Watton Town Council

Data Protection Policy

June 2024

---

1. INTRODUCTION

This Policy sets out the obligations of Watton Town Council (the "**Council**") regarding data protection and the rights of individuals (including any recipients of any public services), contractors, suppliers, employees and other applicable third parties ("**data subjects**") in respect of their personal data under UK's retained version of the EU Regulation 2016/679 General Data Protection Regulation ("**UK GDPR**").

2. GENERAL DATA PROTECTION REGULATION ("GDPR")

2.1 The General Data Protection Regulation ("**GDPR**") came into effect on 25 May 2018, and was implemented in the United Kingdom under the Data Protection Act 2018.

2.2 This Data Protection Policy ("**Policy**") (and other data protection-related policies operated by the Council) have, where possible, been written with the implementation of the UK GDPR and the Data Protection Act 2018 in mind. In particular, this Policy (and other data protection-related policies operated by the Council) have been prepared and subsequently updated to account for the GDPR's implementation within the domestic jurisdiction of the United Kingdom, following the UK's exit from the European Union.

2.3 Please note that as the GDPR now falls under the direct jurisdiction of the UK as the UK GDPR, there may be changes to the UK GDPR which are not mirrored in the version of the GDPR maintained by the European Union ("**EU GDPR**"). Attention to detail is therefore critical when handling personal data, in ensuring that the correct legislative provisions are followed at all times, especially when handling data which may be subject to the EU GDPR. This Policy and the Council's other documents will be reviewed and updated on an ongoing basis to ensure compliance as the law evolves, and should be continually referenced when handling personal data.

2.4 Please note that all references to the GDPR and the UK GDPR in this Policy also include references to the Data Protection Act 2018.

3. PERSONAL DATA

3.1 The UK GDPR defines "**personal data**" as any information relating to an identified or identifiable natural person (a "data subject"). An identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier, or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural, or social identity of that natural person, either by that data alone or in combination with other identifiers the Council possesses or can reasonably access.

3.2 Personal data also includes Special Categories of Personal Data (as defined in part 7.2) and data which has been replaced with one or more artificial identifiers or pseudonyms so that the person to whom the data relates, cannot be identified without additional information ("**Pseudonymised Personal Data**"). However, it does not include anonymous data or data that has had the identity of an individual permanently removed.

4. ABOUT THIS DATA PROTECTION POLICY

4.1 This Policy sets the Council's obligations regarding the collection, processing, transfer, storage, and disposal of personal data. The procedures and principles set out herein must be followed at all times by the Council, its councillors, officers, employees, agents, contractors, or other parties working on behalf of the Council.

4.2 The Council is committed not only to the letter of the law, but also to the spirit of the law and places high importance on the correct, lawful, and fair handling of all personal data, respecting the legal rights, privacy, and trust of all individuals with whom it deals.

4.3 This Policy applies to all staff unless otherwise indicated. The Policy therefore applies to the Council's councillors, officers, managers, employees (whether part-time or fixed term), consultants, contractors, agents, casual and temporary staff, and agency staff (collectively referred to as "**personnel**", "**you**", "**your**").

4.4 Personnel must read, understand and comply with this Policy when processing personal data on behalf of the Council, and attend training as is required by the Council from time to time on its requirements. This Policy sets out what the Council expects from you for it to comply with the UK GDPR and all other applicable laws, and **compliance with this Policy is mandatory at all times, and in all respects**. Related policies are available to help you interpret and act in accordance with this Policy. You must also always comply with any related policies to this Policy. Any breach of this Policy may result in disciplinary action.

4.5 This Policy will apply regardless of the media on which personal data is stored, or whether it relates to past or present employees, workers, members of the public, clients, supplier contacts, councillors, officers, website users or any other data subjects.

4.6 This Policy may be amended from time to time, and personnel will be directed to certain parts of the Policy as and when it is reviewed and updated. Changes will be made to ensure its provisions continue to meet the relevant legal obligations and reflect best practice.

4.7 This Policy does not form part of any employee's contract of employment or any other personnel's contractual terms.

4.8 All managers, supervisors and councillors have a specific responsibility to operate in accordance with the provisions set out in this Policy, and to ensure that personnel under their supervision understand the standards of behaviour expected of them, and to take action to implement appropriate practices, processes, controls and training to ensure compliance with this Policy and the UK GDPR, and to take further action where any behaviour falls below those requirements.

4.9 Where you have any specific responsibilities under this Policy, or with the processing of personal data, such as reporting a personal data breach, conducting a data protection impact assessment ("**DPIA**"), or otherwise, you must comply with this Policy and any relevant related policies.

4.10 This Policy (and any related policies) are internal facing documents. If this Policy, or any of the Council's other data protection policies are to be shared with third parties (whether at a third party's request of otherwise), this shall at all times be at the discretion of the Clerk (who is the Data Compliance Manager (as defined in clause 14.1)). If you are asked to share any of the Council's data protection policies with a third party, please speak to the Clerk prior to doing so.

4.11 We recognise that the correct and lawful treatment of personal data will maintain confidence in the Council as a local authority and will assist us in providing quality local public services whilst upholding the security of personal data. Protecting the confidentiality and integrity of personal data is a critical responsibility that we take seriously at all times. **It is important to note that even though the Council is a local authority, it can still be exposed to serious and highly detrimental fines and penalties, the value of which will depend on the nature of the breach, for failure to comply with the provisions of the UK GDPR.**

5. THE DATA PROTECTION PRINCIPLES

5.1 This Policy aims to ensure compliance with the UK GDPR. The UK GDPR sets out the following principles with which any party handling personal data must comply. All personal data must be:

5.1.1 Processed lawfully, fairly, and in a transparent manner in relation to the data subject.

5.1.2 Collected for specified, explicit, and legitimate purposes and not further processed in a manner that is incompatible with those purposes.

5.1.3 Adequate, relevant, and limited to what is necessary in relation to the purposes for which it is processed.

5.1.4 Accurate and, where necessary, kept up to date. Every reasonable step must be taken to ensure that personal data that is inaccurate, having regard to the purposes for which it is processed, is erased, or rectified without delay.

5.1.5 Kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data is processed.

5.1.6 Processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction, or damage, using appropriate technical or organisational measures.

5.1.7 Not transferred to another country without appropriate safeguards being in place.

5.1.8 Made available to data subjects, who should be allowed to exercise certain rights in relation to their personal data.

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

6. THE RIGHTS OF DATA SUBJECTS

6.1 The UK GDPR sets out the following rights applicable to data subjects (please refer to the parts of this policy indicated for further details):

6.1.1 The right to be informed (Part 16).

6.1.2 The right of access (Part 17);

6.1.3 The right to rectification (Part 18);

6.1.4 The right to erasure (also known as the 'right to be forgotten') (Part 19);

6.1.5 The right to restrict processing (Part 20);

6.1.6 The right to data portability (Part 21);

6.1.7 The right to object (Part 22); and

6.1.8 Rights with respect to automated decision-making and profiling (Parts 23 and 24).

7. LAWFUL, FAIR, AND TRANSPARENT DATA PROCESSING

7.1 You may only collect, process and share personal data fairly and lawfully and for specified purposes. The UK GDPR restricts our and your actions regarding personal data to specified lawful purposes. These restrictions are not intended to prevent processing, but the UK GDPR seeks to ensure that personal data is processed lawfully, fairly, and transparently, without adversely affecting the rights of the data subject. The UK GDPR states that processing of personal data shall be lawful if at least one of the following applies:

7.1.1 the data subject has given consent to the processing of their personal data for one or more specific purposes;

7.1.2 the processing is necessary for compliance with a legal obligation to which the controller is subject;

7.1.3 the processing is necessary to protect the vital interests of the data subject or of another natural person;

7.1.4 the processing 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;

7.1.5 the processing is necessary for the performance of a contract to which the data subject is a party, or in order to take steps at the request of the data subject prior to entering into a contract with them; or

7.1.6 the processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child.

7.2 The Council does not collect "special categories of personal data" (for example, data concerning the data subject's race, ethnicity, politics, religion, trade union membership, genetics, biometrics (if used for ID purposes), health, sex life, or sexual orientation) when it comes to members of the public, third parties and other individuals outside the Council. However, it will collect "special categories of personal data", even if this is in a limited sense, when it comes to its employees, workers and other staff members. When collecting and/or processing such data, at least one of the following conditions must be met, with the condition in clause 7.2.2 being the most likely to apply (albeit this will not always be the case):

7.2.1 the data subject has given their explicit consent to the processing of such data for one or more specified purposes (unless the UK GDPR or other UK applicable laws prohibit them from doing so);

7.2.2 the processing is necessary for the purpose of carrying out the obligations and exercising specific rights of the controller or of the data subject in the

field of employment, social security, and social protection law (insofar as it is authorised by the UK GDPR or applicable UK law);

7.2.3 the processing is necessary to protect the vital interests of the data subject or of another natural person where the data subject is physically or legally incapable of giving consent;

7.2.4 the controller is a foundation, association, or other non-profit body with a political, philosophical, religious, or trade union aim, and the processing is carried out in the course of its legitimate activities, provided that the processing relates solely to the members or former members of that body or to persons who have regular contact with it in connection with its purposes and that the personal data is not disclosed outside the body without the consent of the data subjects;

7.2.5 the processing relates to personal data which is clearly made public by the data subject;

7.2.6 the processing is necessary for the conduct of legal claims or whenever courts are acting in their judicial capacity; or

7.2.7 the processing is necessary for substantial public interest reasons, on the basis of UK domestic law which shall be proportionate to the aim pursued, shall respect the essence of the right to data protection, and shall provide for suitable and specific measures to safeguard the fundamental rights and interests of the data subject – where any processing is carried out on this basis, the controller must have an appropriate policy document in place, which sets out the controller's procedures for complying with the UK GDPR, and explains the controller's policies in respect of data retention and data erasure of the data processed under this condition.

7.3 You must identify and document the legal ground being relied on for each processing activity.

8. CONSENT

8.1 A controller must only process personal data on one or more of the lawful basis set out in the UK GDPR (and in part 7.1 of this Policy), which includes consent.

8.2 A data subject consents to the 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.

8.3 A data subject 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.

8.4 When processing special categories of personal data or personal data relating to criminal convictions and offences, including data relating to allegations and proceedings ("criminal convictions data"), we will usually rely on a legal basis for processing other than explicit consent or consent if possible. Where explicit consent is relied upon, the Council will need to issue a privacy notice to the data subject so that the Council can demonstrate compliance with consent requirements.

8.5 You must evidence consent captured and keep records of all consents in accordance with the Council's related policies and privacy guidelines, to ensure the Council can demonstrate compliance with consent requirements.

9. SPECIFIED, EXPLICIT, AND LEGITIMATE PURPOSES

9.1 The Council collects and processes the personal data set out in Part 25 of this Policy. This includes:

9.1.1 personal data collected directly from data subjects; and

9.1.2 personal data obtained from third parties.

9.2 The Council only collects, processes, and holds personal data for the specific purposes set out in Part 25 of this Policy (or for other purposes expressly permitted by the UK GDPR).

9.3 Data subjects are kept informed at all times of the purpose or purposes for which the Council uses their personal data. Please refer to Part 16 for more information on keeping data subjects informed.

9.4 You must not 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, where necessary, consented.

10. ADEQUATE, RELEVANT, AND LIMITED DATA PROCESSING

10.1 The Council will only collect and process personal data for and to the extent necessary for the specific purpose or purposes of which data subjects have been informed (or will be informed) as under Part 7.1, above, and as set out in Part 25 below.

10.2 You may only collect personal data that you require for your job duties, so do not collect excessive data beyond what is needed. You should ensure that any personal data collected is adequate and relevant for the intended purpose(s).

10.3 You must ensure that when personal data is no longer needed for specific purposes, it is deleted in accordance with our Register of Retention Periods. Alternatively, the personal data should be anonymised, so it no longer qualifies as personal data.

11. ACCURACY OF DATA AND KEEPING DATA UP TO DATE

11.1 The Council shall ensure that all personal data collected, processed, and held by it is kept accurate and up to date. This includes, but is not limited to, the rectification of personal data at the request of a data subject, as set out in Part 18 below.

11.2 The accuracy of personal data shall be checked when it is collected and at regular intervals thereafter. If any personal data is found to be inaccurate or out-of-date, all reasonable steps will be taken without delay to amend or erase that data, as appropriate.

12. DATA RETENTION

12.1 The Council shall not keep personal data for any longer than is necessary in light of the purpose or purposes for which that personal data was originally collected, held, and processed. This includes not keeping personal data in a form which permits the identification of the data subject for longer than needed for the legitimate business purposes or purposes for which we originally collected it, including for the purpose of satisfying any legal, accounting or reporting requirements.

12.2 When personal data is no longer required, all reasonable steps will be taken to erase or otherwise dispose of it without delay. This includes requiring third parties to delete that data where applicable.

12.3 For full details of the Council's approach to data retention, including retention periods for specific personal data types held by the Council, please refer to our Data Retention Policy and Register of Retention Periods.

12.4 Where necessary, you must ensure that data subjects are informed of the period for which personal data is stored, and how that period is determined in any applicable privacy notice or fair processing notice.

13. SECURE PROCESSING

13.1 The Council shall ensure that all personal data collected, held, and processed is kept secure and protected against unauthorised or unlawful processing and against accidental loss, destruction, or damage. The Council will develop, implement and maintain safeguards appropriate to its size, scope and business, its available resources, the amount of personal data that it holds or maintains on behalf of others and identified risks including the use of encryption and Pseudonymisation where applicable). The Council will regularly evaluate and test the effectiveness of those safeguards to ensure security of its processing or personal data.

13.2 You are responsible for protecting the Personal Data that the Council holds, and you must exercise particular care in protecting Special Categories of Personal Data from loss and unauthorised access, use or disclosure. You must follow all procedures and technologies the Council puts in place to maintain the security of all personal data from the point of collection to the point of destruction. Personal data may only be transferred 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. If you have any concerns about the security of personal data transferred to third-party providers, please contact the Data Compliance Manager immediately.

13.3 You should maintain data security by protecting the confidentiality, integrity and availability of the personal data, defined as follows:

13.3.1 Confidentiality: only people who have a need to know and are authorised to use the personal data can access it;

13.3.2 Integrity: personal data is accurate and suitable for the purposes for which it was processed; and

13.3.3 Availability: authorised users are able to access the personal data when they need it for authorised purposes.

13.4 You must comply with and not attempt to circumvent the administrative, physical and technical safeguards we implement and maintain in accordance with the UK GDPR and relevant standards to protect personal data.

13.5 Further details of the technical and organisational measures which shall be taken are provided in Parts 26 to 31 of this Policy.

14. ACCOUNTABILITY AND RECORD-KEEPING

14.1 The Council's Data Compliance Manager is Jane Scarrott - telephone number: 01953 881007, email address: clerk@wattontowncouncil.gov.uk, postal address: Watton Town Council, Wayland Hall, Middle Street, Watton, Norfolk IP25 6AG.

14.2 The Data Compliance Manager shall be responsible for overseeing the implementation of this Policy and for monitoring compliance with this Policy, the

Council's other data protection-related policies, and with the UK GDPR and other applicable data protection legislation.

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

14.3.1 if you are unsure of the lawful basis which you are relying on to process personal data (see part 7.1);

14.3.2 if you need to rely on consent and/or need to obtain Explicit Consent (see part 8);

14.3.3 if you need to draft privacy notices or fair processing notices;

14.3.4 if you are unsure about the retention period for the personal data being processed (see part 12);

14.3.5 if you are unsure about what security or other measures you need to implement to protect personal data (see part 26 to 31);

14.3.6 if there has been a personal data breach (see part 33) please contact us to request a copy of our data breach policy;

14.3.7 if you are intending to transfer, considering transferring, or are being requested to transfer **ANY PERSONAL DATA** outside of the United Kingdom (see part 32);

14.3.8 if you need any assistance dealing with rights invoked by a data subject (see parts 16 to 22);

14.3.9 whenever you are engaging in a significant, new or change in processing activity which is likely to require a DPIA (see parts 15.3 and 15.4) or plan to use personal data for purposes other than it was collected for;

14.3.10 if you plan to undertake any activities involving Automated Processing including profiling or automated decision making;

14.3.11 if you need help complying with applicable laws when carrying out direct marketing activities (see part 34); or

14.3.12 if you need help with any contracts or other areas in relation to sharing personal data with third parties (including our vendors) (see part 35).

14.4 The Council 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.

14.5 The Council has written procedures and management documents, including a documented decision-making process to ensure traceability by way of an internal privacy policy

14.6 The Council shall keep written internal records of all personal data collection, holding, and processing, which shall incorporate the following information:

14.6.1 The name and details of the Council, its Data Compliance Manager, and any applicable third-party data processors or recipients of personal data;

14.6.2 The purposes for which the Council collects, holds, and processes personal data;

14.6.3 Details of the categories of personal data collected, held, and processed by the Council, and the categories of data subject to which that personal data relates;

14.6.4 Details of any transfers of personal data to countries outside of the UK, including all mechanisms and security safeguards;

14.6.5 Details of how long personal data will be retained by the Council (please refer to the Council's Data Retention Policy and Data Retention Register); and

14.6.6 Detailed descriptions of all technical and organisational measures taken by the Council to ensure the security of personal data.

14.7 The Council has adequate resources and controls in place to ensure and to document UK GDPR compliance including:

14.7.1 appointing the Data Compliance Manager as being responsible for all data protection compliance;

14.7.2 implementing Privacy by Design when processing personal data and completing DPIAs where processing presents a high risk to rights and freedoms of data subjects;

14.7.3 integrating data protection into internal documents including this Policy, privacy notices or fair processing notices and other data protection-related policies;

14.7.4 regularly training personnel on the UK GDPR, this Policy, data protection-related policies and data protection matters including, for example, data subject's rights, consent, legal basis, DPIA and personal data breaches. We will maintain a record of training attendance by personnel; and

14.7.5 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.

15. PRIVACY BY DESIGN & DATA PROTECTION IMPACT ASSESSMENTS

15.1 The Council is required to implement "privacy by design" (being appropriate technical and organisational measures in an effective manner to ensure compliance with the UK GDPR).

15.2 You must assess what privacy by design measures can be implemented on all programmes, processes or systems that process personal data by taking into account the following:

15.2.1 the state of the art;

15.2.2 the cost of implementation;

15.2.3 the nature, scope, context and purposes of processing; and

15.2.4 the risks of varying likelihood and severity for rights and freedoms of the data subject posed by the processing.

15.3 The Council shall carry out DPIAs for any and all new projects and/or new uses of personal data which involve the use of new technologies and the processing involved is likely to result in a high risk to the rights and freedoms of data subjects under the UK GDPR.

15.4 DPIAs shall be overseen by the Data Compliance Manager and shall address the following:

15.4.1 a description of the processing, its purposes and the controller's legitimate interests if appropriate;

15.4.2 an assessment of the necessity and proportionality of the processing in relation to its purpose;

15.4.3 an assessment of the risk to individuals; and

15.4.4 the risk mitigation measures in place and demonstration of compliance.

15.5 The Council will also conduct DPIAs in relation to high risk processing, or when implementing a major system or business change program involving the processing of personal data including:

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

15.5.2 any automated processing including profiling and automated decision making;

15.5.3 large scale processing of special categories of personal data or personal data related to criminal convictions;

15.5.4 large scale, systematic monitoring of publicly accessible data.

16. KEEPING DATA SUBJECTS INFORMED

16.1 The Council shall provide the information set out in Part 16.2 to every data subject, either through privacy notices or fair processing notices. Such notices will be concise, transparent, intelligible, easily accessible, and in clear and plain language so that a data subject can easily understand them:

16.1.1 where personal data is collected directly from data subjects, those data subjects will be informed of its purpose at the time of collection; and

16.1.2 where personal data is obtained from a third party, the relevant data subjects will be informed of its purpose as soon as possible after collecting/receiving the personal data and no later than:

(a) if the personal data is used to communicate with the data subject, when the first communication is made; or

(b) if the personal data is to be transferred to another party, before that transfer is made; or

(c) as soon as reasonably possible and in any event not more than one month after the personal data is obtained.

16.2 The following information shall be provided:

16.2.1 details of the Council including, but not limited to, the identity of its Data Compliance Manager (and where applicable identifying the Council as the controller);

16.2.2 the purpose(s) for which the personal data is being collected and will be processed (as detailed in Part 25 of this Policy) and the legal basis justifying that collection and processing;

16.2.3 where applicable, the legitimate interests upon which the Council is justifying its collection and processing of the personal data;

16.2.4 where the personal data is not obtained directly from the data subject, the categories of personal data collected and processed;

16.2.5 where the personal data is to be transferred to one or more third parties, details of those parties;

16.2.6 where the personal data is to be transferred to a third party that is located outside of the United Kingdom (the "**UK**"), details of that transfer, including but not limited to the safeguards in place (see Part 32 of this Policy for further details);

16.2.7 details of data retention, including the period of retention;

16.2.8 details of the data subject's rights under the UK GDPR, including the right to limit our use and disclosure of their personal data;

16.2.9 details of the data subject's right to withdraw their consent to the Council's processing of their personal data at any time;

16.2.10 details of the data subject's right to complain to the Information Commissioner's Office (the "**supervisory authority**" under the UK GDPR);

16.2.11 where applicable, details of any legal or contractual requirement or obligation necessitating the collection and processing of the personal data and details of any consequences of failing to provide it; and

16.2.12 details of any automated decision-making or profiling that will take place using the personal data, including information on how decisions will be made, the significance of those decisions, and any consequences.

17. DATA SUBJECT ACCESS

The Council has a separate Subject Access Request Policy which provides detailed instructions in the event that the Council receives a subject access request.

18. RECTIFICATION OF PERSONAL DATA

18.1 Data subjects have the right to require the Council to rectify any of their personal data that is inaccurate or incomplete.

18.2 The Council shall rectify the personal data in question, and inform the data subject of that rectification, within one month of the data subject informing the Council of the issue. The period can be extended by up to two months in the case of complex requests. If such additional time is required, the data subject shall be informed.

18.3 In the event that any affected personal data has been disclosed to third parties, those parties shall be informed of any rectification that must be made to that personal data.

19. ERASURE OF PERSONAL DATA

19.1 Data subjects have the right to request that the Council erases the personal data it holds about them in the following circumstances:

19.1.1 it is no longer necessary for the Council to hold that personal data with respect to the purpose(s) for which it was originally collected or processed;

19.1.2 the data subject wishes to withdraw their consent to the Council holding and processing their personal data;

19.1.3 the data subject objects to the Council holding and processing their personal data (and there is no overriding legitimate interest to allow the Council to continue doing so) (see Part 22 of this Policy for further details concerning the right to object);

19.1.4 the personal data has been processed unlawfully;

19.1.5 the personal data needs to be erased in order for the Council to comply with a particular legal obligation.

19.2 Unless the Council has reasonable grounds to refuse to erase personal data, all requests for erasure shall be complied with, and the data subject informed of the erasure, within one month of receipt of the data subject's request. The period can be extended by up to two months in the case of complex requests. If such additional time is required, the data subject shall be informed.

19.3 In the event that any personal data that is to be erased in response to a data subject's request has been disclosed to third parties, those parties shall be informed of the erasure (unless it is impossible or would require disproportionate effort to do so).

20. RESTRICTION OF PERSONAL DATA PROCESSING

20.1 Data subjects may request that the Council ceases processing the personal data it holds about them. If a data subject makes such a request, the Council shall retain only the amount of personal data concerning that data subject (if any) that is necessary to ensure that the personal data in question is not processed further.

20.2 In the event that any affected personal data has been disclosed to third parties, those parties shall be informed of the applicable restrictions on processing it (unless it is impossible or would require disproportionate effort to do so).

21. DATA PORTABILITY

21.1 To facilitate the right of data portability, the Council shall make available all applicable personal data to data subjects in the following formats:

21.1.1 printed media;

21.1.2 digital file in comma separated value (CSV) format; and

21.1.3 locked portable data file (PDF).

21.2 Where technically feasible, if requested by a data subject, personal data shall be sent directly to the required controller.

21.3 All requests for copies of personal data shall be complied with within one month of the data subject's request. The period can be extended by up to two months in the case of complex or numerous requests. If such additional time is required, the data subject shall be informed.

22. OBJECTIONS TO PERSONAL DATA PROCESSING

22.1 Data subjects have the right to object to the Council processing their personal data based on legitimate interests, direct marketing (including profiling), and processing for scientific and/or historical research and statistics purposes.

22.2 Where a data subject objects to the Council processing their personal data based on its legitimate interests, the Council shall cease such processing immediately, unless it can be demonstrated that the Council's legitimate grounds for such processing override the data subject's interests, rights, and freedoms, or that the processing is necessary for a legal obligation, or the conduct of legal claims.

22.3 Where a data subject objects to the Council processing their personal data for direct marketing purposes, the Council shall cease such processing immediately.

23. AUTOMATED DECISION-MAKING

The Council does not use personal data in automated decision-making processes.

24. PROFILING

24.1 The Council uses personal data for profiling purposes. The Council collects employee pay, sickness and absence data.

24.2 When personal data is used for profiling purposes, the following shall apply:

24.2.1 clear information explaining the profiling shall be provided to data subjects, including the significance and likely consequences of the profiling;

24.2.2 appropriate mathematical or statistical procedures shall be used;

24.2.3 technical and organisational measures shall be implemented to minimise the risk of errors. If errors occur, such measures must enable them to be easily corrected; and

24.2.4 all personal data processed for profiling purposes shall be secured in order to prevent discriminatory effects arising out of profiling (see Parts 26 to 31 of this Policy for more details on data security).

24.3 Where automated processing is used, including any profiling, a DPIA must be carried out prior to the processing taking place.

25. PERSONAL DATA COLLECTED, HELD, AND PROCESSED

25.1 The Council collects and holds personal data as set out in its Data Retention Register (a copy of which is available from the Data Compliance Manager).

25.2 Disclosure of personal data, transmission data and storage of data are all managed and monitored in a lawful way. All these processing activities are in line with data protection law:

25.2.1 Processed lawfully, fairly and in a transparent manner.

25.2.2 Collected for specific and legitimate purposes. It cannot be used for anything other than these stated purposes.

25.2.3 Relevant and limited to whatever the requirements are for which they are processed.

25.2.4 Accurate and where necessary kept up to date. Any inaccuracies must be fixed or removed without undue delay.

25.2.5 Stored for only as long as is required.

25.2.6 Secured with an appropriate security solution, which protects against unauthorised or unlawful processing and against accidental loss, destruction or damage.

26. DATA SECURITY - TRANSFERRING PERSONAL DATA AND COMMUNICATIONS

26.1 The Council shall ensure that the following measures are taken with respect to all communications and other transfers involving personal data:

26.1.1 all emails containing personal data must be marked “confidential”;

26.1.2 personal data may only be transmitted over secure networks;

26.1.3 personal data may not be transmitted over a wireless network if there is a reasonable wired alternative;

26.1.4 personal data contained in the body of an email, whether sent or received, should be copied from the body of that email and stored securely. The email itself and associated temporary files should be deleted;

26.1.5 where personal data is to be transferred in hardcopy form, it should be passed directly to the recipient or sent using a signed for courier service;

26.1.6 all personal data transferred physically should be transferred in a suitable container marked "confidential";

26.1.7 no personal data may be transferred to any councillors, employees, workers, agents, contractors, or other parties, whether such parties are working on behalf of the Council or not, without authorisation from the Data Compliance Manager, unless otherwise permitted in the course of your duties or under the provisions of this Policy;

26.1.8 No personal data should be transferred to any device personally belonging to any councillor, officer or employee and personal data may only be transferred to devices belonging to agents, contractors, or other parties working on behalf of the Council where the party in question has agreed to comply fully with the Council's Data Protection Policy and the UK GDPR; and

26.1.9 personal data must not be transferred and/or transported using unencrypted removable media, such as USB drives, because they are insecure.

27. DATA SECURITY - STORAGE

27.1 The Council shall ensure that the following measures are taken with respect to the storage of personal data:

27.1.1 all hardcopies of personal data, along with any electronic copies stored on physical, removable media should be stored securely in a locked box, drawer, cabinet, or similar;

27.1.2 personal data must be handled with care at all times and should not be left unattended or on view;

27.1.3 no personal data should be stored on any mobile device (including, but not limited to, laptops, tablets, and smartphones), whether such device belongs to the Council or otherwise without the formal written approval of the Data Compliance Manager and, in the event of such approval, strictly in accordance with all instructions and limitations described at the time the approval is given, and for no longer than is absolutely necessary;

27.1.4 desks, filing cabinets and cupboards should be kept locked if they hold confidential information of any kind; and

27.1.5 all personal data stored electronically should be backed up daily with backups stored onsite and offsite. All backups are encrypted.

28. DATA SECURITY - DISPOSAL

When any personal data is to be erased or otherwise disposed of for any reason (including where copies have been made and are no longer needed), it should be securely deleted and disposed of. For further information on the deletion and disposal of personal data, please refer to the Council's Data Retention Policy.

29. DATA SECURITY - USE OF PERSONAL DATA

29.1 The Council shall ensure that the following measures are taken with respect to the use of personal data:

29.1.1 no personal data may be shared informally and if a councillor, or an employee, agent, sub-contractor, or other party working on behalf of the Council requires access to any personal data that they do not already have access to, such access should be formally requested from the Data Compliance Manager;

29.1.2 personal data must be handled with care at all times and should not be left unattended or on view to unauthorised employees, agents, sub-contractors, or other parties at any time;

29.1.3 if personal data is being viewed on a computer screen and the computer in question is to be left unattended for any period of time, the user must lock the computer and screen before leaving it;

29.1.4 only personnel who need to access the personal data will be permitted to have access; and

29.1.5 where personal data held by the Council is used for marketing or public information purposes, it shall be the responsibility of the Town Clerk to ensure that the appropriate consent is obtained and that no data subjects have opted out, whether directly or via a third-party service. Evidence of the consent process and opt out must be kept by the Town Clerk and reviewed by the Data Compliance Manager on a monthly basis.

30. DATA SECURITY - IT SECURITY

30.1 The Council shall use the following measures with respect to IT and information security:

30.1.1 Users are requested to ensure that all passwords used to protect personal data should be changed regularly and should not use words or phrases that can be easily guessed or otherwise compromised. All passwords should contain a combination of uppercase and lowercase letters, numbers, and symbols;

30.1.2 under no circumstances should any passwords be written down or shared between any councillors, officers, employees, agents, contractors, or other parties working on behalf of the Council, irrespective of seniority or department. If a password is forgotten, it must be reset using the applicable method. IT staff do not have access to passwords;

30.1.3 all software (including, but not limited to, applications and operating systems) shall be kept up to date. The Council's IT staff, or those engaged by the Council to manage its IT requirements from time to time, shall be responsible for installing any and all security-related updates, and shall do so prudently and punctually when updates are made available by the publisher or manufacturer, unless there are valid technical reasons not to do so; and

30.1.4 no software may be installed on any Council-owned computer or device without the prior approval of the IT Manager and the Data Compliance Manager.

31. ORGANISATIONAL MEASURES

31.1 The Council shall ensure that the following measures are taken with respect to the collection, holding, and processing of personal data:

31.1.1 all councillors, officers, employees, agents, contractors, or other parties working on behalf of the Council shall be made fully aware of both their individual responsibilities and the Council's responsibilities under the UK GDPR and under this Policy, and shall be provided with a copy of this Policy;

31.1.2 only councillors, officers, employees, agents, sub-contractors, or other parties working on behalf of the Council that need access to, and use of, personal data in order to carry out their assigned duties correctly shall have access to personal data held by the Council;

31.1.3 all councillors, officers, employees, agents, contractors, or other parties working on behalf of the Council handling personal data:

(a) will be appropriately trained to do so;

(b) will be appropriately supervised; and

(c) shall be required and encouraged to exercise care, caution, and discretion when discussing work-related matters that relate to personal data, whether in the workplace or otherwise;

31.1.4 methods of collecting, holding, and processing personal data shall be regularly evaluated and reviewed;

31.1.5 all personal data held by the Council shall be reviewed periodically, as set out in the Council's Data Retention Policy;

31.1.6 the performance of those councillors, officers, employees, agents, contractors, or other parties working on behalf of the Council handling personal data shall be regularly evaluated and reviewed;

31.1.7 all councillors, officers, employees, agents, contractors, or other parties working on behalf of the Council handling personal data will be bound to do so in accordance with the principles of the UK GDPR and this Policy by contract;

31.1.8 all agents, contractors, or other parties working on behalf of the Council handling personal data must ensure that any and all of their employees who are involved in the processing of personal data are held to the same conditions as those relevant employees of the Council arising out of this Policy and the UK GDPR; and

31.1.9 where any agent, contractor or other party working on behalf of the Council handling personal data fails in their obligations under this Policy that party shall indemnify and hold harmless the Council against any costs, liability, damages, loss, claims or proceedings which may arise out of that failure.

32. TRANSFERRING PERSONAL DATA TO A COUNTRY OUTSIDE THE UK

32.1 The UK GDPR restricts data transfers to countries outside of the UK to ensure that the level of data protection afforded to individuals by the UK 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.

32.2 The Council does not expect that it will routinely transfer (or otherwise make available remotely) personal data to countries outside of the UK. Any instances

where this happens are likely to be irregular, and you should not be making any such transfers, or providing any remote access in any routine sense as part of your role.

32.3 There are strict rules in place that must be complied with if any data is transferred, or otherwise made remotely available outside of the UK, and the Council will have to comply with such rules if any transfers are so made, or remote access is provided. Therefore, if you need to transfer or make data available outside the UK, or think that this may be required, you must in all cases check with the Clerk (as the Data Compliance Manager) prior to making any transfer, or providing for any data to be made available remotely. The Clerk can then take the necessary steps, and seek any advice which is required, to ensure that the Council complies with the requirements of the UK GDPR, and all other data protection legislation, when making the transfer or making data available remotely.

32.4 In the event that the Council's practices change, and personal data is to be transferred outside of the UK, or made available remotely outside the UK as a matter of course, or on a more regular basis, this policy will be updated to reflect the necessary changes in line with the requirements of the UK GDPR, and other applicable data protection legislation within the UK.

33. DATA BREACH NOTIFICATION

33.1 All personal data breaches must be reported immediately to the Council's Data Compliance Manager.

33.2 If a personal data breach occurs and that breach is likely to result in a risk to the rights and freedoms of data subjects (e.g. financial loss, breach of confidentiality, discrimination, reputational damage, or other significant social or economic damage), the Data Compliance Manager must ensure that the Information Commissioner's Office is informed of the breach without delay, and in any event, within 72 hours after having become aware of it.

33.3 In the event that a personal data breach is likely to result in a high risk (that is, a higher risk than that described under Part 33.2) to the rights and freedoms of data subjects, the Data Compliance Manager must ensure that all affected data subjects are informed of the breach directly and without undue delay.

33.4 Data breach notifications shall include the following information:

33.4.1 the categories and approximate number of data subjects concerned;

33.4.2 the categories and approximate number of personal data records concerned;

33.4.3 the name and contact details of the Data Compliance Manager (or other contact point where more information can be obtained);

33.4.4 the likely consequences of the breach; and

33.4.5 details of the measures taken, or proposed to be taken, by the Council to address the breach including, where appropriate, measures to mitigate its possible adverse effects.

33.5 Please refer to the Council's data breach policy for further details on handling a personal data breach.

34. DIRECT MARKETING

34.1 We are subject to certain rules when marketing to individuals, in particular those who have received public services from us. Marketing is widely defined under the UK GDPR and other data protection legislation, and does not just mean marketing in

a traditional business sense. It can include matters as simple as the Council informing service users of public services, events, or other matters which may be of interest to them.

34.2 For example, a service user's prior consent is required for electronic direct marketing (for example, by email, text or automated calls). Therefore, if the Council is directly contacting service users to inform them about our public services, events, local matters of interest, we are required to comply with the UK GDPR and all other data protection legislation, including gaining prior consent from the service user.

34.3 The limited exception for existing service recipients is known as the "soft opt in". This allows organisations to send marketing texts or emails if they have obtained contact details in the course of providing services to that person, they are marketing or informing in respect of similar services, and they gave the person an opportunity to opt out of marketing when first collecting the details and in every subsequent message.

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

34.5 A service user's objection to direct marketing must be promptly honoured. If a service user 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.

35. SHARING PERSONAL DATA

35.1 Generally, we are not allowed to share personal data with third parties unless certain safeguards and arrangements have been put in place.

35.2 You may only share the personal data we hold with another councillor, officer, employee, agent or representative of the Council if the recipient needs to know the information for their job, and the transfer complies with any applicable cross-border transfer restrictions.

35.3 You may only share the personal data we hold with third parties, such as our service providers if:

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

35.3.2 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;

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

35.3.4 the transfer complies with any applicable cross border transfer restrictions; and

35.3.5 a fully executed written contract that contains UK GDPR approved third party clauses has been obtained.