Data Protection Policy

Corporate Information Governance Group.

Data Protection Policy

CONTENTS

CLAUSE

SCHEDULE

1. POLICY STATEMENT

1.1 **Canterbury City Council** regards the lawful and correct processing of personal and sensitive data as an integral part of its purpose. We believe this is vital for maintaining the confidence of our customers, employees, Members and other stakeholders about whom we process data.

1.2 This Data Protection Policy explains how we will meet our legal obligations under the Data Protection Act 2018 applying the General Data Protection Regulation ((EU) 2016/679).

2. INTERPRETATION

2.1 **Automated Decision-Making (ADM)**: when a decision is made which is based solely on Automated Processing (including profiling) which produces legal effects or significantly affects an individual. The GDPR prohibits Automated Decision-Making (unless certain conditions are met) but not Automated Processing.

2.2 **Automated Processing**: any form of automated processing of Personal Data consisting of the use of Personal Data to evaluate certain personal aspects relating to an individual, in particular to analyse or predict aspects concerning that individual's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements. Profiling is an example of Automated Processing.

2.3 **Consent**: agreement which must be freely given, specific, informed and be an unambiguous indication of the Data Subject's wishes by which they, by a statement or by a clear positive action, signifies agreement to the Processing of Personal Data relating to them.

2.4 **Council**: Canterbury City Council, Military Road, Canterbury CT1 1YW, the Data Controller.

2.5 **Council Personnel**: all employees, workers, contractors, agency workers and consultants of the Council.

2.6 **Criminal Convictions Data**: personal data relating to criminal convictions and offences.

2.7 **Data Controller**: who determines when, why and how to process Personal Data for its own business purposes and responsible for establishing practices and policies in line with the GDPR.

2.8 **Data Controller Notification**: notification to the ICO by the Data Controller of its processing activities.

2.9 **Data Subject**: a living, identified or identifiable individual about whom THE COUNCIL holds Personal Data. Data Subjects may be nationals or residents of any country and may have legal rights regarding their Personal Data.

2.10 **Data Privacy Impact Assessment (PIA)**: tools and assessments used to identify and reduce risks of a data processing activity. PIAs can be carried out as part of Privacy by Design and should be conducted for all major system or business change programs involving the Processing of Personal Data.

2.11 **Data Protection Officer (DPO)**: the person required to be appointed under the GDPR.

2.12 **EEA**: the 28 countries in the EU, and Iceland, Liechtenstein and Norway.

2.13 **Explicit Consent**: consent which requires a very clear and specific statement (that is, not just action).

2.14 **GDPR**: the General Data Protection Regulation ((EU) 2016/679).

2.15 **ICO**: Information Commissioner's Office.

2.16 Information Asset Register(s): maps out how personal and sensitive information flows through each service, the lawful bases for processing the information, how long it is kept for, technical and organisational security measures, who information is shared with, whether or not personal information is transferred outside the EEA, whether or not third parties are used to process personal information and the Information Asset Owner(s) with responsibility for managing the risk to the Council's personal and business critical information held within his/her service area.

2.17 **Members**: elected councillors for the District of Canterbury.

2.18 **Personal Data**: any information identifying a Data Subject or information relating to a Data Subject that THE COUNCIL can identify (directly or indirectly) from that data alone or in combination with other identifiers we possess or can reasonably access. Personal Data includes Special Categories of Personal Data and Pseudonymised Personal Data but excludes anonymous data or data that has had the identity of an individual permanently removed. Personal data can be factual (for example, a name, email address, location or date of birth) or an opinion about that person's actions or behaviour.

2.19 **Personal Data Breach**: any act or omission that compromises the security, confidentiality, integrity or availability of Personal Data or the physical, technical, administrative or organisational safeguards that we or our third-party service providers put in place to protect it. The loss, or unauthorised

access, disclosure or acquisition, of Personal Data is a Personal Data Breach.

2.20 **Privacy by Design**: implementing appropriate technical and organisational measures in an effective manner to ensure compliance with the GDPR.

2.21 **Privacy Guidelines**: The Council's privacy/GDPR related guidelines provided to assist in interpreting and implementing this Data Protection Policy and Related Policies, as set out in the Appendix, as amended from time to time.

2.22 **Privacy Notices**: separate notices setting out information that may be provided to Data Subjects when THE COUNCIL collects information about them. These notices may take the form of general privacy statements applicable to a specific group of individuals (for example, employee privacy notices or the website privacy policy) or they may be stand-alone, one time privacy statements covering Processing related to a specific purpose.

2.23 **Processing or Process**: any activity that involves the use of Personal 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 transmitting or transferring Personal Data to third parties.

2.24 **Pseudonymisation or Pseudonymised**: replacing information that directly or indirectly identifies an individual with one or more artificial identifiers or pseudonyms so that the person, to whom the data relates, cannot be identified without the use of additional information which is meant to be kept separately and secure.

2.25 **Related Policies**: The Council's policies, operating procedures or processes related to this Data Protection Policy designed to protect Personal Data, as set out in the Appendix, as amended from time to time.

2.26 **Special Categories of Personal Data**: information revealing racial or ethnic origin, political opinions, religious or similar beliefs, trade union membership, physical or mental health conditions, sexual life, sexual orientation, biometric or genetic data.

3. INTRODUCTION

3.1 This Data Protection Policy sets out how we handle the Personal Data of our customers, suppliers, employees, workers and other third parties.

3.2 This Data Protection Policy applies to all Personal Data we Process regardless of the media on which that data is stored or whether it relates to past or present employees, workers, customers, clients or supplier contacts, website users or any other Data Subject.

3.3 This Data Protection Policy applies to all Council Personnel and Members. You must read, understand and comply with this Data Protection Policy when Processing Personal Data on our behalf and attend training on its requirements. This Data Protection Policy sets out what we expect from you in order for us to comply with applicable law. Your compliance with this Data Protection Policy is mandatory. Related Policies and Privacy Guidelines are available to help you interpret and act in accordance with this Data Protection Policy. You must also comply with all such Related Policies and Privacy Guidelines.

3.4 Any breach of this Data Protection Policy by COUNCIL Personnel may result in disciplinary action.

3.5 Any breach of this Data Protection Policy by agency workers, contractors and consultants may result in termination of contract.

3.6 Any breach of this Data Protection Policy by Members may be regarded as a breach of the Council's Code of Conduct for Members.

3.7 A Member who discloses personal information held by us for their own personal use or the use of their political party for electioneering purposes without our consent is likely to have committed an offence.

3.8 Where you have a specific responsibility in connection with Processing such as capturing Consent, reporting a Personal Data Breach, conducting a PIA as referenced in this Data Protection Policy or otherwise, then you must comply with the Related Policies and Privacy Guidelines.

4. SCOPE

We recognise that the correct and lawful treatment of Personal Data will maintain confidence in our organisation and will provide for successful business operations. Protecting the confidentiality and integrity of Personal Data is a critical responsibility that we take seriously at all times.

The Council is exposed to potential fines of up to EUR20 million (approximately £18 million) or 4% of total worldwide annual turnover, whichever is higher and depending on the breach, for failure to comply with the provisions of the GDPR.

Directors are responsible for ensuring all Council Personnel comply with this Data Protection Policy and need to implement appropriate practices, processes, controls and training to ensure such compliance.

The DPO is responsible for overseeing this Data Protection Policy and developing Related Policies and Privacy Guidelines. That post is held by Matthew Archer, Head of Corporate Governance dataprotection@canterbury.gov.uk

Please contact the DPO with any questions about the operation of this Data Protection Policy or the GDPR or if you have any concerns that this Data Protection Policy is not being or has not been followed. In particular, you must always contact the DPO in the following circumstances:

(a) if you are unsure of the lawful basis which you are relying on to process Personal Data (including the legitimate interests used by us) (see p*aragraph 5.1* below);

(b) if you need to rely on Consent and/or need to capture Explicit Consent (see p*aragraph 5.2* below);

(c) if you need to draft Privacy Notices (see p*aragraph 5.3* below);

(d) if you are unsure about the retention period for the Personal Data being Processed (see p*aragraph 9* below);

(e) if you are unsure about what security or other measures you need to implement to protect Personal Data (see p*aragraph 10.1* below);

(f) if there has been a Personal Data Breach (p*aragraph 10.2* below);

(g) if you are unsure on what basis to transfer Personal Data outside the EEA (see p*aragraph 11* below);

(h) if you need any assistance dealing with any rights invoked by a Data Subject (see p*aragraph 12*);

(i) whenever you are engaging in a significant new, or change in, Processing activity which is likely to require a PIA (see p*aragraph 13.4* below) or plan to use Personal Data for purposes others than what it was collected for;

(j) If you plan to undertake any activities involving Automated Processing including profiling or Automated Decision-Making (see p*aragraph 13.5* below);

(k) If you need help complying with applicable law when carrying out direct marketing activities (see p*aragraph 13.6* below); or

(l) if you need help with any contracts or other areas in relation to sharing Personal Data with third parties (including our contractors/consultants) (see p*aragraph 13.7* below).

5. DATA PROTECTION PRINCIPLES

We adhere to the principles relating to Processing of Personal Data set out in the GDPR which require Personal Data to be:

(a) Processed lawfully, fairly and in a transparent manner (Lawfulness, Fairness and Transparency).

(b) Collected only for specified, explicit and legitimate purposes (Purpose Limitation).

(c) Adequate, relevant and limited to what is necessary in relation to the purposes for which it is Processed (Data Minimisation).

(d) Accurate and where necessary kept up to date (Accuracy).

(e) Not kept in a form which permits identification of Data Subjects for longer than is necessary for the purposes for which the data is Processed (Storage Limitation).

(f) Processed in a manner that ensures its security using appropriate technical and organisational measures to protect against unauthorised or unlawful Processing and against accidental loss, destruction or damage (Security, Integrity and Confidentiality).

(g) Not transferred to another country without appropriate safeguards being in place (Transfer Limitation).

(h) Made available to Data Subjects and Data Subjects allowed to exercise certain rights in relation to their Personal Data (Data Subject's Rights and Requests).

We are responsible for and must be able to demonstrate compliance with the data protection principles listed above (Accountability).

6. LAWFULNESS, FAIRNESS, TRANSPARENCY

6.1 *Lawfulness and Fairness*

Personal data must be Processed lawfully, fairly and in a transparent manner in relation to the Data Subject.

You may only collect, Process and share Personal Data fairly and lawfully and for specified purposes. The GDPR restricts our actions regarding Personal Data to specified lawful purposes. These restrictions are not intended to prevent Processing, but ensure that we Process Personal Data fairly and without adversely affecting the Data Subject.

The GDPR allows Processing for specific purposes, some of which are set out below:

(a) the Data Subject has given his or her Consent;

(b) the Processing is necessary for the performance of a contract with the Data Subject;

(c) to meet our legal compliance obligations;

(d) to protect the Data Subject's vital interests;

(e) required for the performance of a public task on grounds of necessity –this takes two forms:

- because we are carrying out a specific task in the public interest (e.g. providing homelessness services), where the task is laid down by the law (i.e. the overall task is contained in a statute, regulation, statutory guidance or laid down by case law); or

- because we are exercising our own official authority (e.g. fulfilling our duties, carrying out our functions or exercising our powers), where that authority is laid down by the law (i.e. the overall authority is contained in a statute, regulation, statutory guidance or laid down by case law).

(f) to pursue our legitimate interests for purposes where they are not overridden because the Processing prejudices the interests or fundamental rights and freedoms of Data Subjects. The purposes for which we process Personal Data for legitimate interests need to be set out in applicable Privacy Notices.

We accept that, in order to rely on the public task lawful basis, the processing must be strictly required in order for us to perform the relevant public task. This means that if a less privacy invasive course than sharing personal information is available then we should adopt the less invasive course.
You must identify and document the legal ground being relied on for each Processing activity.

6.2 *Consent*

We will only process Personal Data on the basis of one or more of the lawful bases set out in the GDPR, which include Consent.

A Data Subject consents to Processing of their Personal Data if they indicate agreement clearly either by a statement or positive action to the Processing. Consent requires affirmative action so silence, pre-ticked boxes or inactivity are unlikely to be sufficient. If Consent is given in a document which deals with other matters, then the Consent must be kept separate from those other matters.

Data Subjects must be easily able to withdraw Consent to Processing at any time and withdrawal must be promptly honoured. Consent may need to be refreshed if you intend to Process Personal Data for a different and incompatible purpose which was not disclosed when the Data Subject first consented.

Unless we can rely on another lawful basis of Processing, Explicit Consent is usually required for Processing Special Categories of Personal Data and Criminal Convictions Data, for Automated Decision-Making and for cross border data transfers. Usually we will be relying on another lawful basis (and not require Explicit Consent) to Process most types of Special Categories of Personal Data and Criminal Convictions Data.

Where Explicit Consent is required, you must issue a Privacy Notice to the Data Subject to capture Explicit Consent.

You will need to evidence Consent captured and keep records of all Consents in accordance with Related Policies and Privacy Guidelines so that we can demonstrate compliance with Consent requirements.

6.3 *Transparency (Notifying Data Subjects)*

The GDPR requires us to provide detailed, specific information to Data Subjects depending on whether the information was collected directly from Data Subjects or from elsewhere. Such information must be provided through appropriate Privacy Notices which must be concise, transparent, intelligible, easily accessible, and in clear and plain language so that a Data Subject can easily understand them.

Whenever we collect Personal Data directly from Data Subjects, including for human resources or employment purposes, we will provide the Data Subject with all the information required by the GDPR including the identity of the Controller and DPO, how and why we will use, Process, disclose, protect and retain that Personal Data through a Privacy Notice which must be presented when the Data Subject first provides the Personal Data.

When Personal Data is collected indirectly (for example, from a third party or publicly available source), you must provide the Data Subject with all the information required by the GDPR as soon as possible after collecting/receiving the data. You must also check that the Personal Data was collected by the third party in accordance with the GDPR and on a basis which contemplates our proposed Processing of that Personal Data.

7. PURPOSE LIMITATION

7.1 Personal Data must be collected only for specified, explicit and legitimate purposes. It must not be further Processed in any manner incompatible with those purposes.

7.2 You cannot use Personal Data for new, different or incompatible purposes from that disclosed when it was first obtained unless you have informed the Data Subject of the new purposes and they have Consented where necessary.

8. DATA MINIMISATION

8.1 Personal Data must be adequate, relevant and limited to what is necessary in relation to the purposes for which it is Processed.

8.2 You may only Process Personal Data when performing your job duties requires it. You cannot Process Personal Data for any reason unrelated to your job duties.

8.3 You may only collect Personal Data that you require for your job duties: do not collect excessive data. Ensure any Personal Data collected is adequate and relevant for the intended purposes.

8.4 You must ensure that when Personal Data is no longer needed for specified purposes, it is deleted or anonymised in accordance with our data retention schedule as referred to in the Information Asset Registers.

9. ACCURACY

9.1 Personal Data must be accurate and, where necessary, kept up to date. It must be corrected or deleted without delay when inaccurate.

9.2 You will ensure that the Personal Data we use and hold is accurate, complete, kept up to date and relevant to the purpose for which we collected it. You must check the accuracy of any Personal Data at the point of collection and at regular intervals afterwards. You must take all reasonable steps to destroy or amend inaccurate or out-of-date Personal Data.

10. STORAGE LIMITATION

10.1 Personal Data must not be kept in an identifiable form for longer than is necessary for the purposes for which the data is processed.

10.2 You must not keep Personal Data in a form which permits the identification of the Data Subject for longer than needed for the legitimate business purpose or purposes for which we originally collected it including for the purpose of satisfying any legal, accounting or reporting requirements.

10.3 We will maintain retention policies and procedures to ensure Personal Data is deleted after a reasonable time for the purposes for which it was being held, unless a law requires such data to be kept for a minimum time. You must comply with our data retention schedule as referred to in the Information Asset Registers.

10.4 You will take all reasonable steps to destroy or erase from our systems all Personal Data that we no longer require in accordance with our applicable data retention schedules and policies. This includes requiring third parties to delete such data where applicable.

10.5 You will ensure Data Subjects are informed of the period for which data is stored and how that period is determined in any applicable Privacy Notice.

11. SECURITY, INTEGRITY AND CONFIDENTIALITY

11.1 *Protecting Personal Data*

Personal Data must be secured by appropriate technical and organisational measures against unauthorised or unlawful Processing, and against accidental loss, destruction or damage.

We will develop, implement and maintain safeguards appropriate to our size, scope and business, our available resources, the amount of Personal Data that we own or maintain on behalf of others and identified risks (including use of encryption and Pseudonymisation where applicable). We will regularly evaluate and test the effectiveness of those safeguards to ensure security of our Processing of Personal Data.

You are responsible for protecting the Personal Data we hold. You must implement reasonable and appropriate security measures against unlawful or unauthorised Processing of Personal Data and against the accidental loss of, or damage to, Personal Data. You must exercise particular care in protecting Special Categories of Personal Criminal Convictions Data from loss and unauthorised access, use or disclosure.

You must follow all procedures and technologies we put in place to maintain the security of all Personal Data from the point of collection to the point of destruction. You may only transfer Personal Data to third-party service providers who agree to comply with the required policies and procedures and who agree to put adequate measures in place, as requested.

You must maintain data security by protecting the confidentiality, integrity and availability of the Personal Data, defined as follows:

(a) Confidentiality means that only people who have a need to know and are authorised to use the Personal Data can access it.

(b) Integrity means that Personal Data is accurate and suitable for the purpose for which it is processed.

Availability means that authorised users are able to access the Personal Data when they need it for authorised purposes.

You must comply with all applicable aspects of our information Security, Risk and Governance Framework (see below hyperlink) and not attempt to circumvent the administrative, physical and technical safeguards we implement and maintain in accordance with the GDPR and relevant standards to protect Personal Data.

Details are available on the council's Intranet site.

11.2 *Reporting a Personal Data Breach*

The GDPR requires the Council to notify Personal Data Breaches to the ICO and, in certain instances, the Data Subject.

This will be done by the DPO; you should not attempt to notify them yourself.

We have put in place procedures to deal with any suspected Personal Data Breach and will notify Data Subjects or the ICO where we are legally required to do so.

If you know or suspect that a Personal Data Breach has occurred, immediately notify the DPO by reporting it as an information security incident using the form on the council's Intranet site and on the ICT portal.

You must preserve all evidence.

12. TRANSFER LIMITATION

The GDPR restricts data transfers to countries outside the EEA in order to ensure that the level of data protection afforded to individuals by the GDPR is not undermined. You transfer Personal Data originating in one country across borders when you transmit, send, view or access that data in or to a different country.

You may only transfer Personal Data outside the EEA if one of the following conditions applies:

(a) the European Commission has issued a decision confirming that the country to which we transfer the Personal Data ensures an adequate level of protection for the Data Subjects' rights and freedoms;

(b) appropriate safeguards are in place such as binding corporate rules (BCR), standard contractual clauses approved by the European Commission, an approved code of conduct or a certification mechanism, a copy of which can be obtained from the DPO;

(c) the Data Subject has provided Explicit Consent to the proposed transfer after being informed of any potential risks; or

(d) the transfer is necessary for one of the other reasons set out in the GDPR including the performance of a contract between us and the Data Subject, reasons of public interest, to establish, exercise or defend legal claims or to protect the vital interests of the Data Subject where the Data Subject is physically or legally incapable of giving Consent and, in some limited cases, for our legitimate interest.

13. DATA SUBJECT RIGHTS

Data Subjects have rights when it comes to how we handle their Personal Data. These include rights to:

(a) withdraw Consent to Processing at any time;

(b) receive certain information about the Data Controller's Processing activities;

(c) request access to their Personal Data that we hold;

(d) prevent our use of their Personal Data for direct marketing purposes;

(e) ask us to erase Personal Data if it is no longer necessary in relation to the purposes for which it was collected or Processed or to rectify inaccurate data or to complete incomplete data;

(f) restrict Processing in specific circumstances;

(g) challenge Processing which has been justified on the basis of our legitimate interests or in the public interest;

(h) request a copy of an agreement under which Personal Data is transferred outside of the EEA;

(i) object to decisions based solely on Automated Processing, including profiling (ADM);

(j) prevent Processing that is likely to cause damage or distress to the Data Subject or anyone else;

(k) be notified of a Personal Data Breach which is likely to result in high risk to their rights and freedoms;

(l) make a complaint to the ICO;

(m) seek a judicial remedy; and

(n) in limited circumstances, receive or ask for their Personal Data to be transferred to a third party in a structured, commonly used and machine readable format (the right to data portability).

You must verify the identity of an individual requesting data under any of the rights listed above (do not allow third parties to persuade you into disclosing Personal Data without proper authorisation).

To ensure we comply with our Data Subject response process, you must immediately forward any Data Subject request to dataprotection@canterbury.gov.uk

14. ACCOUNTABILITY

14.1 We will implement appropriate technical and organisational measures in an effective manner, to ensure compliance with data protection principles. We are responsible for, and must be able to demonstrate, compliance with the data protection principles.

We will have adequate resources and controls in place to ensure and to document GDPR compliance including:

(a) appointing a suitably qualified DPO who reports to an executive board of management (in our case, the Corporate Management Team);

(b) implementing Privacy by Design when Processing Personal Data and completing PIAs where Processing presents a high risk to rights and

freedoms of Data Subjects;

(c) integrating data protection into internal documents including this Data Protection Policy, Related Policies, Privacy Guidelines or Privacy Notices;

(d) regularly train Council Personnel and Members on the GDPR, this Data Protection Policy, Related Policies and Privacy Guidelines and data protection matters including, for example, Data Subject's rights, Consent, lawful bases, PIA and Personal Data Breaches. We will maintain a record of training attendance; and

(e) regularly testing the privacy measures implemented and conducting periodic reviews and audits to assess compliance, including using results of testing to demonstrate compliance improvement effort.

14.2 *Record Keeping*

The GDPR requires us to keep full and accurate records of all our Data Processing activities.

You must keep and maintain accurate corporate records reflecting our Processing including records of Consents and procedures for obtaining Consents.

14.3 *Training and Audit*

You must undergo all mandatory data privacy related training in accordance with our corporate training programme.

You must regularly review all the systems and processes under your control to ensure they comply with this Data Protection Policy and check that adequate governance controls and resources are in place to ensure proper use and protection of Personal Data.

14.4 *Privacy by Design and Data Protection Impact Assessment (PIA)*

We are required to implement Privacy by Design measures when Processing Personal Data by implementing appropriate technical and organisational measures (like Pseudonymisation) in an effective manner, to ensure compliance with data privacy principles.

You must, in consultation with EKS (ICT), assess what Privacy by Design measures can be implemented on all programs/systems/processes that Process Personal Data by taking into account the following:

(a) the most up to date technology;

(b) the cost of implementation;
(c) the nature, scope, context and purposes of Processing; and

(d) the risks of varying likelihood and severity for rights and freedoms of Data Subjects posed by the Processing.

We will also conduct PIAs in respect to high risk Processing.

You should conduct a PIA (and discuss your findings with the DPO) when implementing major system or business change programs involving the Processing of Personal Data including:

(e) use of new technologies (programs, systems or processes), or changing technologies (programs, systems or processes);

(f) Automated Processing including profiling and ADM;

(g) large scale Processing of Special Categories of Personal Data or Criminal Convictions Data; and

(h) large scale, systematic monitoring of a publicly accessible area.

A PIA must include:

(i) a description of the Processing, its purposes and the Data Controller's legitimate interests if appropriate;

(j) an assessment of the necessity and proportionality of the Processing in relation to its purpose;

(k) an assessment of the risk to individuals; and

(l) the risk mitigation measures in place and demonstration of compliance.

You must complete our PIA template.

14.5 *Automated Processing (Including Profiling) and Automated Decision-Making*

Generally, ADM is prohibited when a decision has a legal or similar significant effect on an individual unless:

(a) a Data Subject has Explicitly Consented;

(b) the Processing is authorised by law; or

(c) the Processing is necessary for the performance of or entering into a contract.

If certain types of Special Categories of Personal Data or Criminal Convictions Data are being processed, then grounds (b) or (c) will not be allowed but such Special Categories of Personal Data and Criminal Convictions Data can be Processed where it is necessary (unless less intrusive means can be used) for substantial public interest like fraud prevention.

If a decision is to be based solely on Automated Processing (including profiling), then Data Subjects must be informed when you first communicate with them of their right to object. This right must be explicitly brought to their attention and presented clearly and separately from other information.

Further, suitable measures must be put in place to safeguard the Data Subject's rights and freedoms and legitimate interests.

We will also inform the Data Subject of the logic involved in the decision making or profiling, the significance and envisaged consequences and give the Data Subject the right to request human intervention, express their point of view or challenge the decision.

A PIA must be carried out before any Automated Processing (including profiling) or ADM activities are undertaken.

14.6 *Direct Marketing*

We are subject to certain rules and privacy laws when marketing to our customers.

For example, a Data Subject's prior consent is required for electronic direct marketing (for example, by email, text or automated calls). The limited exception for existing customers known as 'soft opt in' allows us to send marketing texts or emails if we have obtained contact details in the course of a service transaction to that person, we are marketing similar services, and you gave the person an opportunity to opt out of marketing when first collecting the details and in every subsequent message.

The right to object to direct marketing must be explicitly offered to the Data Subject in an intelligible manner so that it is clearly distinguishable from other information.

A Data Subject's objection to direct marketing must be promptly honoured. If a customer opts out at any time, their details should be suppressed as soon as possible. Suppression involves retaining just enough information to ensure that marketing preferences are respected in the future.

14.7 *Sharing Personal Data*

Generally, we are not allowed to share Personal Data unless certain safeguards and contractual arrangements have been put in place.

You may only share the Personal Data we hold with third parties, such as our service providers if:

(a) they have a need to know the information for the purposes of providing the contracted services;

(b) sharing the Personal Data complies with the Privacy Notice provided to the Data Subject and, if required, the Data Subject's Consent has been obtained;

(c) the third party has agreed to comply with the required data security standards, policies and procedures and put adequate security measures in place;

(d) the transfer complies with any applicable cross border transfer

restrictions; and

(e) a fully executed written contract that contains GDPR approved third party clauses has been obtained.

You must comply with the Kent & Medway Information Sharing Agreement on sharing data with third parties.

15. COUNCILLORS

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

- 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 Data Controller Notification.

- as a member of a political party canvassing for votes or working for a party. This is usually covered by the party's Data Controller Notification. Councillors who are not a member of a political party must make their own arrangements to notify the ICO.

- carrying out casework. In this case the Councillor is the Data Controller and is required to notify the ICO. The Council will register each councillor with the ICO on their behalf.

Where a Councillor is representing a constituent who has made a complaint, the councillor's lawful basis for processing the personal information is where it is needed for the performance of a task carried out in the public interest. Sensitive personal information is processed for reasons of substantial public interest and Schedule 1 Part 2 of the Data Protection Act 2018 'elected representatives responding to requests'. We will not generally seek to rely on consent as the lawful bases for processing in these circumstances.

In representing their constituents, Members may share personal information with us, other councillors and the Member of Parliament.

Personal information held by us should not be used by Members for political purposes unless we and the individuals concerned agree.

When campaigning for election as the representative of a political party, candidates can use personal information, such as mailing lists, legitimately held by their parties. However, personal information Members hold in their role as representatives of local residents, such as complaints casework, should not be used without the consent of the individual.

Members need to arrange for appropriate security to protect their constituents' personal information. They must take into account the nature of the information and the harm that can result.
They should consider what technical and organisational measures, such as use of passwords, computer access privileges, procedures and training, are appropriate to keep the information safe.

Members will keep personal information for the minimum period necessary, usually no longer than 4 years. All information will be held securely and

disposed of confidentially.

16. AMENDMENTS TO THIS DATA PROTECTION POLICY

We reserve the right to amend this Data Protection Policy at any time.

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	-	20 June 2018
Review Date	-	19 June 2019
Reviewer	-	CIGG

Revision History			
Revision Date	**Reviewer (s)**	**Version**	**Description of Revision**
14/06/2018		1.0	