SAFFRON WALDEN
TOWN COUNCIL

Data Protection and Data Retention Policy

Version	Adopted Date	Minute Reference	Review Date
1	May 2018		May 2022

Data Protection Policy

Introduction

1.1 This Policy sets out the obligations of Saffron Walden Town Council regarding data protection and the rights of its employees, volunteers and the members of the public ("data subjects") in respect of their personal data under EU Regulation 2016/679 General Data Protection Regulation ("GDPR").

1.2 The 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.

1.3 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 employees, agents, contractors, or other parties working on behalf of the Council.

1.4 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.

The Data Protection Principles

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

- Processed lawfully, fairly, and in a transparent manner in relation to the data subject;
- Collected for specified, explicit, and legitimate purposes and not further processed in a manner that is incompatible with those purposes. Further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be considered to be incompatible with the initial purposes;
- Adequate, relevant, and limited to what is necessary in relation to the purposes for which it is processed;
- 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;
- 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. Personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes, or statistical purposes, subject to implementation of the appropriate technical and

organisational measures required by the GDPR in order to safeguard the rights and freedoms of the data subject; and

- 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.

The Rights of Data Subjects

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

The right to be informed (Part 12).

The right of access (Part 13);

The right to rectification (Part 14);

The right to erasure (also known as the 'right to be forgotten') (Part 15);

The right to restrict processing (Part 16);

The right to data portability (Part 17);

The right to object (Part 18); and

Rights with respect to automated decision-making and profiling (Parts 19 and 20).

Lawful, Fair, and Transparent Data Processing

4.1 The GDPR seeks to ensure that personal data is processed lawfully, fairly, and transparently, without adversely affecting the rights of the data subject. The GDPR states that processing of personal data shall be lawful if at least one of the following applies:

- The data subject has given consent to the processing of their personal data for one or more specific purposes;
- 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;
- The processing is necessary for compliance with a legal obligation to which the data controller is subject;
- The processing is necessary to protect the vital interests of the data subject or of another natural person;
- 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 data controller; or
- The processing is necessary for the purposes of the legitimate interests pursued by the data 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.

4.2 If the personal data in question is "special category data" (also known as "sensitive 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), at least one of the following conditions must be met:

- The data subject has given their explicit consent to the processing of such data for one or more specified purposes (unless EU or EU Member State law prohibits them from doing so);
- The processing is necessary for the purpose of carrying out the obligations and exercising specific rights of the data controller or of the data subject in the field of employment, social security, and social protection law (insofar as it is authorised by EU or EU Member State law or a collective agreement pursuant to EU Member State law which provides for appropriate safeguards for the fundamental rights and interests of the data subject);
- 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;
- The data 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;
- The processing relates to personal data which is clearly made public by the data subject;
- The processing is necessary for the conduct of legal claims or whenever courts are acting in their judicial capacity;
- The processing is necessary for substantial public interest reasons, on the basis of EU or EU Member State 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;
- The processing is necessary for the purposes of preventative or occupational medicine, for the assessment of the working capacity of an employee, for medical diagnosis, for the provision of health or social care or treatment, or the management of health or social care systems or services on the basis of EU or EU Member State law or pursuant to a contract with a health professional, subject to the conditions and safeguards referred to in Article 9(3) of the GDPR;
- The processing is necessary for public interest reasons in the area of public health, for example, protecting against serious cross-border threats to health or ensuring high standards of quality and safety of health care and of medicinal products or

medical devices, on the basis of EU or EU Member State law which provides for suitable and specific measures to safeguard the rights and freedoms of the data subject (in particular, professional secrecy); or

- The processing is necessary for archiving purposes in the public interest, scientific or historical research purposes, or statistical purposes in accordance with Article 89(1) of the GDPR based on EU or EU Member State law which shall be proportionate to the aim pursued, respect the essence of the right to data protection, and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject.
-

Specified, Explicit, and Legitimate Purposes

5.1 The Council collects and processes the personal data set out in Part 21 of this Policy. This includes:

- Personal data collected directly from data subjects
- Personal data obtained from third parties.

5.2 The Council only collects, processes, and holds personal data for the specific purposes set out in Part 20 of this Policy (or for other purposes expressly permitted by the GDPR).

5.3 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 12 for more information on keeping data subjects informed.

Adequate, Relevant, and Limited Data Processing

6.1 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 5, above, and as set out in Part 20, below.

Accuracy of Data and Keeping Data Up-to-Date

7.1 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 14, below.

7.2 The accuracy of personal data shall be checked when it is collected and at 12 monthly 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.

Data Retention

8.1 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. Health and Safety documents relating to PPE, Medical Records and any other documentation in line with health and safety legislations may be kept for up to 40 years.

8.2 When personal data is no longer required, all reasonable steps will be taken to erase or otherwise dispose of it without delay.

8.3 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.

Secure Processing

9.1 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. Further details of the technical and organisational measures which shall be taken are provided in Parts 22 to 27 of this Policy.

Accountability and Record-Keeping

10.1 The Council 's Data Protection Contact is the Town Clerk Contact details – townclerk@saffronwalden.gov.uk or Tel: 01799 516501

10.2 The Data Protection Contact 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 GDPR and other applicable data protection legislation.

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

- The name and details of the Council, its Data Protection Contact, and any applicable third-party data processors;
- The purposes for which the Council collects, holds, and processes personal data;
- 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;
- Details of any transfers of personal data to non-EEA countries including all mechanisms and security safeguards;
- Details of how long personal data will be retained by the Council (please refer to the Council's Data Retention Policy); and
- Detailed descriptions of all technical and organisational measures taken by the Council to ensure the security of personal data.

Data Protection Impact Assessments

11.1 The Council shall carry out Data Protection Impact Assessments 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 GDPR.

11.2 Data Protection Impact Assessments shall be overseen by the Data Protection Contact and shall address the following:

- The type(s) of personal data that will be collected, held, and processed;
- The purpose(s) for which personal data is to be used;
- The Council 's objectives;
- How personal data is to be used;
- The parties (internal and/or external) who are to be consulted;
- The necessity and proportionality of the data processing with respect to the purpose(s) for which it is being processed;
- Risks posed to data subjects;
- Risks posed both within and to the Council; and
- Proposed measures to minimise and handle identified risks.

Keeping Data Subjects Informed

12.1 The Council shall provide the information set out in Part 12.2 to every data subject:

- Where personal data is collected directly from data subjects, those data subjects will be informed of its purpose at the time of collection; and
- Where personal data is obtained from a third party, the relevant data subjects will be informed of its purpose:
    - If the personal data is used to communicate with the data subject, when the first communication is made; or
    - if the personal data is to be transferred to another party, before that transfer is made; or
    - as soon as reasonably possible and in any event not more than one month after the personal data is obtained.

12.2 The following information shall be provided:

- Details of the Council including, but not limited to, the identity of its Data Protection Contact;
- The purpose(s) for which the personal data is being collected and will be processed (as detailed in Part 21 of this Policy) and the legal basis justifying that collection and processing;
- Where applicable, the legitimate interests upon which the Council is justifying its collection and processing of the personal data;
- Where the personal data is not obtained directly from the data subject, the categories of personal data collected and processed;
- Where the personal data is to be transferred to one or more third parties, details of those parties;

- Where the personal data is to be transferred to a third party that is located outside of the European Economic Area (the "EEA"), details of that transfer, including but not limited to the safeguards in place (see Part 28 of this Policy for further details);
- Details of data retention;
- Details of the data subject's rights under the GDPR;
- Details of the data subject's right to withdraw their consent to the Council 's processing of their personal data at any time;
- Details of the data subject's right to complain to the Information Commissioner's Office (the "supervisory authority" under the GDPR);
- 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
- 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.

Data Subject Access

13.1 Data subjects may make subject access requests ("SARs") at any time to find out more about the personal data which the Council holds about them, what it is doing with that personal data, and why.

13.2 Data subjects wishing to make a SAR should do using a Subject Access Request Form, sending the form to the Council 's Data Protection Contact.

13.3 Responses to SARs shall normally be made within one month of receipt, however this may be extended by up to two months if the SAR is complex and/or numerous requests are made. If such additional time is required, the data subject shall be informed.

13.4 All SARs received shall be handled by the Council 's Data Protection Contact.

13.4 The Council does not charge a fee for the handling of normal SARs. The Council reserves the right to charge reasonable fees for additional copies of information that has already been supplied to a data subject, and for requests that are manifestly unfounded or excessive, particularly where such requests are repetitive.

Rectification of Personal Data

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

14.2 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.

14.3 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.

Erasure of Personal Data

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

- 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;
- The data subject wishes to withdraw their consent to the Council holding and processing their personal data;
- 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 18 of this Policy for further details concerning the right to object);
- The personal data has been processed unlawfully;
- The personal data needs to be erased in order for the Council to comply with a particular legal obligation;
- The personal data is being held and processed for the purpose of providing information society services to a child.

15.2 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.

15.3 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).

Restriction of Personal Data Processing

16.1 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.

16.2 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).

Data Portability

17.1 The Council processes personal data using automated means. This includes electronic drives, Sage Payroll, Sage HR, Sage Accounts, HMRC Online, Nest Pensions, Email, DVLA Licencing, CHAS, Constructionline, ECA/ECS, CITB, purposes of an online tender/contract work, RAM Tracking, Gas Safe.

17.2 Where data subjects have given their consent to the Council to process their personal data in such a manner, or the processing is otherwise required for the performance of a contract between the Council and the data subject, data subjects have the right, under the GDPR, to receive a copy of their personal data and to use it for other purposes (namely transmitting it to other data controllers).

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

- Paper copies;
- Electronic copies sent via email.

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

17.5 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.

Objections to Personal Data Processing

18.1 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.

18.2 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 the conduct of legal claims.

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

18.4 Where a data subject objects to the Council processing their personal data for scientific and/or historical research and statistics purposes, the data subject must, under the GDPR, "demonstrate grounds relating to his or her particular situation". The Council is not required to comply if the research is necessary for the performance of a task carried out for reasons of public interest.

Automated Decision-Making

19.1 The Council uses personal data in automated decision-making processes. This includes the use of RAM Vehicle tracking to verify your working hours.

19.2 Where such decisions have a legal (or similarly significant effect) on data subjects, those data subjects have the right to challenge such decisions under the GDPR, requesting human intervention, expressing their own point of view, and obtaining an explanation of the decision from the Council.

19.3 The right described in Part 19.2 does not apply in the following circumstances:

- The decision is necessary for the entry into, or performance of, a contract between the Council and the data subject;
- The decision is authorised by law; or
- The data subject has given their explicit consent.

Personal Data Collected, Held, and Processed

20.1 The following personal data is collected, held, and processed by the Council (for details of data retention, please refer to the Council 's Data Retention Policy):

Type of Data	**Purpose of Data**
Surname	Necessary for the performance of an employment contract
Forenames	Necessary for the performance of an employment contract
Address, including postcode	Necessary for the performance of an employment contract
Telephone number	Necessary for the performance of an employment contract
Nationality	For compliance with a legal obligation (Right to work in the UK)
Date of Birth	Necessary for the performance of an employment contract – (Driving insurance, Minimum wage, Security Checks)

Type of Data	Purpose of Data
Driving Licence details (Including points)	For compliance with a legal obligation & Necessary for the performance of an employment contract – (Driving insurance)
National Insurance Number	Necessary for the performance of an employment contract and/or for any emergency contact details
Marriage status	Necessary for the performance of an employment contract and/or for any emergency contact details
Criminal Convictions	Necessary for the performance of an employment contract (DBS & Vetting)
Emergency Contact details (Name and number)	Necessary to protect the vital interests of the data subject. (Required in case of an emergency)
Conditions of employment	Necessary for the performance of an employment contract
Holiday records	Necessary for the performance of an employment contract
DBS Checks	Necessary for the performance of an employment contract & For compliance with a legal obligation.
Vetting Checks	Necessary for the performance of an employment contract & For compliance with a legal obligation.
Working time opt out form	For compliance with a legal obligation.
Training records (Including qualifications)	Necessary for the performance of an employment contract

Type of Data	Purpose of Data
PPE Check list	Necessary for the performance of an employment contract, for compliance with a legal obligation & to protect the vital interests of the data subject.
Appraisal Records	Necessary for the performance of an employment contract.
Timesheet records.	Necessary for the performance of an employment contract
P45 & P60	Necessary for the performance of an employment contract & For compliance with a legal obligation.
Disciplinary and/or capability records	For the purposes of the legitimate interest pursued by the data controller & Necessary for the performance of an employment contact
Pay records	Necessary for the performance of an employment contract & For compliance with a legal obligation.
Medical records / health questionnaires	Necessary to protect the vital interests of the data subject & for compliance with a legal obligation.
Sickness records	Necessary to protect the vital interests of the data subject & for compliance with a legal obligation.
Training cost agreement	Necessary for the performance of an employment contract
Bank Account Details	Necessary for the performance of an employment contact
P11D	For compliance with a legal obligation.

Data Security - Transferring Personal Data and Communications

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

- All emails containing personal data must be marked "confidential";
- Personal data may be transmitted over secure networks only; transmission over unsecured networks is not permitted in any circumstances; sent securely through AVG (Avast Business) Cloud care anti-virus software.
- Personal data may not be transmitted over a wireless network if there is a wired alternative that is reasonably practicable;
- 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 should be deleted. All temporary files associated therewith should also be deleted off the system. If these are being deleted from an email this does have a 90-day retention within the 'exchange' however after the 90 days this is deleted permanently, only the user of the email who deleted would be able to reinstate this. Data being deleted from the systems Drives or from a document within the servers will be held in the cloud for 30-days, on the 30th day this will automatically be deleted permanently, only the Council IT management company would be able to reinstate the documents deleted.
- Where personal data is to be sent by facsimile transmission the recipient should be informed in advance of the transmission and should be waiting by the fax machine to receive the data;
- Where personal data is to be transferred in hardcopy form it should be passed directly to the recipient or sent using secure postal mail service.
- All personal data to be transferred physically, whether in hardcopy form or on removable electronic media shall be transferred in a suitable container marked "confidential".

Data Security - Storage

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

- All electronic copies of personal data should be stored securely using passwords and with restricted access.
- 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.
- All personal data stored electronically should be backed up daily with backups stored off site in a locked safe with restricted access.
- 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 Protection Contact. In the event of such approval, information will be held strictly in accordance with all

instructions and limitations described at the time the approval is given, and for no longer than is absolutely necessary.

- No personal data should be transferred to any device personally belonging to an 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 letter and spirit of this Policy and of the GDPR (which may include demonstrating to the Council that all suitable technical and organisational measures have been taken).

Data Security - Disposal

23.1 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.

Data Security - Use of Personal Data

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

- No personal data may be shared informally and if 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 Protection Contact.
- No personal data may be transferred to any employees, agents, contractors, or other parties, whether such parties are working on behalf of the Council or not, without the authorisation of the Data Protection Contact.
- 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.
- 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.

Data Security - IT Security

25.1 The Council shall ensure that the following measures are taken with respect to IT and information security:

- 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 must contain a combination of uppercase and lowercase letters, numbers. All software used by the Council is designed to require such passwords.

- Under no circumstances should any passwords be written down or shared between any 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.
- All software (including, but not limited to, applications and operating systems) shall be kept up-to-date. The Council 's IT staff shall be responsible for installing any and all security-related updates not more than 1 week after the updates are made available by the publisher or manufacturer.
- No software may be installed on any Council -owned computer or device unless it is in compliance with the Town Council's IT policy and protocols.

Organisational Measures

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

- All 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 GDPR and under this Policy, and shall be provided with a copy of this Policy;
- Only 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;
- All employees, agents, contractors, or other parties working on behalf of the Council handling personal data will be appropriately trained to do so;
- All employees, agents, contractors, or other parties working on behalf of the Council handling personal data will be appropriately supervised;
- All employees, agents, contractors, or other parties working on behalf of the Council handling personal data 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;
- Methods of collecting, holding, and processing personal data shall be regularly evaluated and reviewed;
- All personal data held by the Council shall be reviewed periodically, as set out in the Council 's Data Retention Policy;
- The performance of those employees, agents, contractors, or other parties working on behalf of the Council handling personal data shall be regularly evaluated and reviewed;
- All 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 GDPR and this Policy by contract;
- 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 GDPR; and

- 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.

Transferring Personal Data to a Country Outside the EEA

27.1 The Council does not transfer ('transfer' includes making available remotely) personal data to countries outside of the EEA.

Data Breach Notification

28.1 All personal data breaches must be reported immediately to the Council 's Data Protection Contact.

28.2 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 Protection Contact 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.

28.3 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 28.2) to the rights and freedoms of data subjects, the Data Protection Contact must ensure that all affected data subjects are informed of the breach directly and without undue delay.

28.4 Data breach notifications shall include the following information:

- The categories and approximate number of data subjects concerned;
- The categories and approximate number of personal data records concerned;
- The name and contact details of the Council 's data protection contact (or other contact point where more information can be obtained);
- The likely consequences of the breach;
- 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.

Implementation of Policy

29.1 This Policy shall be deemed effective as of Friday 25th May 2018 No part of this Policy shall have retroactive effect and shall thus apply only to matters occurring on or after this date.

Data Retention Policy

Introduction

1.1 This Policy sets out the obligations of Saffron Walden Town Council regarding retention of personal data collected, held, and processed by the Council in accordance with EU Regulation 2016/679 General Data Protection Regulation ("GDPR").

1.2 The 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.

1.3 The GDPR also addresses "special category" personal data (also known as "sensitive" personal data). Such data includes, but is not necessarily limited to, 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.

1.4 Under the GDPR, personal data shall be kept in a form which permits the identification of data subjects for no longer than is necessary for the purposes for which the personal data is processed. In certain cases, personal data may be stored for longer periods where that data is to be processed for archiving purposes that are in the public interest, for scientific or historical research, or for statistical purposes (subject to the implementation of the appropriate technical and organisational measures required by the GDPR to protect that data).

1.5 In addition, the GDPR includes the right to erasure or "the right to be forgotten". Data subjects have the right to have their personal data erased (and to prevent the processing of that personal data) in the following circumstances:

a) Where the personal data is no longer required for the purpose for which it was originally collected or processed (see above);

b) When the data subject withdraws their consent;

c) When the data subject objects to the processing of their personal data and the Council has no overriding legitimate interest;

d) When the personal data is processed unlawfully (i.e. in breach of the GDPR);

e) When the personal data has to be erased to comply with a legal obligation; or

f) Where the personal data is processed for the provision of information society services to a child.

1.6 For further information on other aspects of data protection and compliance with the GDPR, please refer to the Council 's Data Protection Policy.

Aims and Objectives

2.1 The primary aim of this Policy is to set out limits for the retention of personal data and to ensure that those limits, as well as further data subject rights to erasure, are complied with. By extension, this Policy aims to ensure that the Council complies fully with its obligations and the rights of data subjects under the GDPR.

2.2 In addition to safeguarding the rights of data subjects under the GDPR, by ensuring that excessive amounts of data are not retained by the Council, this Policy also aims to improve the speed and efficiency of managing data.

Scope

3.1 This Policy applies to all personal data held by the Council and by third-party data processors processing personal data on the Council 's behalf.

3.2 Personal data, as held by the above is stored in the following ways and in the following locations:

g) The Council's servers, located in a cupboard with restricted access, this is located at the Council 's main office.

h) Computers permanently located in the Council 's premises at 11 Emson Close, Saffron Walden, Essex

i) Laptop computers and other mobile devices provided by the Council to its employees (with limited use where possible).

j) Physical records stored in the main office.

k) 3rd party data processors, ie use of "the Cloud"

Data Subject Rights and Data Integrity

4.1 All personal data held by the Council is held in accordance with the requirements of the GDPR and data subjects' rights thereunder, as set out in the Council 's Data Protection Policy.

4.2 Data subjects are kept fully informed of their rights, of what personal data the Council holds about them, how that personal data is used as set out in Parts 12 and 13 of the Council 's Data Protection Policy, and how long the Council will hold that personal data (or, if no fixed retention period can be determined, the criteria by which the retention of the data will be determined).

4.3 Data subjects are given control over their personal data held by the Council including the right to have incorrect data rectified, the right to request that their personal data be deleted or otherwise disposed of (notwithstanding the retention periods otherwise set by this Data Retention Policy), the right to restrict the Council 's use of their personal data, the right to data portability, and further rights relating to automated decision-making and profiling , as set out in Parts 14 to 20 of the Council 's Data Protection Policy.

Technical and Organisational Data Security Measures

5.1 The following technical measures are in place within the Council to protect the security of personal data. Please refer to Parts 22 to 26 of the Council 's Data Protection Policy for further details:

l) All emails containing personal data must be marked "confidential";

m) Personal data may only be transmitted over secure networks;

n) Personal data may not be transmitted over a wireless network if there is a reasonable wired alternative;

o) 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;

p) Where personal data is to be sent by facsimile transmission the recipient should be informed in advance and should be waiting to receive it;

q) Where personal data is to be transferred in hardcopy form, it should be passed directly to the recipient or sent using a secure postal mail service.

r) All personal data transferred physically should be transferred in a suitable container marked "confidential";

s) No personal data may be shared informally and if access is required to any personal data, such access should be formally requested from the Data Protection Contact.

t) All hardcopies of personal data, along with any electronic copies stored on physical media should be stored securely;

u) No personal data may be transferred to any employees, agents, contractors, or other parties, whether such parties are working on behalf of the Council or not, without authorisation;

v) Personal data must be handled with care at all times and should not be left unattended or on view;

w) Computers used to view personal data must always be locked before being left unattended;

x) No personal data should be stored on any mobile device, whether such device belongs to the Council or otherwise without the formal written approval of the Data Protection Contact and then strictly in accordance with all instructions and limitations described at the time the approval is given, and for no longer than is absolutely necessary;

y) No personal data should be transferred to any device personally belonging to an 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 GDPR;

z) All personal data stored electronically should be backed up daily with backups

stored off site in a locked safe with restricted access.

aa) All electronic copies of personal data should be stored securely using passwords and with restricted access.

bb) All passwords used to protect personal data should be changed regularly and should must be secure;

cc) Under no circumstances should any passwords be written down or shared. If a password is forgotten, it must be reset using the applicable method. IT staff do not have access to passwords;

dd) All software should be kept up-to-date. Security-related updates should be installed not more than 1 week after becoming available.

ee) No software may be installed on any Council -owned computer or device without approval.

5.2 The following organisational measures are in place within the Council to protect the security of personal data. Please refer to Part 27 of the Council 's Data Protection Policy for further details:

a) All employees and 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 GDPR and under the Council 's Data Protection Policy;

b) Only employees and other parties working on behalf of the Council that need access to, and use of, personal data in order to perform their work shall have access to personal data held by the Council;

c) All employees and other parties working on behalf of the Council handling personal data will be appropriately trained to do so;

d) All employees and other parties working on behalf of the Council handling personal data will be appropriately supervised;

e) All employees and other parties working on behalf of the Council handling personal data should exercise care and caution when discussing any work relating to personal data at all times;

f) Methods of collecting, holding, and processing personal data shall be regularly evaluated and reviewed;

g) The performance of those employees and other parties working on behalf of the Council handling personal data shall be regularly evaluated and reviewed;

h) All employees and other parties working on behalf of the Council handling personal data will be bound by contract to comply with the GDPR and the Council 's Data Protection Policy;

i) All agents, contractors, or other parties working on behalf of the Council handling personal data must ensure that any and all relevant employees are held to the same conditions as those relevant employees of the Council arising out of the GDPR and the Council 's Data Protection Policy;

j) Where any agent, contractor or other party working on behalf of the Council

handling personal data fails in their obligations under the GDPR and/or the Council 's Data Protection 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.

Data Disposal

6.1 Upon the expiry of the data retention periods set out below in Part 7 of this Policy, or when a data subject exercises their right to have their personal data erased, personal data shall be deleted, destroyed, or otherwise disposed of as follows:

(b) Personal data stored electronically (including any and all backups thereof) shall be deleted off the system.

(c) Special category personal data stored electronically (including any and all backups thereof) shall be deleted off the system.

(d) Personal data stored in hardcopy form shall be shredded and discarded securely.

(e) Special category personal data stored in hardcopy form shall be shredded and discarded securely.

(f) Any computer on which the hard drive breaks will either be kept in a lockable safe with only access to those permitted or they will be destroyed with a certificate for 'proof of destruction'.

(g) Any CD's will be destroyed.

Data Retention

7.1 As stated above, and as required by law, the Council shall not retain any personal data for any longer than is necessary in light of the purpose(s) for which that data is collected, held, and processed.

7.2 Different types of personal data, used for different purposes, will necessarily be retained for different periods **(**and its retention periodically reviewed), as set out below.

7.3 When establishing and/or reviewing retention periods, the following shall be taken into account:

(a) The objectives and requirements of the Council;

(b) The type of personal data in question;

(c) The purpose(s) for which the data in question is collected, held, and processed;

(d) The Council 's legal basis for collecting, holding, and processing that data;

(e) The category or categories of data subject to whom the data relates;

7.4 If a precise retention period cannot be fixed for a particular type of data, criteria shall be established by which the retention of the data will be determined, thereby ensuring that the data in question, and the retention of that data, can be regularly reviewed against those criteria.

7.5 Notwithstanding the following defined retention periods, certain personal data may be deleted or otherwise disposed of prior to the expiry of its defined retention period where a decision is made within the Council to do so (whether in response to a request by a data subject or otherwise).

7.6 In limited circumstances, it may also be necessary to retain personal data for longer periods where such retention is for archiving purposes that are in the public interest, for scientific or historical research purposes, or for statistical purposes. All such retention will be subject to the implementation of appropriate technical and organisational measures to protect the rights and freedoms of data subjects, as required by the GDPR.

Roles and Responsibilities

8.1 The Council ’s Data Protection Contact is the Town Clerk

8.2 The Data Protection Contact 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 (including, but not limited to, its Data Protection Policy), and with the GDPR and other applicable data protection legislation.

8.3 The Council as an authoritative body shall be directly responsible for ensuring compliance with the above data retention periods throughout the Council.

8.4 Any questions regarding this Policy, the retention of personal data, or any other aspect of GDPR compliance should be referred to the Data Protection Contact.

Implementation of Policy

9.1 This Policy shall be deemed effective as of Friday 25th May 2018. No part of this Policy shall have retroactive effect and shall thus apply only to matters occurring on or after this date.

Subject Access Form

Important Information

Saffron Walden Town Council sometimes collects, holds, and processes certain personal data about our employees, volunteers and the general public. ("data subjects"). As a data subject, you have a legal right, under EU Regulation 2016/679 General Data Protection Regulation ("GDPR") to find out about our use of your personal data as follows:

Confirmation that your personal data is being processed by us;

Access to your personal data;

How we use your personal data and why;

Details of any sharing or transfers of your personal data;

How long we hold your personal data;

Details of your rights under the GDPR including, but not limited to, your rights to withdraw your consent to our use of your personal data at any time and/or to object to our processing of it.

No fee is payable under normal circumstances. We reserve the right to charge a reasonable fee for requests that are manifestly unfounded, excessive, or repetitive. Such charges will be based only on the administrative cost that we will incur in order to respond.

Please complete the required information overleaf and return it to the Town Clerk, Data Protection Contact, 11 Emson Close, Saffron Walden, Essex, or email townclerk@saffronwalden.gov.uk

You do not have to use this form and may instead write to us using the same contact details.

After receiving your subject access request, we may contact you to request additional supporting information and/or proof of your identity. This helps us to safeguard your privacy and personal data.

We will respond to all subject access requests within one month of receipt and will aim to provide all required information to you within the same period. If we require more information from you, or if your request is unusually complicated, we may require more time and will inform you accordingly.

If you are making a subject access request on someone else's behalf, please contact the Town Clerk, Data Protection Contact at townclerk@saffronwalden.gov.uk **before** making your request.

Saffron Walden Town Council

Subject Access Request Form

Your Details

Title:	
Forename(s):	
Surname:	
Address:	
Telephone Number:	
Email Address:	

Information Being Requested

Please provide specific details (along with any relevant dates) of the information being requested and any additional information that may help us to locate your personal data and to confirm your identity.

By completing this form, you are making a subject access request under the GDPR for personal data collected, processed, and held about you by us that you are entitled to receive.

Declaration

By signing below, **you confirm that you are the data subject named in this Subject Access Request Form**. You warrant that you are the individual named and will fully indemnify Saffron Walden Town Council for all losses and expenses incurred if you are not. We cannot accept requests in respect of your personal data from anyone else, including members of your family.

Name:	
Signature:	
Date:	

Full Privacy Notice:

This Privacy Notice tells you what to expect when Saffron Walden Town Council collects and uses your personal data for employment and application for employment purposes in accordance with the Data Protection Act / General Data Protection Regulation.

	Complete the following fields:
Data Controller	Saffron Walden Town Council
Our contact details:	The Data Protection Contact – townclerk@saffronwalden.gov.uk
The purpose we are processing your personal data for is	Administration and maintenance of employee records and the activities required for the support and management of our current and former workers, applicants and Elected members, including: 1. Recruitment, Selection & Termination, 2. DBS checks, 3. Pay, Allowances, Pensions, Deductions and Benefits, 4. Working Arrangements and Leave, 5. Managing Performance and Conduct, 6. Managing Attendance and Employee Support, 7. Managing Change, and 8. Appraisals, Supervisions and Training. 9. Police Vetting's
Using your personal information for other purposes	We will not process your personal data for any other purpose than that for which it was collected, without first providing you with information on that other purpose and seeking your consent if applicable; except were we are required to disclose your personal data in accordance with legislation for example in relation to the prevention and detection of crime, counter

	terrorism, safeguarding, legal proceedings or to protect interests of you or another.
Organisations acting on our behalf to process your personal data	Pension Schemes
The fair and lawful basis we are processing your personal data on is	**Processing basis 1:** Processing is necessary in order to meet our duties as an employer (Article 6 1 c compliance with a legal obligation and Article 9 2 b carrying out obligations and exercising specific rights in relation to employment). **Processing basis 2:** Processing necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract (Article 6 1 b re contract of employment or for the provision of a service to commercial client.) **Processing basis 3:** Processing necessary for compliance with a legal obligation. **Processing basis 4**: Processing is necessary for a legitimate interest of the Council. **Processing basis 5:** Necessary to protect the vital interests of the data subject. **Processing basis 6:** The data subject has given consent to the processing of his/her personal data for one or more specific purposes. (Article 6 1 a and 9 2 a)
Am I required to provide the Council with my personal data	You are required to provide the minimum personal data necessary for us to manage your employment application and if successful your employment with us. Failure to provide the minimum necessary personal data we require could prevent us offering you employment or impact on your pay and conditions.

Does the Council's processing of my personal data involve automated decision-making, including profiling?	Yes. Automated decision making takes place with regards to Vehicle tracking and employees timesheets.
Can I withdraw my consent for processing	You can withdraw your consent for the processing of your personal data at any time if that processing is on the sole basis of your consent (Processing basis 6).
Who we will share your personal data with	HM Revenue and Customs; Pension Schemes; The Disclosure and Barring Service; Central Government Departments; Financial organisations; Educators and Examining bodies; Professional Bodies; Law enforcement agencies and bodies; Courts and Tribunals; Legal representatives; Ombudsman and Regulatory bodies; Service providers; Debt collection and tracing agencies; Trade Unions; Licensing authorities;

	With your explicit consent: Credit Reference Agencies; Mortgage Providers, Housing Associations and landlords. To support TUPE arrangements the minimum necessary personal data and special categories of personal data will be passed to the new employer transferee.
Transfers of personal data to a third country	Not routinely disclosed or transferred to recipients outside of the UK
How long we will retain your personal data for	Your personal data is retained in accordance with our legal obligations, which are set out the Human Resources section of our retention schedule.
What are my rights in relation to my personal data?	You have the right to access the personal data we hold about you; to request we rectify or erase your personal data; to object to or restrict processing in certain circumstances; and a right of data portability in certain circumstances. More information on your rights can be found at – www.saffronwalden.gov.uk
Who can I complain to?	If you are dissatisfied with how we have processed your personal data you can contact the Data Protection Contact to request an internal review. If you are dissatisfied with the outcome of the internal review, you have the right to appeal directly to the Information Commissioner for an independent review. https://ico.org.uk/concerns/
Contact details for our Data	The Town Clerk

Protection Office	11 Emson Close, Saffron Walden, Essex townclerk@saffronwalden.gov.uk Tel: 01799 516501

GDPR Record of Personal Data Processing			
Processing Ref	N/A	Date of Review	
Nature of Activity	Human Resources		
Function	Human Resources		
Description of functions carried out	Managing and supporting Human Resource activities for Current and former workers (including Employees, Agency / Casual / Office Holders, Consultants, Interims, Interns, work experience and volunteers) Pensioners; Applicants (current and unsuccessful); Individuals requiring DBS checks; Individuals attending training courses organised by the Company Safeguarding.		

Data Controller / Data Processor Details	
Data Controller	The Town Clerk of Saffron Walden Town Council
Details of any Joint Data Controllers	N/A
Details of any contracts in place	N/A
Details of any Data Processors	Pension provider, HMRC.
Details of any Data Processor Agreements	Agreement in place with pension provider.
Processing Purpose Details	
Description of the purpose (reason) for processing personal data	Administration and maintenance of employee records and the activities required for the support and management of our current and former workers, applicants and Elected members, including: Recruitment, Selection & Termination, DBS checks, Police Vetting, Pay, Allowances, Pensions, Deductions and Benefits, Working Arrangements and Leave, Managing Performance and Conduct, Managing Attendance and Employee Support, Managing Change, and

	Appraisals, Supervisions and Training. Administration and maintenance of employee records and the activities required for the support and management of them for our commercial clients, including: Recruitment, Selection & Termination, DBS checks, Police Vetting Pay, Allowances, Pensions, Deductions and Benefits, Working Arrangements and Leave, Managing Performance and Conduct, Managing Attendance and Employee Support, Managing Change, and Appraisals, Supervisions and Training.
Basis for the processing of the personal data	**Processing basis 1:** Processing is necessary in order to meet our duties as an employer (Article 6 1 c compliance with a legal obligation and Article 9 2 b carrying out obligations and exercising specific rights in relation to employment). The main employment law statutes are:- Equal Pay Act 1970; Health & Safety at Work etc. Act 1974; Rehabilitation of Offenders Act 1974; Trade Union and Labour Relations (Consolidation) Act 1992; Employment Tribunals Act 1996; Employment Rights Act 1996; Public Interest Disclosure Act 1998; National Minimum

	Wage Act 1998; Employment Relations Act 1999; Employment Act 2002; Employment Relations Act 2004; Disability Discrimination Act 2005; Immigration, Asylum and Nationality Act 2006; and Equalities Act 2010 Payroll information is processed in accordance with HM Revenue and Customs regulations and standards. In addition, there is a substantial amount of secondary legislation in the form of regulations which contain further provisions and may be supported by Codes of Practice. **Processing basis 2:** Processing necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract (Article 6 1 b re contract of employment or for the provision of a service to commercial client.) **Processing basis 3:** Processing necessary for compliance with a legal obligation. **Processing basis 4**: Processing is necessary for a legitimate interest of the Council **Processing basis 5:** Necessary to protect the vital interests of the data subject.

Link to privacy notice and/or Link to awareness raising materials	Prospective workers are informed about the processing of their personal data through information included in the recruitment form and process. Workers are informed about the processing of their personal data through information included in the contract of employment / letter of engagement / letter leaving and at the point of collection when appropriate through internal policies. Privacy Notices are in place for the processing of the personal data of workers when this is done as part of a commercial contract. For the provision of training to individuals not employed by the Council at point of registration it is explained to the individual what personal data is required from them for the purpose of providing the training and levying the appropriate charge.
Details of any Privacy Impact Assessments carried out	N/A
Does the processing involve automated decision making, including profiling	Yes. Automated decision making takes place with regards to Vehicle tracking and employees timesheets.
Is personal data used for direct marketing purposes	No
Details of Personal Data Processing	
Categories of data subjects	Current and former workers including Employees, Agency / Casual / Supply Workers, Office Holders, Consultants, Interims, Interns, work experience and volunteers; Pensioners;

	Applicants (current and unsuccessful); Employee's next of kin; Individuals requiring DBS checks; Individuals requiring Vetting checks; Individuals attending training courses organised by the Company; Employment and Personal Referees.
Categories of personal data being processed	Personal details; Employment details; Business activities; Financial details; Education and training details; We also process special categories of personal data: Physical or mental health; Offences and alleged offences; Gender; Trade Union Membership for individuals who have requested deductions from payroll or for recording Trade Union Facility Time.
Source of the personal data	Personal data will be received from a wide range of sources to support recruitment, ongoing employment, training, leavers and pension activities including the data subject, their representative, next of kin or other family member, other workers, referees, educators and examining bodies, health professionals, partner

	agencies, Pension Schemes, Disclosure and Barring Service, Police Vetting, Courts and law enforcement bodies, HM Revenue and Customs.
How is the personal data collected?	Through established activities linked to the recruitment, employment, training, termination and pension rights of the data subject or commercial contracts.
When is the personal data collected?	Through established activities linked to the recruitment, employment, training, termination and pension rights of the data subject or commercial contracts.
Estimate of the number of records held	49 employees and 49 Leavers
Retention period(s) in place for the personal data	See Human Resources Retention Schedule which is based on national guidance and business need.
Recipients of Personal Data (in the UK)	
Categories of the recipients of the personal data	Data Subject; Past and prospective workers; HM Revenue and Customs; Pension Schemes; Financial organisations; Educators and Examining bodies; Professional Bodies; the Disclosure and Barring Service; Police Vetting service; Law enforcement agencies and bodies; Courts and Tribunals;

	Legal representatives; Ombudsman and Regulatory bodies; Partner organisations; Service providers; Debt collection and tracing agencies; Trade Unions; Licensing authorities; At the explicit request of the data subject: Credit Reference Agencies; Mortgage Providers, Housing Associations and landlords. To support TUPE arrangements the minimum necessary personal data and special categories of personal data will be passed to the new employer transferee.
Safeguards in place for the transfer of the personal data	Any disclosure or transfer of personal data / special categories of personal data will be in full compliance with the General Data Protection Regulation and established Company processes.
Details of any Information Sharing Agreements in place	Not Applicable
Recipients of Personal Data (outside of the UK)	
Categories of the recipients of the personal data	Not Applicable
Details of any transfers of personal data outside of	Not Applicable

the UK - to a third country or to an international organisation	
Safeguards in place for the transfer of the personal data	Not Applicable
Details of any Information Sharing Agreements in place	Not Applicable
Processing Measures in Place	
Technical and organisational measures in place for data security and protection	Secure IT – AVG Avast Business anti-virus software, Lockable restricted access to paper files.
Format information is held in	Electronic and paper files.
Systems data is held on	The Company processes personal data using automated means. This includes electronic drives, sage payroll, sage HR, Sage Accounts, HMRC Online, Nest Pensions, Email, DVLA Licencing, CHAS, Constructionline, ECA/ECS, CITB, purposes of an online tender/contract work, Gas Safe, RAMM Tracking.
Any Additional Information	
None	

Short Privacy Notice:

As an employer the Company collects and processes your personal data for employment and application for employment purposes. We will process your personal data in accordance with the Data Protection Act and other relevant legislation, and not disclose your personal data to any other third party, unless allowed or required to do so under the General Data Protection Regulations (GDPR). For further details about the processing of your personal data please see the Full Privacy Notice and our company GDPR Policy including retention policy available on our website www.saffronwalden.gov.uk