Trimley St Martin Parish Council Data Protection Policy

1. POLICY STATEMENT

1.1 Everyone has rights with regard as to how their personal information is handled. During the course of the Parish Council's activities, it will collect, store and process personal information about its staff, councillors, suppliers and individuals who have made contact with the Council, and it recognises the need to treat personal information in an appropriate and lawful manner.

1.2 The types of information that the Parish Council may be required to handle include details of current, past and prospective employees, suppliers, and individuals who have made contact with the Council in accordance with our document retention policy. The information, which may be held on paper or on a computer or other media, is subject to certain legal safeguards specified in the Data Protection Act 1998 (the Act) and other regulations. The Act imposes restrictions on how it may use that information.

2. STATUS OF THE POLICY

2.1 This policy sets out the Parish Council's rules on data protection and the legal conditions that must be satisfied in relation to the obtaining, handling, processing, storage, transportation and destruction of personal information.

2.2 If you consider that the policy has not been followed in respect of personal data about yourself or others you should raise the matter with the Clerk to the Parish Council.

3. DEFINITIONS

3.1 Data is information which is stored

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

3.3 Personal data means data relating to a living individual who can be identified from that data (or from that data and other information in our possession).

3.4 The data controller is the Parish Clerk of Trimley St Martin Parish Council, who determines the purposes for which, and the way any personal data is processed. The data controller has a responsibility to establish practices and policies in line with the Act.

3.5 Data users include employees whose work involves using personal data. Data users have a duty to protect the information they handle by following our data protection and security policies at all times.

3.6 Data processors include any person who processes personal data on behalf of a data controller. Employees of data controllers are excluded from this definition, but it could include suppliers which handle personal data on our behalf.

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

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

4 **DATA PROTECTION PRINCIPLES**

Anyone processing personal data must comply with the following principles. Personal data must be:

- Processed fairly and lawfully.
- Processed for limited purposes and in an appropriate way.
- Adequate, relevant and not excessive for the purpose.
- Accurate.
- Not kept longer than necessary for the purpose.
- Processed in line with data subjects' rights.
- Secure.
- Not transferred to people or organisations situated in countries without adequate protection

5 FAIR AND LAWFUL PROCESSING

5.1 The Act is intended to ensure that data processing it is done fairly and without adversely affecting the rights of the data subject. The data subject must be told who the data controller is, the purpose for which the data is to be processed by us, and the identities of anyone to whom the data may be disclosed or transferred.

5.2 For personal data to be processed lawfully, certain conditions must be met. These may include, among other things, requirements that the data subject has consented to the processing, or that the processing is necessary for the legitimate interest of the data controller or the party to whom the data is disclosed. When sensitive personal data is being processed, more than one condition must be met. In most cases the data subject's explicit consent to the processing of such data will be required.

6 PROCESSING FOR LIMITED PURPOSES

Personal data may only be processed for the specific purposes notified to the data subject when the data was first collected or for any other purposes specifically permitted by the Act. This means that personal data must not be collected for one purpose and then used for another. If it becomes necessary to change the purpose for which the data is processed, the data subject must be informed of the new purpose before any processing occurs.

7 ADEQUATE, RELEVANT AND NON-EXCESSIVE PROCESSING

Personal data should only be collected to the extent that it is required for the specific purpose notified to the data subject. Any data which is not necessary for that purpose should not be collected in the first place.

8 ACCURATE DATA

Personal data must be accurate and kept up to date. Information which is incorrect, or misleading is not accurate, and steps should therefore be taken to check the accuracy of any personal data at the point of collection and at regular intervals afterwards. Inaccurate or out-of-date data should be destroyed.

9 TIMELY PROCESSING

Personal data should not be kept longer than is necessary for the purpose. This means that data should be destroyed or erased from the Parish Council's systems when it is no longer required. For guidance on how long certain data is likely to be kept before being destroyed, please refer to Trimley St Martin Parish Council's Data Retention Policy.

10 PROCESSING IN LINE WITH DATA SUBJECT'S RIGHTS

Data must be processed in line with data subjects' rights. Trimley St martin Parish Council must ensure individuals can exercise their rights in the following ways:

- Right to be informed
    - o providing privacy notices
    - o keeping a record of how TRIMLEY ST MARTIN PC uses personal data to demonstrate compliance
- Right of access:
    - o enabling individuals to access their personal data and supplementary information
    - o be aware of and verifying the lawfulness of the processing activities
- Right to rectification:
    - o rectifying or amending personal data of the individual if requested
    - o carrying out the above process within one month
- Right to erasure:
    - o deleting or removing an individual's data if requested and there is no compelling reason for its continued processing.

• Right to restrict processing: o complying with any request to restrict, block or supress the processing of personal data

o retaining only enough data to ensure the right to restriction is respected in the future

• Right to data portability:

o providing individuals with their data so that they can reuse it for their own purposes

o providing it in a commonly used format (i.e. machine-readable format)

• Right to withdraw consent

o respecting the right of an individual to withdraw consent to the processing at any time for any processing of data to which consent was obtained o withdrawal can be by telephone, email or by post.

• The right to lodge a complaint with the Information Commissioner's Office.

contacting the Information Commissioners Office on 0303 123 1113 or via email https://ico.org.uk/global/contact-us/email/ or at the Information Commissioner's Office, Wycliffe House, Water Lane, Wilmslow, Cheshire SK9 5AF.

11 DATA SECURITY

11.1 The Parish Council must ensure that appropriate security measures are taken against unlawful or unauthorised processing of personal data, and against the accidental loss of, or damage to, personal data. Data subjects may apply to the courts for compensation if they have suffered damage from such a loss.

11.2 The Act requires us to put in place procedures and technologies to maintain the security of all personal data from the point of collection to the point of destruction. Personal data may only be transferred to a third-party data processor if he agrees to comply with those procedures and policies, or if he puts in place adequate measures himself.

11.3 Maintaining data security means guaranteeing the confidentiality, integrity and availability of the personal data, defined as follows:

(a) Confidentiality means that only authorised users may access the data.

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

(c) Availability means that authorised users should be able to access the data if they need it for authorised purposes.

11.4 Security procedures include:

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

(b) Methods of disposal. Paper documents should be shredded.

(c) Equipment. Data users should ensure that computer equipment is secure and protected by appropriate anti-virus software.

12 DEALING WITH SUBJECT ACCESS REQUESTS (SAR)

The Parish Council is aware that people have the right to access any personal information that is held about them. If a person requests to see any data that is being held about them, this will be handled in accordance with appendix A to this policy.

13 PROVIDING INFORMATION OVER THE TELEPHONE

Any member of staff dealing with telephone enquiries should be careful about disclosing any personal information held by the Parish Council. In particular they should:

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

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

(c) Refer to the Clerk for assistance in difficult situations. No-one should be bullied into disclosing personal information.

14 ACCESS TO POLICIES REFERRED TO UNDER THIS POLICY For details of all polices relevant to Trimley St Martin Parish Council as a local council please visit the Parish Council's website: http://trimleystmartin.onesuffolk.net/home/our-policies-and-procedures/

Appendix A

SUBJECT ACCESS REQUEST (SAR)

1. UPON RECEIPT OF A SAR, TRIMLEY ST MARTIN PARISH COUNCIL WILL:

(a) Verify whether TRIMLEY ST MARTIN PC is the controller of the data subject's personal data. If it is not a controller, but merely a processor, TRIMLEY ST MARTIN PC will inform the data subject and refer them to the actual controller.

(b) Verify the identity of the data subject; if needed, request any further evidence on the identity of the data subject.

(c) Verity the access request; is it sufficiently substantiated? Is it clear to the data controller what personal data is requested? If not: request additional information.

(d) Verify whether requests are unfounded or excessive (in particular because of their repetitive character); if so, TRIMLEY ST MARTIN PC may refuse to act on the request or charge a reasonable fee.

(e) Promptly acknowledge receipt of the SAR and inform the data subject of any costs involved in the processing of the SAR.

(f) Verify whether TRIMLEY ST MARTIN PC processes the data requested. If it does not process any data, inform the data subject accordingly. At all times make sure the internal SAR procedure is followed and progress can be monitored.

(g) Ensure data will not be changed as a result of the SAR. Routine changes as part of the processing activities concerned are permitted.

(h) Verify whether the data requested also involves data on other data subjects and make sure this data is filtered before the requested data is supplied to the data subject; if data cannot be filtered, ensure that other data subjects have consented to the supply of their data as part of the SAR.

2. RESPONDING TO A SAR

(a) Trimley St Martin Parish Council will respond to a SAR within one month after receipt of the request:

(i) If more time is needed to respond to complex requests, an extension of another two months is permissible, provided this is communicated to the data subject in a timely manner within the first month;

(ii) if the council cannot provide the information requested, it should inform the data subject on this decision without delay and at the latest within one month of receipt of the request.

(b) If a SAR is submitted in electronic form, any personal data should preferably be provided by electronic means as well.

(c) If data on the data subject is processed, make sure to include as a minimum the following information in the SAR response:

(i) the purposes of the processing;

(ii) the categories of personal data concerned; Adopted May 2019 Review due May 2020

(iii) the recipients or categories of recipients to whom personal data has been or will be disclosed, in particular in third countries or international organisations, including any appropriate safeguards for transfer of data, such as Binding Corporate Rules or EU model clauses ;

(iv) where possible, the envisaged period for which personal data will be stored or, if not possible, the criteria used to determine that period;

(v) the existence of the right to request rectification or erasure of personal data or restriction of processing of personal data concerning the data subject or to object to such processing;

(vi) the right to lodge a complaint with the Information Commissioners Office ("ICO"); (vii) if the data has not been collected from the data subject: the source of such data;

(viii) the existence of any automated decision-making, including profiling and any meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject.

(d) Trimley St Martin Parish Council will provide a copy of the personal data undergoing processing.

TRIMLEY ST MARTIN
TSM
PARISH COUNCIL

Appendix B

IMPACT ASSESSMENT

Under the GDPR, data protection impact assessments (DPIAs) are mandatory where the processing poses a high risk to the rights and freedoms of individuals. While they can also be carried out in other situations, councils need to be able to evaluate when a DPIA is required. The following checklist will be used to make that assessment.

Do you need to carry out a DPIA? Consider:

- What is the objective/intended outcome of the project?
- Is it a significant piece of work affecting how services/operations are currently provided?
- Who is the audience or who will be affected by the project? Will the project involve the collection of new personal data about people? e.g. new identifiers or behavioural information relating to individuals
- Will the project involve combining anonymised data sources in a way that may give rise to a risk that individuals could be identified?
- Will the project involve combining datasets originating from different processing operations or data controllers in a way which would exceed the reasonable expectations of the individuals?
- Is data being processed on a large scale? Will the project compel individuals to provide personal data about themselves?
- Will personal data about individuals be disclosed to organisations or people who have not previously had routine access to the personal data?
- Will personal data be transferred outside the EEA? Is personal data about individuals to be used for a purpose it is not currently used for, or in a way it is not currently used?
- Will personal data about children under 13 or other vulnerable persons be collected or otherwise processed?
- Will new technology be used which might be seen as privacy intrusive? E.g. CCTV
- Is data being used for automated decision making with legal or similar significant effect?
- Is data being used for evaluation or scoring? (e.g. performance at work, economic situation, health, interests or behaviour)
- Is sensitive data being collected including: (i) Race (ii) Ethnic origin (iii) Political opinions (iv) Religious or philosophical beliefs (v) Trade union membership (vi) Genetic data (vii) Biometric data (e.g. facial recognition, finger print data) (viii) Health data (ix) Data about sex life or sexual orientation?
- Will the processing itself prevent data subjects from exercising a right or using a service or contract? Is the personal data about individuals of a kind likely to raise privacy concerns or is it personal data people would consider to be particularly private or confidential?
- Will the project require contact to be made with individuals in ways they may find intrusive?

The GDPR **requires** that councils carry out a DPIA when processing is likely to result in a high risk to the rights and freedoms of data subjects. For a council, examples might include using CCTV to monitor public areas.

If two or more of the following apply, it is likely that the PC will be required to carry out a DPIA. This does not apply to existing systems but would apply on the introduction of a new system.

1. Profiling is in use. Example: you monitor website clicks or behaviour and record people's interests.

2. Automated-decision making.

3. CCTV surveillance of public areas.

4. Sensitive personal data as well as personal data relating to criminal convictions or offences.

5. Large scale data processing.

6. Linked databases which could exceed the reasonable expectations of the user.

7. Data concerning vulnerable data subjects

8. "New technologies are in use". E.g. use of social media, etc.

9. Data transfers outside of the EEA.

10. "Unavoidable and unexpected processing". For example, processing performed on a public area that people passing by cannot avoid. Example: Wi-Fi tracking.

TRIMLEY ST MARTIN
TSM
PARISH COUNCIL

Appendix C

DATA BREACH POLICY

Any incident where a data breach is suspected must be notified to the Clerk immediately or, in the absence of the Clerk, to the Chairman. The Clerk will in conjunction with the Chairman and any Councillor(s) they elect to co-opt carry out an initial investigation of the alleged breach.

If after investigating the incident it is confirmed that a personal data breach occurred:

- and it is considered likely to result in a high risk to the rights and freedoms of individuals if, for example, it could result in discrimination, damage to reputation, financial loss, loss of confidentiality, or any other significant economic or social disadvantage the Information Commissioners Office (ICO) will be notified. Any notifications to the ICO will be done as soon as possible and not later than 72 hours after the breach was identified.

- individuals affected will be promptly informed and provided with a description of the likely consequences of the personal data breach; and what measures are being taken, or proposed to be taken, including, where appropriate, the measures taken to mitigate any possible adverse effects

- As with any other breach of procedures or security the investigation will ascertain whether the breach was a result of human error or a systemic issue. The best way to ensure how a recurrence can be prevented will then be determined and implemented.