.2 **Data subjects** for the purpose of this policy include all living individuals about whom we holds personal data. A data subject need not be a UK national or resident. All data subjects have legal rights in relation to their personal information.

3.3 **Personal data** means data relating to a living individual who can be identified from that data (or from that data and other information in our possession). Personal data can be factual (for example, a name, address or date of birth) or it can be an opinion about that person, their actions and behaviour.

3.4 **Data controllers** are the people who or organisations which determine the purposes for which, and the manner in which, any personal data is processed. They are responsible for establishing practices and policies in line with the Act. We are the data controller of all personal data used in our business for our own commercial purposes.

3.5 **Data users** are those of our employees whose work involves processing personal data. Data users must protect the data they handle in accordance with this data protection policy and any applicable data security procedures at all times.

3.6 **Data processors** include any person or organisation that is not a data user that processes personal data on our behalf and on our instructions. Employees of data controllers are excluded from this definition but it could include suppliers which handle personal data on the council's behalf.

3.7 **Processing** is any activity that involves use of the data. It includes obtaining, recording or holding the data, or carrying out any operation or set of operations on the data including organising, amending, retrieving, using, disclosing, erasing or destroying it. Processing also includes transferring personal data to third parties.

3.8 **Sensitive personal data** includes information about a person's racial or ethnic origin, political opinions, religious or similar beliefs, trade union membership, physical or mental health or condition or sexual life, or about the commission of, or proceedings for, any offence committed or alleged to have been committed by that person, the disposal of such proceedings or the sentence of any court in such proceedings. Sensitive personal data can only be processed under strict conditions, including a condition requiring the express permission of the person concerned.

3.9 **Third Party** - Any individual/organisation other than the data subject, the data controller (the council's) or its agents.

3.10 **Relevant Filing System** - Any paper filing system or other manual filing system which is structured so that information about an individual is readily accessible.

4. RESPONSIBILITIES UNDER THE DATA PROTECTION ACT

Each council is a data controller under the Act.

The Data Protection Compliance Manager is responsible for ensuring compliance with the Act and with this policy and may assign officers to support this process.

The Corporate Management Team of each council is responsible for developing and encouraging good information handling practice within the council.

Compliance with data protection legislation is the responsibility of everybody who processes personal information.

The councils, through their staff are responsible for ensuring that any personal data supplied is accurate and up-to-date.

Councillors' Responsibilities

Members are regarded as Data Controllers in their own right if they process personal data either manually or by computer, whether on their own equipment or on equipment provided to them
by the Council.

There are three ways in which councillors might use personal data:

1. When considering issues and making decisions as part of the council's business – for example in committees or working groups. This is covered by the council's notification.

2. As a member of a political party canvassing for votes or working for a party. This is usually covered by the party's notification.

Councillors who are not a member of a political group must make their own arrangements to notify the ICO in order to process personal data in this way.

3. Carrying out casework. In this case the councillor is the data controller and is required to notify the ICO. It is the practice of the councils to notify the Information Commissioner's Office (ICO) on their behalf of all purposes for which the councillors hold and process personal data.

Where holding and proc**e**ssing personal data about individuals in the course of undertaking council business, a councillor will be covered by the council's notification to the ICO, and have the same responsibilities in respect of data protection as an employee of the authority.

5. DATA PROTECTION PRINCIPLES

Anyone processing personal data must comply with the eight enforceable principles of good practice. These provide that personal data must be:

5.1 *Processed fairly and lawfully.*

The Act is not intended to prevent the processing of personal data, but to ensure that it is done fairly and without adversely affecting the rights of the data subject.

For personal data to be processed lawfully, they must be processed on the basis of one of the legal grounds set out in the Act. These include, among other things, the data subject's consent to the processing, or that the processing is necessary for the performance of a contract with the data subject, for the compliance with a legal obligation to which the data controller is subject, or for the legitimate interest of the data controller or the party to whom the data is disclosed. When sensitive personal data is being processed, additional conditions must be met. When processing personal data as data controllers in the course of our business, we will ensure that those requirements are met.

5.2 *Processed for limited purposes and in an appropriate way.*

In the course of our business, we may collect and process the personal data set out in the **Error! Reference source not found.**. This may include data we receive directly from a data subject (for example, by completing forms or by corresponding with us by mail, phone, email or otherwise) and data we receive from other sources (including, for example, business partners, sub-contractors in technical, payment and delivery services, credit reference agencies and others).

We will only process personal data for the specific purposes set out in the **Error! Reference source not found.** or for any other purposes specifically permitted by the Act. We will notify those purposes to the data subject when we first collect the data or as soon as possible thereafter.

5.3 ***Adequate, relevant and not excessive for the purpose.***

Information, which is not strictly necessary for the purpose for which it is obtained, should not be collected. If data are given or obtained which is excessive for the purpose, they should be immediately deleted or destroyed.

5.4 ***Accurate.***

Data, which are kept for a long time, must be reviewed and updated as necessary. No data should be kept unless it is reasonable to assume that they are accurate. It is the responsibility of individuals to ensure that data held by the council are accurate and up-to-date. Individuals should notify the council of any changes in circumstance to enable personal records to be updated accordingly. It is the responsibility of the council to ensure that any notification regarding change of circumstances is noted and acted upon.

5.5 ***Not kept longer than necessary for the purpose.***

We will not keep personal data longer than is necessary for the purpose or purposes for which they were collected. We will take all reasonable steps to destroy, or erase from our systems, all data which is no longer required.

5.6 ***Processed in line with data subjects' rights.***

We will process all personal data in line with data subjects' rights, in particular their right to:

- Request access to any data held about them by a data controller.
- Prevent the processing of their data for direct-marketing purposes.
- Ask to have inaccurate data amended.
- Prevent processing that is likely to cause damage or distress to themselves or anyone else.

We recognise that there is emerging case law on the rights of data subjects. We will review our policy and working practices in the light of this case law and at the same time seek to comply with the requirements of the new General Data Protection Regulations (GDPR).

5.7 ***Secure****.*

See section headed ‘Data Security’.

5.8 ***Not transferred to people or organisations situated in countries without adequate protection.***

We may transfer any personal data we hold to a country outside the European Economic Area ("EEA"), provided that one of the following conditions applies:

- The country to which the personal data are transferred ensures an adequate level of protection for the data subjects' rights and freedoms.
- The data subject has given his consent.
- The transfer is necessary for one of the reasons set out in the Act, including the performance of a contract between us and the data subject, or to protect the vital interests of the data subject.
- The transfer is legally required on important public interest grounds or for the establishment, exercise or defence of legal claims.
- The transfer is authorised by the relevant data protection authority where we have adduced adequate safeguards with respect to the protection of the data subjects' privacy, their fundamental rights and freedoms, and the exercise of their rights.

Subject to the requirements in the clause above, personal data we hold may also be processed by staff operating outside the EEA who work for us or for one of our suppliers. That staff maybe engaged in, among other things, the fulfilment of contracts with the data subject, the processing of payment details and the provision of support services.

6. NOTIFYING DATA SUBJECTS

6.1 If we collect personal data directly from data subjects, we will inform them about:

(a) The purpose or purposes for which we intend to process that personal data.

(b) The types of third parties, if any, with which we will share or to which we will disclose that personal data.

(c) The means, if any, with which data subjects can limit our use and disclosure of their personal data.

6.2 If we receive personal data about a data subject from other sources, we will provide the data subject with this information as soon as possible thereafter.

6.3 We will also inform data subjects whose personal data we process that we are the data controller with regard to that data, [and who the Data Protection Compliance Manager is].

7. DATA SECURITY

7.1 We will take appropriate security measures against unlawful or unauthorised processing of personal data, and against the accidental loss of, or damage to, personal data.

7.2 We will put in place procedures and technologies to maintain the security of all personal data from the point of collection to the point of destruction. Personal data will only be transferred to a data processor if he agrees to comply with those procedures and policies, or if he puts in place adequate measures himself.

7.3 We will maintain data security by protecting the confidentiality, integrity and availability of the personal data, defined as follows:

(a) Confidentiality means that only people who are authorised to use the data can access it.

(b) Integrity means that personal data should be accurate and suitable for the purpose for which it is processed.

(c) Availability means that authorised users should be able to access the data if they need it for authorised purposes. Personal data should therefore be stored on the council's central computer system instead of individual PCs.

7.4 Security procedures include:

(a) Entry controls. Any stranger seen in entry-controlled areas should be reported.

(b) Secure lockable desks and cupboards. Desks and cupboards should be kept locked if they hold confidential information of any kind. (Personal information is always considered confidential.)

(c) Methods of disposal. Paper documents should be shredded. Digital storage devices should be physically destroyed when they are no longer required.

(d) Equipment. Data users must ensure that individual monitors do not show confidential information to passers-by and that they log off from their PC when it is left unattended.

8. DISCLOSURE AND SHARING OF PERSONAL INFORMATION

8.1 Personal data may be shared within the three council's or with East Kent Services or the East Kent Audit Partnership as part of our collaborative working arrangements.

8.2 We may also disclose personal data we hold to third parties:

(a) In the event that we sell or buy any business or assets, in which case we may disclose personal data we hold to the prospective seller or buyer of such business or assets.

(b) If we or substantially all of our assets are acquired by a third party, in which case personal data we hold will be one of the transferred assets.

8.3 If we are under a duty to disclose or share a data subject's personal data in order to comply with any legal obligation, or in order to enforce or apply any contract with the data subject or other agreements; or to protect our rights, property, or safety of our employees, customers, or others. This includes exchanging information with other companies and organisations for the purposes of fraud protection and credit risk reduction.

8.4 We may also share personal data we hold with selected third parties for the purposes set out in the **Error! Reference source not found.**.

9. DEALING WITH SUBJECT ACCESS REQUESTS

9.1 Data subjects must make a formal request for information we hold about them. This must be made in writing. Employees who receive a written request should forward it to the council's FOI officer.

9.2 When receiving telephone enquiries, we will only disclose personal data we hold on our systems if the following conditions are met:

(a) We will check the caller's identity to make sure that information is only given to a person who is entitled to it.

(b) We will suggest that the caller put their request in writing if we are not sure about the caller's identity and where their identity cannot be checked.

9.3 Our employees will refer a request to their line manager [or the Data Protection Compliance Manager] for assistance in difficult situations. Employees should not be bullied into disclosing personal information.

9.4 Any individual who wishes to exercise this right should submit a written request for subject access, provide satisfactory proof of identity, sufficient information to enable the data to be located, and pay the designated fee where appropriate.

9.5 Subject to satisfactory completion of 9.4, the data controller should respond within 40 days, ensuring that all data provided protects the interests of third parties by deleting any reference to them. A copy of the response should be retained for use in case of challenge.

10. DISCLOSURE OF DATA

The council must ensure that personal data are not disclosed to unauthorised third parties which includes family members, friends, landlords, government bodies, and in certain circumstances, the Police. All staff and members should exercise caution when asked to disclose personal data held on another individual to a third party.

The important thing to bear in mind is whether or not disclosure of the information is relevant to, and necessary for, the conduct of the council's business. Best practice, however, would be to take the contact details of the person making the enquiry and pass them onto senior management or the Data Protection Officer for a decision on the release of the information.

This policy determines that personal data may be legitimately disclosed where one of the following conditions apply:

1. the individual has given their consent (eg a member of staff or a Service User has consented to the council corresponding with a named third party);
2. where the disclosure is in the legitimate interests of the authority (eg disclosure to staff - personal information can be disclosed to other council employees if it is clear that those members of staff require the information to enable them to perform their jobs);
3. where the authority is legally obliged to disclose the data (eg ethnic minority and disability monitoring);

The Act permits certain disclosures without consent so long as the information is requested for one or more of the following purposes:

- to safeguard national security*;
- prevention or detection of crime including the apprehension or prosecution of offenders*;
- assessment or collection of tax duty*;
- discharge of regulatory functions (includes health, safety and welfare of persons at work)*;
- to prevent serious harm to a third party;
- to protect the vital interests of the individual, this refers to life and death situations.

* Requests must be supported by appropriate paperwork.

Unless consent has been obtained from the data subject, information should not be disclosed over the telephone. Instead, the enquirer should be asked to provide documentary evidence to support their request. Ideally a statement from the data subject consenting to disclosure to the third party should accompany the request.

If in doubt, staff should seek advice from their Head of Department or The Council's Data Protection Officer.

11. DATA SHARING

Information shared with third party organisations should comply with the Data Sharing Policy which forms part of the suite of Information Security policies available on the council's intranet.

12. RETENTION AND DISPOSAL OF DATA

The council discourages the retention of personal data for longer than they are required. Personal data must be disposed of in a way that protects the rights and privacy of data subjects (eg, shredding, disposal as confidential waste, secure electronic deletion).

13. USE OF CCTV

The council's use of CCTV is regulated by the ICO Code of Practice, supplemented by local policy and guidance.

14. FREEDOM OF INFORMATION ACT 2000

The Freedom of Information Act 2000 (FOIA) allows public access to all types of information held by public authorities. Requests for personal information will be dealt with under the Data Protection Act. The FOIA will not disclose private and confidential information about individuals without taking into account the requirements of the Data Protection Act.

15. COMPLAINTS

The council's 'comments and complaints procedure' will be applied in the event of any complaints received about requests for access to information under the Act. Details can be found on each council's website.

16. POLICY REVIEW

This policy will be managed and reviewed annually by the Corporate Information Governance Group. Reviews will be subject to scrutiny and, from time to time, updates and re-issues will be circulated.

However, the policy will be reviewed sooner if a weakness in the policy is highlighted, in the case of new risks, and/or changes in legislation.

17. FURTHER INFORMATION

For further guidance or advice on the Data Protection Act, please contact:

Canterbury: foi@canterbury.gov.uk, telephone 01227 862175.
Dover: Harvey.rudd@dover.gov.uk telephone 01304 872321.
Thanet:

Policy Compliance

If any person or organisation in scope is found to have breached this policy one of the following consequences may be followed:-

- Councils' disciplinary procedure.
- Breach of contract.
- Member code of conduct.

If you do not understand the implications of this policy or how it may apply to you, seek advice from your line manager or Senior Information Risk Officer.

Document Control		
Title/Version	-	Data Protection Policy
Owner	-	Corporate Information Governance Group
Date Approved	-	
Review Date	-	
Reviewer	-	CIGG

Revision History			
Revision Date	**Reviewer (s)**	**Version**	**Description of Revision**
05/08/2016	Matthew Archer	1.0	First Draft for Consideration
08/09/2016	Hannah Lynch	1.1	Formatting/ Amendments
23/09/2016	CIGG	1.2	Final Review