

Meltham Town Council

Data Protection Policy

1. Introduction

1.1 Meltham Town Council (the Council) is fully committed to compliance with the requirements of the Data Protection Act (DPA) 2018 and the General Data Protection Regulation (GDPR) which will become enforceable on 25th May 2018.

2. Purpose

2.1 This policy provide important information about:

- The data protection principles with which Meltham Town Council must comply;
- What is meant by personal information (or data) and sensitive personal information (or data);
- Roles and responsibilities
- How we gather, use and (ultimately) delete personal information and sensitive personal information in accordance with the data protection principles;
- Where more detailed privacy information can be found, e.g. about the personal information we gather and use about you, how it is used, stored and transferred, for what purposes, the steps taken to keep that information secure and for how long it is kept;
- Your rights and obligations in relation to data protection; and
- The consequences of failure to comply with this policy.

3. Data Protection Principles

3.1 Meltham Town Council will comply with the following data protection principles when processing personal information:

- we will process personal information lawfully, fairly and in a transparent manner;
- we will collect personal information for specified, explicit and legitimate purposes only, and will not process it in a way that is incompatible with those legitimate purposes;
- we will only process the personal information that is adequate, relevant and necessary for the relevant purposes;
- we will keep accurate and up to date personal information, and take reasonable steps to ensure that inaccurate personal information are deleted or corrected without delay;
- we will keep personal information in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the information is processed;
- we will take appropriate technical and organisational measures to ensure that personal information are kept secure and protected against unauthorised or unlawful processing, and against accidental loss, destruction or damage.

4. Definitions

criminal records information	means personal information relating to criminal convictions and offences, allegations, proceedings, and related security measures;
-------------------------------------	--

data breach	means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal information;
data subject	means the individual to whom the personal information relates;
personal information	(sometimes known as personal data) means information relating to an individual who can be identified (directly or indirectly) from that information;
processing information	means obtaining, recording, organising, storing, amending, retrieving, disclosing and/or destroying information, or using or doing anything with it;
pseudonymised	means the process by which personal information is processed in such a way that it cannot be used to identify an individual without the use of additional information, which is kept separately and subject to technical and organisational measures to ensure that the personal information cannot be attributed to an identifiable individual;
sensitive personal information	(sometimes known as 'special categories of personal data' or 'sensitive personal data') means personal information about an individual's race, ethnic origin, political opinions, religious or philosophical beliefs, trade union membership (or non-membership), genetics information, biometric information (where used to identify an individual) and information concerning an individual's health, sex life or sexual orientation.

5. Roles and responsibilities

5.1 The data controller is Meltham Town Council, Carlile Institute, Meltham, HD9 4AE.

5.2 The GDPR requires that the Council appoint a Data Protection Officer (DPO). The Council's DPO is: the Local Council Public Advisory Service.

5.3 The Council will follow procedures that aim to ensure that all employees, elected members, contractors, agents, consultants, partners or other servants of the council who have access to any personal data held by or on behalf of the council, are fully aware of and abide by their duties and responsibilities under the Act / Regulations.

5.4 GDPR requires continued care by everyone within the council, councillors and staff, in the sharing of information about individuals, whether as a hard copy or electronically.

5.5 A breach of the regulations could result in the council facing a fine from the Information Commissioner's Office (ICO) for the breach itself and also to compensate the individual(s) who could be adversely affected. Therefore, the handling of information is seen as medium risk to the council (both financially and reputationally) and one which must be included in the Risk Register of the Council.

5.6 Such risk can be minimised by undertaking an information audit, issuing privacy statements, undertaking privacy impact assessments (an audit of potential data protection risks with new projects), minimising who holds data protected information and the Council undertaking training in data protection awareness.

5.7 If individual Councillors act as a representative of residents of the area (e.g. taking forward complaints made by their local residents) then they would be a data controller in their own right and are not covered by the Council's compliance arrangements. It is a matter for individual Councillors to satisfy themselves that they are appropriately registered and compliant with GDPR.

6. How we gather, use and (ultimately) delete personal information and sensitive personal information

6.1 Meltham Town Council processes personal data for the following reasons:

- Staff administration
- Council / Councillor administration
- Provision of services (e.g. allotments)
- Grants administration
- Provision of information
- Dealing with general enquires
- Monitoring / Crime Prevention
- Contracting with suppliers, companies and other organisations
- Equal Opportunities monitoring

7. Documentation and records

7.1 We will keep written records of processing activities including:

- the purposes of the processing;
- a description of the categories of individuals and categories of personal data;
- categories of recipients of personal data; and
- retention schedules.

7.2 As part of our record of processing activities we document, or link to documentation, on:

- information required for privacy notices;
- records of consent;
- controller-processor contracts;
- the location of personal information;
- Data Protection Impact Assessments; and
- records of data breaches.

7.3 If we process sensitive personal information or criminal records information, we will keep written records of:

- the relevant purpose(s) for which the processing takes place, including (where required) why it is necessary for that purpose;
- the lawful basis for our processing; and

7.4 We will conduct regular reviews of the personal information we process and update our documentation accordingly.

8. Information Audit

8.1 The Council has undertaken an information audit which details the types of personal data held, where it came from, the purpose for holding that information and with

whom the council will share that information. This will include information held electronically or as a hard copy.

8.2 The information audit will be reviewed at least annually or when the council undertakes a new activity.

8.3 The information audit review will be conducted ahead of the review of this policy and will be minuted.

9. Privacy notice(s)

9.1 Meltham Town Council will issue privacy notices from time to time, informing you about the personal information that we collect and hold relating to you, how you can expect your personal information to be used and for what purposes.

9.2 We will take appropriate measures to provide information in privacy notices in a concise, transparent, intelligible and easily accessible form, using clear and plain language.

10. Basis for processing personal information

10.1 In relation to any processing activity we will, before the processing starts for the first time, and then regularly while it continues, review the purposes of the particular processing activity, and select the most appropriate lawful basis (or bases) for that processing, i.e.:

- that the data subject has consented to the processing;
- that the processing is 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;
- that the processing is necessary for compliance with a legal obligation to which the Council is subject;
- that the processing is necessary in order to protect the vital interests of the data subject or of another natural person;
- that 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

10.2 Except where the processing is based on consent, we will satisfy ourselves that the processing is necessary for the purpose of the relevant lawful basis (i.e. that there is no other reasonable way to achieve that purpose);

10.3 We will document our decision as to which lawful basis applies, to help demonstrate our compliance with the data protection principles.

10.4 We will include information about both the purposes of the processing and the lawful basis for it in our relevant privacy notice(s);

10.5 Where sensitive personal information is processed, we will also identify a lawful special condition for processing that information and document it.

10.6 Where criminal offence information is processed, we will identify a lawful condition for processing that information and document it.

11. Sensitive personal information

- 11.1 Sensitive personal information is sometimes referred to as 'special categories of personal data' or 'sensitive personal data'.
- 11.2 Meltham Town Council may from time to time need to process sensitive personal information. We will only process sensitive personal information if:
- a) we have a lawful basis for doing so as set out in paragraph 10 above, e.g. it is necessary for the performance of the employment contract, to comply with Meltham Town Council's legal obligations; and
 - b) one of the special conditions for processing sensitive personal information applies, e.g.:
 - the data subject has given explicit consent;
 - the processing is necessary for the purposes of exercising the employment law rights or obligations of the Council or the data subject;
 - the processing is necessary to protect the data subject's vital interests, and the data subject is physically incapable of giving consent;
 - processing relates to personal data which are manifestly made public by the data subject;
 - the processing is necessary for the establishment, exercise or defence of legal claims; or
 - the processing is necessary for reasons of substantial public interest.
- 11.3 Meltham Town Council's GDPR Privacy Notice(s) set out the types of sensitive personal information that is processed, what it is used for and the lawful basis for the processing.

12. Children

- 12.1 There is special protection for the personal data of a child. The age when a child can give their own consent is 13. If the Council requires consent from young people under 13, we must obtain a parent or guardian's consent in order to process the personal data lawfully. Consent forms for children age 13 plus, must be written in language that they will understand.

13. Individual rights

- 13.1 You (in common with other data subjects) have the following rights in relation to your personal information:
- to be informed about how, why and on what basis that information is processed - see Meltham Town Council's GDPR Privacy Notice(s).
 - to obtain confirmation that your information is being processed and to obtain access to it and certain other information, by making a subject access request - see Meltham Town Council's Subject Access Policy;
 - to have data corrected if it is inaccurate or incomplete;
 - to have data erased if it is no longer necessary for the purpose for which it was originally collected/processed, or if there are no overriding legitimate grounds for the processing (this is sometimes known as 'the right to be forgotten');
 - to restrict the processing of personal information where the accuracy of the information is contested, or the processing is unlawful (but you do not want the data to be erased), or where the employer no longer needs the personal information but you require the data to establish, exercise or defend a legal claim; and

- to restrict the processing of personal information temporarily where you do not think it is accurate (and the employer is verifying whether it is accurate), or where you have objected to the processing (and the employer is considering whether the organisation's legitimate grounds override your interests).

13.2 If you wish to exercise any of the rights in paragraph 13, please contact the Town Clerk.

14. Individual obligations

14.1 Individuals are responsible for helping Meltham Town Council keep their personal information up to date. For example, Council staff should inform the Council if the information they have provided to the Council changes, for example if you move house or change details of the bank or building society account to which you are paid.

14.2 Staff and councillors may have access to the personal information of other members of staff, councillors, suppliers and customers of the Council in the course of your employment or engagement. If so, Meltham Town Council expects you to help meet its data protection obligations to those individuals.

14.3 If you have access to personal information, you must:

- only access the personal information that you have authority to access, and only for authorised purposes;
- only allow other staff to access personal information if they have appropriate authorisation;
- only allow individuals who are not Meltham Town Council staff to access personal information if you have specific authority to do so from the Town Clerk.
- keep personal information secure (e.g. by complying with rules on access to premises, computer access, password protection and secure file storage and destruction and other precautions set out in the Meltham Town Council's Information Security Policy).
- not remove personal information, or devices containing personal information (or which can be used to access it), from Meltham Town Council's premises unless appropriate security measures are in place (such as pseudonymisation, encryption or password protection) to secure the information and the device; and
- not store personal information on local drives or on personal devices that are used for work purposes.

14.4 You should contact the Town Clerk if you are concerned or suspect that one of the following has taken place (or is taking place or likely to take place):

- processing of personal data without a lawful basis for its processing or, in the case of sensitive personal information, without one of the conditions in paragraph 11 being met;
- any data breach as set out in paragraph 17 below;
- access to personal information without the proper authorisation;
- personal information not kept or deleted securely;
- removal of personal information, or devices containing personal information (or which can be used to access it), from Meltham Town Council's premises without appropriate security measures being in place;
- any other breach of this Policy or of any of the data protection principles set out in paragraph 4 above.

15. Information security

15.1 Meltham Town Council will use appropriate technical and organisational measures to keep personal information secure, and in particular to protect against unauthorised or unlawful processing and against accidental loss, destruction or damage. These may include:

- making sure that, where possible, personal information is pseudonymised or encrypted;
- ensuring the ongoing confidentiality, integrity, availability and resilience of processing systems and services;
- ensuring that, in the event of a physical or technical incident, availability and access to personal information can be restored in a timely manner; and
- a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing.

15.2 Where Meltham Town Council uses external organisations to process personal information on its behalf, additional security arrangements need to be implemented in contracts with those organisations to safeguard the security of personal information. In particular, contracts with external organisations must provide that:

- the organisation may act only on the written instructions of the Council;
- those processing the data are subject to a duty of confidence;
- appropriate measures are taken to ensure the security of processing;
- sub-contractors are only engaged with the prior consent of Meltham Town Council and under a written contract;
- the organisation will assist Meltham Town Council in providing subject access and allowing individuals to exercise their rights under the GDPR;
- the organisation will assist Meltham Town Council in meeting its GDPR obligations in relation to the security of processing, the notification of data breaches and data protection impact assessments;
- the organisation will delete or return all personal information to Meltham Town Council as requested at the end of the contract; and
- the organisation will submit to audits and inspections, provide Meltham Town Council with whatever information it needs to ensure that they are both meeting their data protection obligations, and tell Meltham Town Council immediately if it is asked to do something infringing data protection law.

16. Storage and retention of personal information

16.1 Personal information (and sensitive personal information) will be kept securely in accordance with Meltham Town Council's Information Security Policy.

16.2 Personal information (and sensitive personal information) should not be retained for any longer than necessary. The length of time over which data should be retained will depend upon the circumstances, including the reasons why the personal information was obtained.

16.3 Meltham Town Council's data audit sets out the relevant retention period, or the criteria that should be used to determine the retention period. Where there is any uncertainty, staff should consult the Town Clerk.

16.4 Personal information (and sensitive personal information) that is no longer required will be deleted permanently from our information systems and any hard copies will be

destroyed securely.

17. Data breaches

17.1 A data breach may take many different forms, for example:

- loss or theft of data or equipment on which personal information is stored;
- unauthorised access to or use of personal information either by a member of staff or third party;
- loss of data resulting from an equipment or systems (including hardware and software) failure;
- human error, such as accidental deletion or alteration of data;
- unforeseen circumstances, such as a fire or flood;
- deliberate attacks on IT systems, such as hacking, viruses or phishing scams; and
- 'blagging' offences, where information is obtained by deceiving the organisation which holds it.

17.2 Meltham Town Council will:

- make the required report of a data breach to the Information Commissioner's Office without undue delay and, where possible within 72 hours of becoming aware of it, if it is likely to result in a risk to the rights and freedoms of individuals; and
- notify the affected individuals, if a data breach is likely to result in a high risk to their rights and freedoms and notification is required by law.

18. International transfers

18.1 The Council will not transfer personal information outside the European Economic Area (EEA), which comprises the countries in the European Union and Iceland, Liechtenstein and Norway.

19. Training

19.1 Meltham Town Council will ensure that staff are adequately trained regarding their data protection responsibilities. Individuals whose roles require regular access to personal information, or who are responsible for implementing this policy or responding to subject access requests under this policy, will receive additional training to help them understand their duties and how to comply with them.

20. Consequences of failing to comply

20.1 Meltham Town Council takes compliance with this policy very seriously. Failure to comply with the policy:

- puts at risk the individuals whose personal information is being processed; and
- carries the risk of significant civil and criminal sanctions for the individual and the Council;
- may, in some circumstances, amount to a criminal offence by the individual.

20.2 Because of the importance of this policy, an employee's failure to comply with any requirement of it may lead to disciplinary action under our procedures

21. Actions arising from this policy

21.1 The main actions arising from this policy are:

- The Council must pay the relevant fee to the Information Commissioners Office (ICO) and comply with the statutory regime.
- Resources will be made available to support the Town Clerk and DPO in ensuring compliance
- A Data Protection Officer (DPO) will be appointed
- A copy of this policy will be available on the Council's website. The policy will be considered as a core policy for the Council.
- Standing Orders will be amended to include responsibilities in data protection.
- An information audit will be conducted and reviewed at least annually or when projects and services change.
- Privacy notices will be prepared and published on the Council's website.
- Data Protection will be included in the Council's Risk Register, and the processes will be managed by the Council.

21.2 This policy document is written with current information and advice. It will be reviewed at least annually or when further advice is issued by the ICO.

21.3 All employees, volunteers and councillors are expected to comply with this policy at all times to protect privacy, confidentiality and the interests of the Council.

21.4 Further information about the General Data Protection Regulations, your rights and the Council's obligations can be found on the ICO website: <https://ico.org.uk/>

Date of adoption...14 May 2018.....

Date for review...Feb 2019